جامعة حائل
University of Ha'il

نموذج معيار إدارة الثغرات

مقيّد - داخلي

التاريخ:	05/04/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من خلال الهجمات السيبرانية، والتقليل من الآثار الناتجة عن هذه الهجمات على أعمال جامعة حائل، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-١٠-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية في جامعة حائل، وينطبق على جميع العاملين في جامعة حائل.

المعايير

1	المتطلبات العامة
الهدف	تحديد المتطلبات العامة لتقييم الثغرات التي يجب أن يتبعها فريق تقييم الثغرات الداخلي أو الخارجي قبل بدء عملية تقييم الثغرات.
المخاطر المحتملة	يمكن أن يؤدي تقييم الثغرات غير المخطط له بشكل صحيح إلى مخرجات غير كافية أو غير دقيقة، أو قد تؤثر عملية تقييم الثغرات على كفاءة الأنظمة والخدمات.
الإجراءات المطلوبة	
1-1	يجب إعداد خطة لتقييم الثغرات يوضح فيها نطاق العمل وتاريخ البدء والانتهاء. A plan for vulnerability assessment that covers the assessment scope, start date, and end date shall be developed.
2-1	يجب التأكد من أن خطة تقييم الثغرات متوافقة مع المتطلبات التشريعية والتنظيمية ذات العلاقة. Vulnerability assessment plan shall be based on the relevant legislative and regulatory requirements.

3-1	ينبغي التأكد من أن نشاط إدارة الثغرات (والذي يشمل الاكتشاف والفحص والتصنيف والمعالجة) يسير وفقاً لمنهجية محددة ووفقاً لنماذج سياسات وإجراءات وعمليات إدارة مخاطر الأمن السيبراني والمخاطر المؤسسية المعتمدة في جامعة حائل. Vulnerability management activity shall follow a defined methodology, in accordance with Hail University's enterprise and cybersecurity risk management policies, procedures, and processes.
4-1	ينبغي صياغة تقرير بعد الانتهاء من نشاط تقييم الثغرات. ويجب أن يتضمن التقرير الأقسام التالية على الأقل: • الملخص التنفيذي. • مقدمة لإعداد التقارير. • المنهجية. • الأصول المستهدفة. • تقرير تفصيلي لنتائج تقييم الثغرات. A report shall be developed after finalizing the vulnerability assessment activities. The report shall include the following sections at minimum: • Executive Summary • Reporting Introduction • Methodology • Target Assets • Detailed Findings
5-1	بعد الانتهاء من تقرير تقييم الثغرات، يجب إعداد خطة عمل لتنفيذ التوصيات، على أن يتضمن التقرير ما يلي على الأقل: • المسؤول التقني عن الأصل (Technical Owner). • مالك الأصل (Business Owner). • الإجراءات المطلوبة لتنفيذ التوصيات. • الفترة الزمنية اللازمة لتنفيذ التوصيات.

	An action plan shall be developed after finalizing the vulnerability assessment report in order to implement the recommendations. The report shall have at minimum: • Technical Owner • Business Owner • Required Actions • Clear Deadlines
6-1	ينبغي مقارنة نتائج تقييم الثغرات مع النتائج السابقة للتأكد من معالجة الثغرات السابقة في الوقت المحدد. Results from previously conducted vulnerability scans and assessments shall be compared with current results to ensure that remediation actions have been implemented in a timely manner.
2	آلية تقييم الثغرات
الهدف	تحديد ووضع خطة لوسائل تقييم الثغرات والأدوات المستخدمة التي يجب أن يتبعها فريق تقييم الثغرات الداخلي أو الخارجي قبل بدء عملية تقييم الثغرات.
المخاطر المحتملة	قد يؤدي تقييم الثغرات من غير آلية واضحة ومعتمدة إلى نتائج غير واضحة أو غير دقيقة، وبالتالي قد تُستغل تلك الثغرات قبل اكتشافها وأيضاً قد تتسبب بإهدار الموارد والوقت.
الإجراءات المطلوبة	
1-2	يجب إجراء تقييم الثغرات دورياً أو مرة واحدة في السنة على الأقل. Vulnerability assessment shall be performed periodically or at least annually.
2-2	يجب إجراء تقييم الثغرات مرة واحدة شهرياً للمكونات التقنية للأنظمة الحساسة الخارجية. (CSCC-2-9-1-2) Vulnerability assessment shall be conducted on a monthly basis for all external critical systems (Internet-facing systems). (CSCC-2-9-1-2)
3-2	يجب إجراء تقييم الثغرات مرة واحدة كل ثلاثة أشهر للمكونات التقنية للأنظمة الحساسة الداخلية. (CSCC-2-9-1-2)

	Vulnerability assessment shall be conducted on a quarterly basis for all internal critical systems. (CSCC-2-9-1-2)
4-2	يجب التأكد من تنفيذ تقييم الثغرات وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، مع الأخذ بالاعتبار الإرشادات التالية: 2-4-1 توفير المتطلبات الخاصة ببدء فحص واكتشاف الثغرات الواردة في إجراءات إدارة الثغرات. 2-4-2 تحديد المكونات التقنية المستهدفة بالفحص وتوفير الصلاحيات اللازمة للقيام بفحص واكتشاف الثغرات. 2-4-3 التأكد من أن عملية فحص واكتشاف الثغرات تغطي ثغرات الشبكة وثغرات الخدمات والرسائل النصية التعريفية (Banner Grabbing). 2-4-4 إجراء فحص واكتشاف ثغرات عن طريق وسائل وتقنيات معتمدة. 2-4-5 تصنيف الثغرات حسب خطورتها ووفقاً لمنهجية إدارة المخاطر السيبرانية. Vulnerability assessment exercise shall be conducted as per the relevant legislative and regulatory requirements, and it shall take into account the following guidelines: 2-4-1 The exercise shall meet specific vulnerability assessment requirements which are mentioned in the procedures. 2-4-2 The exercise shall define the systems/applications targeted for assessment, as well as any targeted system/application specific requirements. 2-4-3 The assessment shall include network-related vulnerabilities, service-based vulnerabilities, and banner grabbing. 2-4-4 Vulnerability assessment shall be performed using approved methods and mechanisms. 2-4-5 Risk rating shall be determined to prioritize findings as per the cybersecurity risk management methodology.
3	معالجة الثغرات
الهدف	تحديد آلية لمعالجة الثغرات بشكل فعّال ومنع أو تقليل احتمالية استغلال هذه الثغرات، وتقليل الآثار الناتجة عن هذه الهجمات على سير الأعمال.
المخاطر المحتملة	قد يؤدي عدم معالجة الثغرات إلى استغلال تلك الثغرات واستخدامها لشن هجمات سيبرانية.

	الإجراءات المطلوبة
1-3	يجب إعداد خطة لمعالجة الثغرات على المكونات التقنية المستهدفة توضح فيها تفاصيل الثغرات والتوصيات وتاريخ البدء وتاريخ الانتهاء والإدارات/المشرفين المعنيين بمعالجة الثغرات. An action plan for remediation, fixing the identified gaps and patching targeted systems/applications, shall be developed. The plan shall include vulnerabilities details, recommendations, assessment start date and end date, and the functions/teams involved in the exercise.
2-3	يجب توثيق خطة العمل واعتمادها من قبل إدارة الأمن السيبراني. The vulnerability assessment action plan shall be documented and approved by Cybersecurity Department.
3-3	يجب أن تكون جميع المكونات التقنية لدى جامعة حائل مضمونة ومدعومة من قبل المورد/المصنّع وفقاً لاتفاقية مستوى الخدمة مع المورد/المصنّع. All systems and devices within Hail University shall have vendor/manufacturer warranty as per the Service Level Agreement with the vendor/manufacturer.
4-3	يجب أن تكون لجميع المكونات التقنية الموجودة لدى جامعة حائل حزم تحديثات وإصلاحات أمنية محدثة على مستوى نظام التشغيل والتطبيقات. All systems and devices within Hail University should have up-to-date security patches at the operating system and application level.
5-3	من المستحسن أن يتم توفير تقنيات أتمتة (إن وجدت) تحديثات أنظمة التشغيل والبرامج (بما في ذلك برامج الأطراف الخارجية) داخل جامعة حائل. Automated tools for updating operating systems and software (including third party software) are encouraged to be deployed in the environment.
6-3	يجب معالجة الثغرات الحرجة (Critical Vulnerabilities) فور اكتشافها ووفقاً لآليات إدارة التغيير المعتمدة لدى جامعة حائل. ينبغي أن تكون لجميع الثغرات التي تشكل مخاطر مرتفعة أو متوسطة خطة عمل لإغلاقها ومعالجتها خلال أسبوعين كحد أقصى من تاريخ إصدار الإصلاح أو حزمة التحديثات والإصلاحات من قبل المورد، إلا إذا كان هناك مبرر تقني أو مبرر بناءً على احتياجات العمل يمنع ذلك وتم التبليغ عنه رسمياً.

Critical vulnerabilities shall be patched immediately after their discovery as per Hail University change management procedures. Any high or medium risk vulnerabilities should have a priority in the action plan, and be closed and remediated within a maximum of two weeks from releasing the fix or patch from the vendor, unless there is business or technical justification that is communicated officially.	

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني.

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الالكتروني و إدارة الأمن السيبراني.

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذا المعيار دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة الاستخدام المقبول للأصول

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني؛ لتقليل المخاطر السيبرانية، المتعلقة باستخدام أنظمة جامعة حائل وأصولها، وحمايتها من التهديدات الداخلية والخارجية، والعناية بالأهداف الأساسية للحماية؛ وهي المحافظة على سرية المعلومة، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- البنود العامة

1-1 يجب التعامل مع المعلومات حسب التصنيف المحدد، وبما يتوافق مع سياسة تصنيف البيانات وسياسة حماية البيانات والمعلومات الخاصة بـجامعة حائل بشكل يضمن حماية سرية المعلومات وسلامتها وتوافرها.

2-1 يحظر انتهاك حقوق أي شخص، أو شركة محمية بحقوق النشر، أو براءة الاختراع، أو أي ملكية فكرية أخرى، أو قوانين أو لوائح مماثلة؛ بما في ذلك، على سبيل المثال لا الحصر، تثبيت برامج غير مصرح بها أو غير قانونية.

3-1 يجب عدم ترك المطبوعات على الطابعة المشتركة دون رقابة.

4-1 يجب حفظ وسائط التخزين الخارجية بشكل آمن وملائم، مثل التأكد من ضبط درجة الحرارة بدرجة معينة، وحفظها في مكان معزول وآمن.

5-1 يمنع استخدام كلمة المرور الخاصة بمستخدمين آخرين، بما في ذلك كلمة المرور الخاصة بمدير المستخدم أو مرؤوسيه.

6-1 يجب الالتزام بسياسة المكتب الآمن والنظيف، والتأكد من خلو سطح المكتب، وكذلك شاشة العرض من المعلومات المصنفة.

7-1 يمنع الإفصاح عن أي معلومات تخص جامعة حائل، بما في ذلك المعلومات المتعلقة بالأنظمة والشبكات لأي جهة أو طرف غير مصرح له سواءً كان ذلك داخلياً أو خارجياً.

8-1 يُمنع نشر معلومات تخص جامعة حائل عبر وسائل الإعلام، وشبكات التواصل الاجتماعي دون تصريح مسبق.

9-1 يُمنع استخدام أنظمة جامعة حائل وأصولها بغرض تحقيق منفعة وأعمال شخصية، أو تحقيق أي غرض لا يتعلق بنشاط وأعمال جامعة حائل.

1-10 يُمنع ربط الأجهزة الشخصية بالشبكات، والأنظمة الخاصة بـجامعة حائل دون الحصول على تصريح مسبق، وبما يتوافق مع سياسة أمن الأجهزة المحمولة (BYOD).

1-11 يُمنع القيام بأي أنشطة تهدف إلى تجاوز أنظمة الحماية الخاصة بـجامعة حائل، بما في ذلك برامج مكافحة الفيروسات، وجدار الحماية، والبرمجيات الضارة دون الحصول على تصريح مسبق، وبما يتوافق مع الإجراءات المعتمدة لدى جامعة حائل.

1-12 تحتفظ إدارة الأمن السيبراني بحقها في مراقبة الأنظمة والشبكات والحسابات الشخصية المتعلقة بالعمل، ومراجعتها دورياً لمراقبة الالتزام بسياسات الأمن السيبراني ومعاييره.

1-13 يُمنع استضافة أشخاص غير مصرح لهم بالدخول للأماكن الحساسة دون الحصول على تصريح مسبق.

1-14 يجب ارتداء البطاقة التعريفية في جميع مرافق جامعة حائل.

1-15 يجب تبليغ إدارة الأمن السيبراني في حال فقدان المعلومات أو سرقتها أو تسريبها.

2- حماية أجهزة الحاسب الآلي

2-1 يمنع استخدام وسائط التخزين الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني

2-2 يُمنع القيام بأي نشاط من شأنه التأثير على كفاءة الأنظمة والأصول وسلامتها دون الحصول على إذن مسبق من إدارة الأمن السيبراني، بما في ذلك الأنشطة التي تُمكّن المستخدم من الحصول على صلاحيات وامتيازات أعلى.

2-3 يجب تأمين الجهاز قبل مغادرة المكتب وذلك بقفل الشاشة، أو تسجيل الخروج (Sign out or Lock)، سواء كانت المغادرة لفترة قصيرة أو عند انتهاء ساعات العمل.

2-4 يُمنع ترك أي معلومات مصنفة في أماكن يسهل الوصول إليها، أو الاطلاع عليها من قبل أشخاص غير مصرح لهم.

2-5 يُمنع تثبيت أدوات خارجية على جهاز الحاسب الآلي دون الحصول على إذن مسبق من عمادة تقنية المعلومات والتعليم الالكتروني.

2-6 يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بأي نشاط قد يتسبب بضرر على أجهزة الحاسب الآلي الخاصة بـ جامعة حائل أو أصولها.

3- الاستخدام المقبول للإنترنت والبرمجيات

3-1 يجب إبلاغ إدارة الأمن السيبراني في حال وجود مواقع مشبوهة ينبغي حجبها؛ أو العكس.

3-2 يجب ضمان عدم انتهاك حقوق الملكية الفكرية أثناء تنزيل معلومات أو مستندات لأغراض العمل.

3-3 يُمنع استخدام البرمجيات غير المرخصة أو غيرها من الممتلكات الفكرية.

3-4 يجب استخدام متصفح آمن ومصرح به للوصول إلى الشبكة الداخلية أو شبكة الإنترنت.

3-5 يُمنع استخدام التقنيات التي تسمح بتجاوز الوسيط (Proxy) أو جدار الحماية (Firewall) للوصول إلى شبكة الإنترنت.

3-6 يُمنع تنزيل البرمجيات والأدوات أو تثبيتها على أصول جامعة حائل دون الحصول على تصريح مسبق من عمادة تقنية المعلومات والتعليم الالكتروني.

7-3 يُمنع استخدام شبكة الإنترنت في غير أغراض العمل، بما في ذلك تنزيل الوسائط والملفات واستخدام برمجيات مشاركة الملفات.

8-3 يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود مخاطر سيبرانية، كما يجب التعامل بحذر مع الرسائل الأمنية التي قد تظهر خلال تصفح شبكة الإنترنت أو الشبكات الداخلية.

9-3 يُمنع إجراء فحص أمني لغرض اكتشاف الثغرات الأمنية، ويشمل ذلك إجراء اختبار الاختراقات، أو مراقبة شبكات جامعة حائل وأنظمتها، أو الشبكات والأنظمة الخاصة بالجهات الخارجية دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

10-3 يُمنع استخدام مواقع مشاركة الملفات دون الحصول على تصريح مسبق من إدارة الأمن السيبراني.

11-3 يُمنع زيارة المواقع المشبوهة بما في ذلك مواقع تعليم الاختراق.

4- الاستخدام المقبول للبريد الإلكتروني ونظام الاتصالات

1-4 يُمنع استخدام البريد الإلكتروني أو الهاتف أو الفاكس أو الفاكس الإلكتروني في غير أغراض العمل، وبما يتوافق مع سياسات الأمن السيبراني ومعاييره.

2-4 يُمنع تداول رسائل تتضمن محتوى غير لائق أو غير مقبول، بما في ذلك الرسائل المتداولة مع الأطراف الداخلية والخارجية.

3-4 يجب استخدام تقنيات التشفير عند إرسال معلومات حساسة عن طريق البريد الإلكتروني أو أنظمة الاتصالات.

4-4 يجب عدم تسجيل عنوان البريد الإلكتروني الخاص بـجامعة حائل في أي موقع ليس له علاقة بالعمل.

5-4 يجب تبليغ إدارة الأمن السيبراني عند الاشتباه بوجود رسائل بريد إلكتروني تتضمن محتوى قد يتسبب بأضرار لأنظمة جامعة حائل أو أصولها.

6-4 تحتفظ جامعة حائل بحقها في كشف محتويات رسائل البريد الإلكتروني بعد الحصول على التصاريح اللازمة من صاحب الصلاحية وإدارة الأمن السيبراني وفقاً للإجراءات والتنظيمات ذات العلاقة.

7-4 يُمنع فتح رسائل البريد الإلكتروني والمرفقات المشبوهة أو غير المتوقعة حتى وإن كانت تبدو من مصادر موثوقة.

5- الاجتماعات المرئية والاتصالات القائمة على شبكة الإنترنت

1-5 يُمنع استخدام أدوات أو برمجيات غير مصرح بها لإجراء اتصالات أو عقد اجتماعات مرئية.

2-5 يُمنع إجراء اتصالات أو عقد اجتماعات مرئية لا تتعلق بالعمل دون الحصول على تصريح مسبق.

6- استخدام كلمات المرور

1-6 يجب اختيار كلمات مرور آمنة، والمحافظة على كلمات المرور الخاصة بأنظمة جامعة حائل وأصولها. كما يجب اختيار كلمات مرور مختلفة عن كلمات مرور الحسابات الشخصية، مثل حسابات البريد الشخصي ومواقع التواصل الاجتماعي.

1-6 يُمنع مشاركة كلمة المرور عبر أي وسيلة كانت، بما في ذلك المراسلات الإلكترونية، والاتصالات الصوتية، والكتابة الورقية. كما يجب على جميع المستخدمين عدم الكشف عن كلمة المرور لأي طرف آخر بما في ذلك زملاء العمل وموظفو عمادة تقنية المعلومات والتعليم الالكتروني.

2-6 يجب تغيير كلمة المرور، عند تزويدك بكلمة مرور جديدة من قبل مسؤول النظام.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** الإدارة العامة للموارد البشرية وجميع العاملين في جامعه حائل.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.

2- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يُعرّض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المُتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة الحماية من البرمجيات الضارة

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة بـجامعة حائل من تهديدات البرمجيات الضارة وتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والخوادم الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- البنود العامة

1-1 يجب على جامعة حائل تحديد تقنيات وآليات الحماية الحديثة والمتقدمة وتوفيرها والتأكد من موثوقيتها.

2-1 يجب تطبيق تقنيات وآليات الحماية لحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم من البرمجيات الضارة (Malware) وإدارتها بشكل آمن.

3-1 يجب التأكد من أن تقنيات وآليات الحماية قادرة على اكتشاف جميع أنواع البرمجيات الضارة المعروفة وإزالتها، مثل الفيروسات (Virus)، وأحصنة طروادة (Trojan Horse)، والديدان (Worms)، وبرمجيات التجسس (Spyware)، وبرمجيات الإعلانات المتسللة (Adware)، ومجموعة الجذر (Root Kits).

4-1 قبل اختيار تقنيات وآليات الحماية، يجب التأكد من ملاءمتها لأنظمة التشغيل الخاصة بـجامعة حائل مثل أنظمة ويندوز (Windows)، وأنظمة يونكس (UNIX)، وأنظمة لينكس (Linux)، ونظام ماك (Mac)، وغيرها.

5-1 في حال تسبب تحديث تقنيات الحماية بضرر للأنظمة أو متطلبات الأعمال، يجب التأكد من أن تقنيات الحماية قابلة للاسترجاع إلى النسخة السابقة.

6-1 يجب تقييد صلاحيات تعطيل التثبيت أو إلغائه أو تغيير إعدادات تقنيات الحماية من البرمجيات الضارة ومنحها لمشرفي نظام الحماية فقط.

2- إعدادات تقنيات وآليات الحماية من البرمجيات الضارة

2-1 يجب ضبط إعدادات تقنيات الحماية وآلياتها وفقاً للمعايير التقنية الأمنية المعتمدة لدى جامعة حائل، مع الأخذ بالاعتبار إرشادات المورد وتوصياته.

2-2 يجب ضبط إعدادات برنامج مكافحة الفيروسات على خوادم البريد الإلكتروني لفحص جميع رسائل البريد الإلكتروني الواردة والصادرة.

2-3 لا يُسمح للأشخاص التابعين لأطراف خارجية بالاتصال بالشبكة أو الشبكة اللاسلكية لـجامعة حائل دون تحديث برنامج مكافحة الفيروسات وضبط الإعدادات المناسبة.

2-4 يجب ضمان توافر خوادم برامج الحماية من البرمجيات الضارة، كما يجب أن تكون البيئة الاحتياطية مناسبة لخوادم برامج الحماية من البرمجيات الضارة المخصصة للمهام والأعمال غير الحساسة.

2-5 يجب منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت المعروفة باستضافتها لبرمجيات ضارة وذلك باستخدام آلية تصفية محتوى الويب (Filtering Web Content).

2-6 يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع تقنيات وآليات الحماية من البرمجيات الضارة.

2-7 يجب ضبط إعدادات تقنيات الحماية من البرمجيات الضارة للقيام بعمليات التحقق من المحتوى المشبوه في مصادر معزولة مثل صندوق الفحص (Sandbox).

2-8 يجب القيام بعمليات مسح دورية لأجهزة المستخدمين والخوادم والتأكد من سلامتها من البرمجيات الضارة.

2-9 يجب تحديث تقنيات الحماية من البرمجيات الضارة تلقائياً عند توفر إصدارات جديدة من المورد، مع الأخذ بالاعتبار سياسة إدارة التحديثات والإصلاحات.

2-10 يجب توفير تقنيات حماية البريد الإلكتروني وتصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، والتي تستخدم عادةً الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وتطبيقها وإداراتها بشكل آمن.

2-11 يجب ضبط إعدادات تقنيات الحماية بالسماح لقائمة محددة فقط من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة. (CSCC-2-3-1-1)

2-12 يجب حماية الخوادم الخاصة بالأنظمة الحساسة عن طريق تقنيات حماية الأجهزة الطرفية المعتمدة لدى جامعة حائل (End-point Protection). (CSCC-2-3-1-2)

2-13 يجب إعداد تقارير دورية حول حالة الحماية من البرمجيات الضارة يوضح فيها عدد الأجهزة والخوادم المرتبطة بتقنيات الحماية وحالتها (مثل: محدثة، أو غير محدثة، أو غير متصلة، إلخ)، ورفعها إلى المشرف على إدارة الأمن السيبراني.

2-14 يجب إدارة تقنيات الحماية من البرمجيات الضارة مركزياً ومراقبتها باستمرار.

3- متطلبات أخرى

3-1 يجب على إدارة الأمن السيبراني التأكد من توافر الوعي الأمني اللازم لدى جميع العاملين للتعامل مع البرمجيات الضارة والتقليل من مخاطرها.

3-2 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والخوادم من البرمجيات الضارة.

3-3 يجب مراجعة متطلبات الأمن السيبراني لحماية أجهزة المستخدمين والخوادم الخاصة بـجامعة حائل دورياً.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة الالتزام بتشريعات وتنظيمات الأمن السيبراني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن برنامج الأمن السيبراني لدى جامعة حائل يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٧-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة؛ والإجراءات الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- يجب تحديد قائمة التشريعات والتنظيمات، المتعلقة بالأمن السيبراني، والمتطلبات ذات الصلة، وتوثيقها وتحديثها دورياً.

2- يجب توفير التقنيات اللازمة؛ للتحقق من الالتزام بمتطلبات الجهات التشريعية والتنظيمية، المتعلقة بالأمن السيبراني.

3- يجب مراجعة سياسات الأمن السيبراني وإجراءاته دورياً؛ لضمان التزامها بالمتطلبات التشريعية والتنظيمية، ذات العلاقة.

4- يجب التأكد من تطبيق سياسات الأمن السيبراني وإجراءاته دورياً.

5- يجب التأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة؛ بشكل دوري، عن طريق استخدام الأدوات المناسبة مثل:

5-1 أنشطة تقييم مخاطر الأمن السيبراني (Cybersecurity Risk Assessment).

5-2 أنشطة إدارة الثغرات (Vulnerabilities Management).

5-3 أنشطة اختبار الاختراقات (Penetration Test).

5-4 مراجعة معايير الأمن السيبراني.

5-5 المراجعة الأمنية للشفرة المصدرية (Security Source Code Review).

5-6 استبيانات المستخدمين.

5-7 المقابلات مع أصحاب المصلحة.

5-8 مراجعة الصلاحيات على النظام والشبكة.

5-9 مراجعة سجلات الأمن السيبراني وحوادثه.

6- يجب تحديد الإجراءات التصحيحية اللازمة والعمل على تطبيقها؛ لتصحيح الثغرات لجميع متطلبات الالتزام من قبل أصحاب العلاقة.

7- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لبرنامج الالتزام.

8- يجب تنفيذ الإجراءات المناسبة؛ لضمان الالتزام بالمتطلبات التشريعية والتنظيمية، المتعلقة بحقوق الملكية الفكرية، واستخدام البرمجيات.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.

2- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة الإعدادات والتحصين

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية وتحصين وضبط إعدادات الأصول المعلوماتية والتقنية والتطبيقات الخاصة بـجامعة حائل لمقاومة الهجمات السيبرانية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٦-٢-٢ والضابط رقم ١-٦-٣-٥ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة عن الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية والتطبيقات الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- يجب تحديد جميع الأصول المعلوماتية والتقنية المستخدمة داخل جامعة حائل وكذلك التطبيقات والبرمجيات المعتمدة والتأكد من توفير معايير تقنية أمنية (Technical Security Standards) لها.

2- يجب تطوير وتوثيق واعتماد المعايير التقنية الأمنية الخاصة بجميع الأصول المعلوماتية والتقنية والتطبيقات والبرمجيات المصرح بها داخل جامعة حائل.

3- يجب تحصين وضبط إعدادات أجهزة الحاسب الآلي، والأنظمة، والتطبيقات، وأجهزة الشبكات، والأجهزة الأمنية الخاصة بـجامعة حائل بما يتوافق مع المعايير التقنية الأمنية المعتمدة لمقاومة الهجمات السيبرانية.

4- يجب استخدام إحدى الطرق التالية لتطوير المعايير الأمنية التقنية:

1-4 دليل الإعدادات والتحصين (Security Configuration Guidance) الخاص بالمُورد وذلك وفقاً للسياسات والإجراءات التنظيمية الخاصة بـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة وأفضل الممارسات الدولية.

2-4 دليل الإعدادات والتحصين من مصادر موثوقة ومتوافقة مع المعايير المصنعية، مثل: مركز أمن الإنترنت (CIS)، ومعهد الأمن والشبكات وإدارة النظم (SANS)، والمعهد الوطني للمعايير والتقنية (NIST)، ووكالة أنظمة معلومات الدفاع (DISA)، ودليل التطبيق الفني الأمني (STIG)، وغيرها.

3-4 تطوير معايير أمنية تقنية خاصة بـجامعة حائل بما يتناسب مع طبيعة الأعمال وبما يتوافق مع دليل الإعدادات والتحصين الخاص بالمورد والمعايير المصنعية.

5- يجب أن تغطي الضوابط الخاصة بالمعايير التقنية الأمنية بحد أدنى ما يلي:

1-5 إيقاف أو تغيير الحسابات المصنعية والافتراضية.

2-5 منع تثبيت البرمجيات غير المرغوب بها.

3-5 تعطيل منافذ الشبكة غير المستخدمة.

4-5 تعطيل الخدمات غير المستخدمة.

5-5 تقييد استخدام وسائط الحفظ والتخزين الخارجي.

6-5 تغيير الإعدادات الافتراضية التي قد تُستغل في الهجمات السيبرانية.

6- يجب مراجعة الإعدادات والتحصين والتأكد من تطبيقها في الحالات التالية:

1-6 مراجعة الإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.

2-6 مراجعة الإعدادات والتحصين قبل إطلاق وتدشين المشاريع والتغييرات المتعلقة بالأصول المعلوماتية والتقنية.

3-6 مراجعة الإعدادات والتحصين قبل إطلاق وتدشين التطبيقات.

4-6 مراجعة الإعدادات والتحصين لأنظمة التحكم الصناعي دورياً والتأكد من تطبيقها وفقاً للمعايير التقنية الأمنية المعتمدة.

7- يجب اعتماد صورة (Image) لإعدادات وتحصين الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل وفقاً للمعايير التقنية الأمنية، وحفظها في مكان آمن.

8- يجب استخدام صورة (Image) معتمدة في تثبيت أو تحديث الأصول المعلوماتية والتقنية.

9- يجب توفير التقنيات اللازمة لإدارة الإعدادات والتحصين مركزياً، والتأكد من إمكانية تطبيق أو تحديث الإعدادات والتحصين تلقائياً لكافة الأصول المعلوماتية والتقنية في مواعيد زمنية محددة ومخطط لها.

10- يجب توفير نظام مراقبة الإعدادات المتوافقة مع «بروتوكول أتمتة المحتوى الأمني» (Security Content Automation Protocol "SCAP") للتأكد من أن الإعدادات متوافقة مع المعايير التقنية الأمنية المعتمدة ومطبقة بشكل كامل، كما يجب الإبلاغ عن أي تغييرات غير مصرّح بها.

11- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الإعدادات والتحصين.

12- يجب مراجعة متطلبات الأمن السيبراني المتعلقة بالإعدادات والتحصين للأصول المعلوماتية والتقنية والتطبيقات الخاصة بـجامعة حائل سنوياً، أو في حالة حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

إدارة سجلات الأحداث ومراقبة الأمن السيبراني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير؛ لتقليل المخاطر السيبرانية، وحماية الأصول المعلوماتية لـجامعة حائل من التهديدات (Threats) الداخلية والخارجية، عن طريق استخدام نظام إدارة سجلات الأحداث، ومراقبة الأمن السيبراني.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة إدارة سجلات الأحداث، ومراقبة الأمن السيبراني الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- البنود العامة

1-1 يجب توفير تقنيات إدارة المعلومات، والأحداث الأمنية (Security Information and Event Management "SIEM") اللازمة، لجمع سجلات الأحداث السيبرانية للأصول المعلوماتية، والأنظمة والتطبيقات، وقواعد البيانات والشبكات، وأنظمة الحماية في جامعة حائل. ويجب أن تحتوي هذه السجلات على المعلومات الآتية بوصفها حداً أدنى:

1-1-1 نوع الحدث (Event Type)
2-1-1 مكان الحدث، أو النظام الذي تم تنفيذ الحدث عليه (Location of Event or System)
3-1-1 وقت الحدث وتاريخه (Date and Time of Event)
4-1-1 المستخدم أو الأداة المستخدمة لتنفيذ الحدث
5-1-1 حالة الحدث أو نتيجته (Success vs. Failure)

2- الأحداث المراد تسجيلها

1-2 يجب أن تفعّل الأنظمة المراد مراقبتها سجلات الأحداث عند وقوع أحد الأحداث، بحد أدنى؛ ما يلي:

1-1-2 الأحداث (Event Logs) الخاصة بالأمن السيبراني على جميع المكونات التقنية للأنظمة الحساسة (أنظمة التشغيل، قواعد البيانات، التخزين، التطبيقات، والشبكات).

2-1-2 الأحداث (Event Logs) الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها.

3-1-2 الأحداث الخاصة بالحسابات التي تمتلك صلاحيات مهمة وحساسة على الأصول المعلوماتية.

4-1-2 الأحداث الخاصة بالتصفح والاتصال بالإنترنت، والشبكة اللاسلكية.

2-1-5 نقل المعلومات عبر وسائط التخزين الخارجية.

2-1-6 إجراء تغييرات غير مشروعة على السجلات، وملفات الأنظمة الحساسة من خلال تقنيات إدارة تغييرات الملفات ("FIM" File Integrity Management).

2-1-7 تغيير إعدادات النظام، أو الشبكة، أو الخدمات، بما في ذلك تنزيل حزم التحديثات والإصلاحات، أو غيرها من التغييرات على البرامج المثبتة.

2-1-8 أنشطة مشبوهة، مثل الأنشطة التي يكتشفها نظام منع التسلل (Intrusion Prevention System "IPS")

2-2 يجب إعداد إجراءات ومعايير أمنية تطبق أفضل الممارسات؛ لحفظ سجلات الأحداث بطريقة تضمن سلامتها من التعديل، أو الحذف، أو الوصول غير المصرح به.

2-3 يجب مراقبة سجلات الأحداث، وتحليلها دورياً حسب تصنيفها، بما في ذلك مراقبة سلوك مستخدم الأنظمة الحساسة وتحليله.

2-4 يجب مزامنة التوقيت (Clock Synchronization) مركزياً، ومن مصدر دقيق وموثوق، لجميع الأنظمة التي تتم مراقبتها.

2-5 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

2-6 يجب أرشفة سجلات الأحداث، والقيام بالنسخ الاحتياطي دورياً.

2-7 يجب أن تكون مدة الاحتفاظ بسجلات الأحداث السيبرانية 12 شهراً على الأقل، و18 شهراً بالنسبة للأنظمة الحساسة بحد أدنى، وبما يتوافق مع السياسات الداخلية، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني و إدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.

2- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

السياسة العامة للأمن السيبراني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جامعة حائل بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأعمال التنظيمية الخاصة بـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية لـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

وتعتبر هذه السياسة هي المحرك الرئيسي لجميع سياسات الأمن السيبراني وإجراءاته ومعاييره ذات المواضيع المختلفة، وكذلك أحد المدخلات لعمليات جامعة حائل الداخلية، مثل عمليات الموارد البشرية وعمليات إدارة الموردين وعمليات إدارة المشاريع وإدارة التغيير وغيرها.

عناصر السياسة

1- يجب على إدارة الأمن السيبراني تحديد معايير الأمن السيبراني وتوثيق سياساته وبرامجه، بناءً على نتائج تقييم المخاطر، وبشكل يضمن نشر متطلبات الأمن السيبراني، والتزام جامعة حائل بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة. واعتمادها من قبل رئيس الجامعه . كما يجب إطلاع العاملين المعنيين في جامعة حائل والأطراف ذات العلاقة عليها.

2- يجب على إدارة الأمن السيبراني تطوير سياسات الأمن السيبراني وبرامجه ومعاييره وتطبيقها، والمتمثلة في:

2-1 **برنامج استراتيجية الأمن السيبراني (Cybersecurity Strategy)** لضمان خطط العمل للأمن السيبراني والأهـداف والمبادرات والمشاريع وفعاليتها داخل جامعة حائل في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-2 **أدوار ومسؤوليات الأمن السيبراني (Cybersecurity Roles and Responsibilities)** لضمان تحديد مهمات ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في جامعة حائل.

2-3 **برنامج إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management)** لضمان إدارة المخاطر السيبرانية على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية لـجامعة حائل، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-2 **سياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية (Cybersecurity in Information Technology Projects)** للتأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع جامعة حائل وإجراءاتها لحماية السرية، وسلامة الأصول المعلوماتية والتقنية لـجامعة حائل وضمان دقتها وتوافرها، وكذلك التأكد من تطبيق معايير الأمن السيبراني في أنشطة تطوير التطبيقات والبرامج، وفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

5-2 **سياسة الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني (Cybersecurity Regulatory Compliance)** للتأكد من أن برنامج الأمن السيبراني لدى جامعة حائل متوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

6-2 **سياسة المراجعة والتدقيق الدوري للأمن السيبراني (Cybersecurity Periodical Assessment and Audit)** للتأكد من أن ضوابط الأمن السيبراني لدى جامعة حائل مطبقة، وتعمل وفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية التنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المُقرة تنظيمياً على جامعة حائل.

7-2 **سياسة الأمن السيبراني المتعلق بالموارد البشرية (Cybersecurity in Human Resources)** للتأكد من أن مخاطر الأمن السيبراني ومتطلباته المتعلقة بالعاملين (الموظفين والمتعاقدين) في جامعة حائل تعالج بفعالية قبل إنهاء عملهم، وأثنائه وعند انتهائه، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

8-2 **برنامج التوعية والتدريب بالأمن السيبراني (Cybersecurity Awareness and Training Program)** للتأكد من أن العاملين بـجامعة حائل لديهم الوعي الأمني اللازم، وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني، مع التأكد من تزويد العاملين بـجامعة حائل بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني؛ لحماية الأصول المعلوماتية والتقنية لـجامعة حائل والقيام بمسؤولياتهم تجاه الأمن السيبراني.

9-2 **سياسة إدارة الأصول (Asset Management)** للتأكد من أن جامعة حائل لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لـجامعة حائل، من أجل دعم العمليات التشغيلية لـجامعة حائل ومتطلبات الأمن السيبراني، لتحقيق سرية الأصول المعلوماتية والتقنية وسلامتها لـجامعة حائل ودقتها وتوافرها.

10-2 **سياسة إدارة هويات الدخول والصلاحيات (Identity and Access Management)** لضمان حماية الأمن السيبراني للوصول المنطقي (Access Logical) إلى الأصول المعلوماتية والتقنية لـجامعة حائل من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ماهو مطلوب لإنجاز الأعمال المتعلقة بـجامعة حائل.

11-2 **سياسة حماية الأنظمة وأجهزة معالجة المعلومات (Information System and Processing Facilities Protection)** لضمان حماية الأنظمة، وأجهزة معالجة المعلومات؛ بما في ذلك أجهزة المستخدمين، والبنى التحتية لـجامعة حائل من المخاطر السيبرانية.

12-2 **سياسة حماية البريد الإلكتروني (Email Protection)** لضمان حماية البريد الإلكتروني لـجامعة حائل من المخاطر السيبرانية.

2-13 **سياسة إدارة أمن الشبكات (Networks Security Management)** لضمان حماية شبكات جامعة حائل من المخاطر السيبرانية.

2-14 **سياسة أمن الأجهزة المحمولة (Mobile Devices Security)** لضمان حماية أجهزة جامعة حائل المحمولة (بما في ذلك أجهزة الحاسب المحمول، والهواتف الذكية، والأجهزة الذكية اللوحية) من المخاطر السيبرانية. ولضمان التعامل بشكل آمن مع المعلومات الحساسة، والمعلومات الخاصة بأعمال جامعة حائل وحمايتها، أثناء النقل والتخزين، وعند استخدام الأجهزة الشخصية للعاملين في جامعة حائل (مبدأ "BYOD").

2-15 **سياسة حماية البيانات والمعلومات (Data and Information Protection)** لضمان حماية السرية، وسلامة بيانات ومعلومات جامعة حائل ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-16 **سياسة التشفير ومعياره (Cryptography)** لضمان الاستخدام السليم والفعال للتشفير؛ لحماية الأصول المعلوماتية الإلكترونية لـجامعة حائل، وذلك وفقاً للسياسات، والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-17 **سياسة إدارة النسخ الاحتياطية (Backup and Recovery Management)** لضمان حماية بيانات جامعة حائل ومعلوماتها، وكذلك حماية الإعدادات التقنية للأنظمة والتطبيقات الخاصة بـجامعة حائل من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-18 **سياسة إدارة الثغرات ومعياره (Vulnerabilities Management)** لضمان اكتشاف الثغرات التقنية في الوقت المناسب، ومعالجتها بشكل فعال، وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل ذلك، وكذلك تقليل الآثار المترتبة على أعمال جامعة حائل.

2-19 **سياسة اختبار الاختراق ومعياره (Penetration Testing)** لتقييم مدى فعالية قدرات تعزيز الأمن السيبراني واختباره في جامعة حائل، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه، ولاكتشاف نقاط الضعف الأمنية غير المعروفة، والتي قد تؤدي إلى الاختراق السيبراني لـجامعة حائل؛ وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-20 **سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني (Cybersecurity Event Logs and Monitoring Management)** لضمان جمع سجلات أحداث الأمن السيبراني، وتحليلها، ومراقبتها في الوقت المناسب؛ من أجل الاكتشاف الاستباقي للهجمات السيبرانية، وإدارة مخاطرها بفعالية؛ لمنع الآثار السلبية المحتملة على أعمال جامعة حائل أو تقليلها.

2-21 **سياسة إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)** لضمان اكتشاف حوادث الأمن السيبراني وتحديدها في الوقت المناسب، وإدارتها بشكل فعّال، والتعامل مع تهديدات الأمن السيبراني استباقياً، من أجل منع الآثار السلبية المحتملة أو تقليلها على أعمال جامعة حائل، مع مراعاة ما ورد في الأمر السامي الكريم ذو الرقم 37140 والتاريخ 14\8\1438هـ.

2-22 **سياسة الأمن المادي (Physical Security)** لضمان حماية الأصول المعلوماتية والتقنية لـجامعة حائل من الوصول المادي غير المصرح به، والفقدان والسرقة والتخريب.

2-23 **سياسة حماية تطبيقات الويب ومعياره (Web Application Security)** لضمان حماية تطبيقات الويب الداخلية والخارجية لـجامعة حائل من المخاطر السيبرانية.

2-24 **جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال (Cybersecurity Resilience)** لضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال جامعة حائل، ولضمان معالجة الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة وتقليلها لـجامعة حائل وأنظمة معالجة معلوماتها وأجهزتها جراء الكوارث الناتجة عن المخاطر السيبرانية.

2-25 **سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية (Third-Party and Cloud Computing Cybersecurity)** لضمان حماية أصول جامعة حائل من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services") وفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

2-26 **سياسة الأمن السيبراني المتعلقة بالحوسبة السحابية والاستضافة (Cloud Computing and Hosting Cybersecurity)** لضمان معالجة المخاطر السيبرانية، وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعّال، وذلك وفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية، والأوامر والقرارات ذات العلاقة. وضمان حماية الأصول المعلوماتية والتقنية لـجامعة حائل على خدمات الحوسبة السحابية، التي تتم استضافتها أو معالجتها، أو إدارتها بواسطة أطراف خارجية.

2-27 **سياسة حماية أجهزة وأنظمة التحكم الصناعي (Industrial Control Systems Cybersecurity)** لضمان إدارة الأمن السيبراني بشكل سليم وفعال، لحماية توافر أصول جامعة حائل وسلامتها وسريتها؛ وهي الأصول المتعلقة وأنظمة التحكم الصناعي وأنظمته (OT\ICS) ضد الهجوم السيبراني (مثل الوصول غير المصرح به، والتخريب والتجسس والتلاعب) بما يتسق مع إستراتيجية الأمن السيبراني لـجامعة حائل، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وكذلك المتطلبات الدولية المقرّة تنظيمياً على جامعة حائل المتعلقة بالأمن السيبراني.

3- يحق لـإدارة الأمن السيبراني الاطلاع على المعلومات، وجمع الأدلة اللازمة؛ للتأكد من الالتزام بالمتطلبات التشريعية والتنظيمية ذات العلاقة المتعلقة بالأمن السيبراني.

الأدوار والمسؤوليات

1- تُمثل القائمة الآتية مجموعة الأدوار والمسؤوليات اللازمة لإقرار سياسات الأمن السيبراني وإجراءاته، ومعاييره وبرامجه، وتنفيذها واتباعها:

1-1 مسؤوليات صاحب الصلاحية معالي رئيس الجامعة أو من ينيبه، على سبيل المثال:

1-1-1 إنشاء لجنة إشرافية للأمن السيبراني ويكون مدير إدارة الأمن السيبراني أحد أعضائها.

2-1 مسؤوليات الإدارة القانونية، على سبيل المثال:

1-2-1 التأكد من أن شروط ومتطلبات الامن السيبراني والمحافظة على سرية المعلومات (Non-disclosure Clauses) مُلزمة قانونياً في عقود العاملين في جامعة حائل، والأطراف الخارجية.

3-1 مسؤوليات إدارة التدقيق والمراجعة الداخلية، على سبيل المثال:

1-3-1 مراجعة ضوابط الأمن السيبراني وتدقيق تطبيقها وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-1 مسؤوليات الإدارة العامة للموارد البشرية، على سبيل المثال:

1-4-1 تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في جامعة حائل.

5-1 مسؤوليات إدارة الأمن السيبراني، على سبيل المثال:

1-5-1 الحصول على موافقة معالي رئيس الجامعة أو من ينيبه على سياسات الأمن السيبراني، والتأكد من إطلاع الأطراف المعنية عليها وتطبيقها، ومراجعتها وتحديثها بشكل دوري.

6-1 مسؤوليات رؤساء الإدارات الأخرى، على سبيل المثال:

1-6-1 دعم سياسات الأمن السيبراني وإجراءاته ومعاييره وبرامجه، وتوفير جميع الموارد المطلوبة، لتحقيق الأهداف المنشودة، بما يخدم المصلحة العامة لـجامعة حائل.

7-1 مسؤوليات العاملين، على سبيل المثال:

1-7-1 المعرفة بمتطلبات الأمن السيبراني المتعلقة بالعاملين في جامعة حائل، والالتزام بها.

الالتزام بالسياسة

1- يجب على صاحب الصلاحية معالي رئيس الجامعة ضمان الالتزام بسياسة الأمن السيبراني ومعاييره.

2- يجب على المشرف على إدارة الأمن السيبراني التأكد من التزام جامعة حائل بسياسات الأمن السيبراني ومعاييره بشكل دوري.

3- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

4- قد يُعرّض أي انتهاك للسياسات المتعلقة بالأمن السيبراني صاحب المخالفة إلى إجراءٍ تأديبي حسب الإجراءات المتبعة في جامعة حائل.

الاستثناءات

يُمنع تجاوز سياسات الأمن السيبراني ومعاييره، دون الحصول على تصريح رسمي مسبق من مدير إدارة الأمن السيبراني أو اللجنة الإشرافية للأمن السيبراني، ما لم يتعارض مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

جامعة حائل
University of Ha'il

الأمن السيبراني للموارد البشرية

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في جامعة حائل تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٩-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة الخاصة بـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

البنود العامة

1-1 يجب تحديد متطلبات الأمن السيبراني المتعلقة بالعاملين.

2-1 يجب أن يشغل الوظائف ذات العلاقة بالأنظمة الحساسة في جامعة حائل مواطنون ذو الكفاءة اللازمة.

3-1 يجب تنفيذ ضوابط الأمن السيبراني الخاصة بالموارد البشرية خلال دورة حياة عمل الموظف (Lifecycle) في جامعة حائل والتي تشمل المراحل التالية:

- قبل التوظيف
- خلال فترة العمل
- عند انتهاء فترة العمل أو إنهائها

4-1 يجب على العاملين في جامعة حائل فهم أدوارهم الوظيفية، والشروط والمسؤوليات ذات العلاقة بالأمن السيبراني، والموافقة عليها.

5-1 يجب تضمين مسؤوليات الامن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Agreement) في عقود العاملين في جامعة حائل (لتشمل خلال وبعد انتهاء/إنهاء العلاقة الوظيفية مع جامعة حائل).

6-1 يجب إدراج المخالفات ذات العلاقة بالأمن السيبراني في لائحة مخالفات الموارد البشرية في جامعة حائل.

7-1 يُمنع الاطلاع على المعلومات الخاصة بالموظفين دون تصريح مسبق.

8-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالموارد البشرية.

قبل التوظيف

1-2 يجب على العاملين التعهد بالالتزام بسياسات الأمن السيبراني قبل منحهم صلاحية الوصول إلى أنظمة جامعة حائل.

2-2 يجب تحديد أدوار الموظفين ومسؤولياتهم مع الأخذ في الحسبان تطبيق مبدأ عدم تعارض المصالح.

3-2 يجب تحديد أدوار الموظفين ومسؤولياتهم المتعلقة بالأمن السيبراني في الوصف الوظيفي.

4-2 يجب أن تشمل الأدوار والمسؤوليات المتعلقة بالأمن السيبراني الآتي:

- حماية جميع أصول جامعة حائل من الوصول غير المصرح به، أو تخريب تلك الأصول.
- تنفيذ جميع الأنشطة المطلوبة المتعلقة بالأمن السيبراني.
- الالتزام بسياسات الأمن السيبراني ومعاييره الخاصة بـجامعة حائل.
- الالتزام ببرنامج زيادة مستوى الوعي بالمخاطر السيبرانية.

5-2 يجب إجراء مسح أمني للعاملين في وظائف الأمن السيبراني، والوظائف التقنية ذات الصلاحيات الهامة والحساسة، والوظائف ذات العلاقة بالأنظمة الحساسة.

أثناء العمل

1-3 يجب تقديم برنامج توعوي، يختص بزيادة مستوى الوعي بالأمن السيبراني؛ بما في ذلك سياسات الأمن السيبراني ومعاييره، بشكل دوري.

2-3 يجب على إدارة الموارد البشرية إبلاغ الإدارات ذات العلاقة عن أي تغيير في أدوار العاملين أو مسؤولياتهم بهدف اتخاذ الإجراءات اللازمة المتعلقة بإلغاء صلاحيات الوصول أو تعديلها.

3-3 يجب التأكد من تطبيق متطلبات الأمن السيبراني الخاصة بالموارد البشرية.

4-3 يجب إدراج مدى الالتزام بالأمن السيبراني ضمن جوانب تقييم الموظفين.

5-3 يجب التأكد من تطبيق مبدأ الحاجة إلى المعرفة (Need-to-know) في تكليف المهمات.

انتهاء الخدمة أو إنهاؤها

1-4 يجب تحديد إجراءات انتهاء الخدمة المهنية أو إنهائها بشكل يغطي متطلبات الأمن السيبراني.

2-4 يجب على إدارة الموارد البشرية إبلاغ الوحدات ذات العلاقة في حال اقتراب موعد انتهاء العلاقة الوظيفية أو إنهائها لاتخاذ الإجراءات اللازمة.

3-4 يجب التأكد من إعادة جميع الأصول الخاصة بـجامعة حائل وإلغاء صلاحيات الدخول للعاملين في آخر يوم عمل لهم وقبل حصولهم على المخالصات اللازمة.

4-4 يجب تحديد المسؤوليات والواجبات التي ستبقى سارية المفعول بعد انتهاء خدمة العاملين في جامعة حائل، بما في ذلك اتفاقية المحافظة على سرية المعلومات، على أن يتم إدراج تلك المسؤوليات والواجبات في جميع عقود العاملين.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** إدارة الموارد البشرية.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة أمن البريد الإلكتروني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية البريد الإلكتروني لـجامعة حائل من المخاطر السيبرانية والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة البريد الإلكتروني الخاصة بـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- يجب توفير تقنيات حديثة لحماية البريد الإلكتروني وتحليل وتصفية (Filtering) رسائل البريد الإلكتروني وحظر الرسائل المشبوهة، مثل الرسائل الإقتحامية (Spam Emails) ورسائل التصيّد الإلكتروني (Phishing Emails).

2- يجب أن تستخدم أنظمة البريد الإلكتروني أرقام تعريف المستخدم وكلمات المرور مرتبطة، لضمان عزل اتصالات المستخدمين المختلفين.

3- يجب توفير التقنيات اللازمة لتشفير البريد الإلكتروني الذي يحتوي على معلومات مصنفة.

4- يجب تطبيق خاصية التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).

5- يجب أرشفة رسائل البريد الإلكتروني والقيام بالنسخ الاحتياطي دورياً.

6- يجب تحديد مسؤولية البريد الإلكتروني للحسابات العامة والمشتركة (Generic Account)

7- يجب توفير تقنيات الحماية اللازمة من الفيروسات، والبرمجيات الضارة غير المعروفة مسبقا (Zero-Day Protection) على خوادم البريد الإلكتروني؛ والتأكد من فحص الرسائل قبل وصولها لصندوق بريد المستخدم.

8- يجب توثيق مجال البريد الإلكتروني لـجامعة حائل عن طريق استخدام الوسائل اللازمة؛ مثل طريقة إطار سياسة المرسل (Sender Policy Framework) لمنع تزوير البريد الإلكتروني (Email Spoofing). كما يجب التأكد من موثوقية مجالات رسائل البريد الواردة (Incoming message DMARC verification).

9- يجب أن يقتصر الوصول إلى رسائل البريد الإلكتروني على العاملين لدى جامعة حائل.

10- يجب اتخاذ الإجراءات اللازمة؛ لمنع استخدام البريد الإلكتروني لـجامعة حائل في غير أغراض العمل.

11- يمنع وصول مسؤول النظام (System Administrator) إلى معلومات البريد الإلكتروني الخاصة بأي موظف دون الحصول على تصريح مسبق.

12- يجب تحديد حجم مرفقات البريد الإلكتروني الصادر والوارد، وسعة صندوق البريد لكل مستخدم. وكذلك العمل على الحد من إتاحة إرسال الرسائل الجماعية لعدد كبير من المستخدمين.

13- يجب تذييل رسائل البريد الإلكتروني المرسلة إلى خارج جامعة حائل بإشعار إخلاء المسؤولية.

14- يجب تطبيق التقنيات اللازمة؛ لحماية سرية رسائل البريد الإلكتروني وسلامتها، وتوافرها أثناء نقلها وحفظها؛ وتشمل هذه الإجراءات استخدام تقنيات التشفير وتقنيات منع تسريب البيانات.

15- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لنظام البريد الإلكتروني.

16- يجب تعطيل خدمة تحويل البريد الإلكتروني من الخادم (Open Mail Relay).

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.

2- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يُعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة أمن الشبكات

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بأمن الشبكات الخاصة بـجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الشبكات التقنية الخاصة بـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- البنود العامة

1-1 تحديد وتوثيق جميع أجهزة الشبكة داخل جامعة حائل والتأكد من أن جميع الأجهزة محدثة ومعتمدة.

2-1 توثيق واعتماد معايير تقنية أمنية (Technical Security Standards) لجميع أجهزة الشبكة المستخدمة داخل جامعة حائل.

3-1 إدارة صلاحيات الدخول إلى الشبكات الخاصة بـجامعة حائل وفقاً لسياسة إدارة هويات الدخول والصلاحيات، بحيث يكون الاتصال بالشبكة متوفراً عند الحاجة ومتاحاً للمستخدمين المصرح لهم فقط.

2- متطلبات الوصول إلى الشبكة

1-2 تطوير واعتماد إجراءات خاصة بمنح وإلغاء صلاحيات الدخول إلى الشبكة وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات الخاصة بـجامعة حائل.

2-2 للحصول على صلاحية الدخول إلى الشبكة، يجب على المستخدم تقديم طلب إلى عمادة تقنية المعلومات والتعليم الالكتروني يوضح فيه نوع الطلب وفترة صلاحيته ومبرراته.

3-2 في حال إضافة أو التعديل على قوائم جدار الحماية، يجب على مسؤول الشبكة توثيق متطلبات الأعمال ومعلومات الطلب في نظام جدار الحماية.

4-2 يجب استخدام اسم المستخدم وكلمة المرور للدخول إلى الشبكة الخاصة بـجامعة حائل وذلك وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

5-2 مراجعة إعدادات وقوائم جدار الحماية (Firewall Rules) دورياً، وكل ستة أشهر على الأقل للأنظمة الحساسة. (CSCC-2-4-1-2)

2-6 توفير الحماية اللازمة عند تصفح الإنترنت والاتصال به، وتقييد الدخول إلى المواقع الإلكترونية المشبوهة، ومواقع مشاركة تخزين الملفات، ومواقع الدخول عن بعد.

2-7 عدم ربط الشبكة اللاسلكية بالشبكة الداخلية لـجامعة حائل، إلا بناءً على دراسة متكاملة للمخاطر المترتبة على ذلك، والتعامل معها بما يضمن حماية الأصول التقنية الخاصة وسرية البيانات وسلامتها، وحماية النظم والتطبيقات المتصلة بـجامعة حائل.

2-8 يُمنع ربط الأنظمة الحساسة بالشبكة اللاسلكية لـجامعة حائل.

2-9 يجب توفير التقنيات اللازمة لوضع القيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.

2-10 يمنع الربط المباشر لأي جهاز بالشبكة المحلية للأنظمة الحساسة قبل فحصه والتأكد من توافر عناصر الحماية المحققة للمستوى المقبول للأنظمة الحساسة (CSCC-2-4-1-3).

3- متطلبات وصول الأطراف الخارجية إلى الشبكة

3-1 يخضع منح صلاحية وصول الأطراف الخارجية إلى شبكة جامعة حائل لمتطلبات الأمن السيبراني المشار إليها في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية.

3-2 استخدام تقنيات تشفير ومصادقة آمنة لنقل البيانات من الأطراف الخارجية وإليها.

3-3 تحديد مدة زمنية معينة للأطراف الخارجية للدخول إلى شبكة جامعة حائل.

3-4 مراجعة صلاحيات المستخدمين والأطراف الخارجية دورياً وذلك وفقًا لسياسات الأمن السيبراني المعتمدة في جامعة حائل.

4- حماية الشبكات

4-1 يجب عزل وتقسيم الشبكات مادياً ومنطقياً باستخدام جدار الحماية (Firewall) ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth). (ECC-2-5-3-1)

4-2 تطبيق العزل المنطقي لشبكة الأنظمة الحساسة (VLAN).

4-3 تطبيق العزل المنطقي بين شبكة بيئة الإنتاج وشبكة بيئة الاختبار والشبكات الأخرى.

4-4 يمنع ربط الأنظمة الحساسة بالإنترنت في حال كانت هذه الأنظمة تقدم خدمة داخلية لـجامعة حائل ولا توجد هناك حاجة ضرورية جداً للدخول على الخدمة من خارج جامعة حائل. (CSCC-2-4-1-6)

4-5 تطبيق العزل المنطقي بين شبكة الاتصالات الهاتفية عبر الإنترنت (Voice Over IP "VOIP") وشبكة البيانات.

4-6 تقييد استخدام منافذ الشبكة المادية في جميع مرافق جامعة حائل وذلك باستخدام خاصية حماية المنافذ (Port Security) أو تقنية التحقق من الأجهزة (Port-Based Authentication) لحماية الشبكة من احتمالية ربط أجهزة غير مصرح بها أو أجهزة مشبوهة دون أن يتم كشفها.

4-7 توفير أنظمة الحماية في قناة تصفح الإنترنت للحماية من التهديدات المتقدمة المستمرة (APT Protection) التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المتوقعة مسبقاً (Zero-Day Malware)، وإدارتها بشكل آمن.

8-4 يمنع اتصال الشبكة الداخلية بالإنترنت مباشرةً، ويكون الاتصال عن طريق استخدام موزع اتصالات الإنترنت (Proxy) لتحليل وتصفية البيانات المنتقلة من وإلى جامعة حائل.

9-4 ضبط إعدادات قوائم جدار الحماية بحيث تُحظر جميع أنواع الاتصالات بين أجزاء الشبكة تلقائياً (Explicitly)، ويتم إتاحة قوائم جدار الحماية بناءً على طلب المستخدم ومتطلبات الأعمال.

10-4 يجب توفير التقنيات اللازمة لأمن نظام أسماء النطاقات (DNS).

11-4 يجب توفير أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention Systems) على جميع أجزاء الشبكة وتحديثها دورياً.

12-4 يجب توفير أنظمة الحماية من التهديدات المتقدمة المستمرة على مستوى الشبكة (Network APT) على شبكة الأنظمة الحساسة.

13-4 يجب تطبيق آليات حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة (APT) والبرمجيات الضارة غير المعروفة مسبقاً وإدارتها بشكل آمن. (ECC-2-5-3-8)

14-4 يجب توفير أنظمة الحماية من هجمات تعطيل الشبكات (Distributed Denial of Service Attack "DDoS") على الأنظمة الخارجية الحساسة. (CSCC-2-4-1-8)

5- الأمن المادي والبيئي

1-5 يجب حفظ أجهزة الشبكات في بيئة آمنة وملائمة، والتأكد من ضبط درجة الحرارة والرطوبة وكذلك وجود مصادر طاقة احتياطية مثل (Uninterruptible Power Supply "UPS").

2-5 يجب تقييد الدخول المادي إلى أجهزة الشبكات للمصرح لهم فقط لحفظ الأجهزة وحمايتها من السرقة أو العبث.

3-5 يجب حفظ سجلات الدخول ومراقبة مناطق أجهزة الشبكات الخاصة بالأنظمة الحساسة (CCTV) ومراجعتها دورياً.

6- متطلبات أخرى

1-6 يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لأمن الشبكات.

2-6 يجب مراجعة متطلبات الأمن السيبراني الخاصة بأمن الشبكات سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة إدارة حزم التحديثات والإصلاحات

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات الخاصة بـجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ٢-٣-٣-٣ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات وأجهزة وأنظمة التحكم الصناعي الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- يجب إدارة حزم التحديثات والإصلاحات (Patch Management) بشكل يضمن حماية الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات.

2- يجب تنزيل حزم التحديثات والإصلاحات من مصادر مرخصة وموثوقة وفقاً للإجراءات المتبعة داخل جامعة حائل.

3- يجب استخدام أنظمة تقنية موثوقة وآمنة لإجراء مسح دوري للكشف عن الثغرات وحزم التحديثات ومتابعة تطبيقها.

4- يجب على عمادة تقنية المعلومات والتعليم الالكتروني اختبار حزم التحديثات والإصلاحات في البيئة الاختبارية (Test Environment) قبل تثبيتها على الأنظمة والتطبيقات وأجهزة معالجة المعلومات في بيئة الإنتاج (Production Environment)، للتأكد من توافق حزم التحديثات والإصلاحات مع الأنظمة والتطبيقات.

5- يجب وضع خطة للاسترجاع (Rollback Plan) وتطبيقها في حال تأثير حزم التحديثات والإصلاحات سلباً على أداء الأنظمة أو التطبيقات أو الخدمات.

6- يجب على اللجنة الإشرافية للأمن السيبراني التأكد من تطبيق حزم التحديثات والإصلاحات دورياً.

7- يجب منح الأولوية لحزم التحديثات والإصلاحات التي تعالج الثغرات الأمنية حسب مستوى المخاطر المرتبطة بها.

8- يجب جدولة التحديثات والإصلاحات بما يتماشى مع مراحل الإصدارات البرمجية التي يطرحها المورد.

9- يجب تنصيب التحديثات والإصلاحات مرّة واحدة شهرياً على الأقل للأنظمة الحسّاسة المتصلة بالإنترنت، ومرّة واحدة كل ثلاثة أشهر للأنظمة الحسّاسة الداخلية. (CSCC-2-3-1-3)

10- يجب تنصيب التحديثات والإصلاحات للأصول التقنية على النحو التالي:

نوع الأصل	مدة التكرار لتنصيب التحديثات	
	الأصول المعلوماتية والتقنية	الأصول المعلوماتية والتقنية للأنظمة الحساسة
أنظمة التشغيل	شهرياً	شهرياً
قواعد البيانات	ثلاثة أشهر	شهرياً
أجهزة الشبكة	ثلاثة أشهر	شهرياً
التطبيقات	ثلاثة أشهر	شهرياً

11- يجب أن تتبع عملية إدارة التحديثات والإصلاحات متطلّبات عملية إدارة التغيير.

12- في حال وجود ثغرات أمنية ذات مخاطر عالية، يجب تنصيب حزم التحديثات والإصلاحات الطارئة وفقاً لعملية إدارة التغيير الطارئة (Emergency Change Management).

13- يجب تنزيل التحديثات والإصلاحات على خادم مركزي (Centralized Patch Management Server) قبل تنصيبها على الأنظمة والتطبيقات وقواعد البيانات وأجهزة الشبكة وأجهزة معالجة المعلومات، ويُستثنى من ذلك حزم التحديثات والإصلاحات التي لا يتوفر لها أدوات آلية مدعومة.

14- بعد تنصيب حزم التحديثات والإصلاحات، يجب استخدام أدوات مستقلة وموثوقة للتأكد من أن الثغرات تمت معالجتها بشكل فعال.

15- يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لإدارة حزم التحديثات والإصلاحات.

16- يجب مراجعة سياسة إدارة حزم التحديثات والإصلاحات وإجراءاتها سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل مستمر.

2- يجب على إدارة الأمن السيبراني وعمادة تقنية المعلومات والتعليم الالكتروني في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة أمن الخوادم

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالخوادم (Servers) الخاصة بـجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الخوادم الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- البنود العامة

1-1 يجب تحديد جميع الخوادم الخاصة بـجامعة حائل وتوثيقها، والتأكد من أن برمجيات الخوادم محدثة ومعتمدة.

2-1 يجب تطوير وتطبيق معايير تقنية أمنية (Technical Security Standards) للخوادم المستخدمة داخل جامعة حائل باستخدام أفضل المعايير الدولية.

3-1 يجب ضبط إعدادات الخوادم وفقاً للمعايير التقنية الأمنية المعتمدة قبل تشغيل الخوادم في بيئة الإنتاج.

4-1 يجب توفير الحماية اللازمة لجميع الخوادم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة.

5-1 يجب عمل نسخ احتياطية منتظمة للخوادم وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة حائل لضمان إمكانية استعادتها في حال تعرّضها لتلف أو حادث غير مقصود. (توصي الهيئة بعمل نسخ احتياطية يومياً للأنظمة الحساسة).

6-1 يجب تحديث برمجيات الخوادم بما في ذلك أنظمة التشغيل وبرامج التطبيقات وتزويدها بأحدث حزم التحديثات والإصلاحات الأمنية وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في جامعة حائل.

2- إعدادات الخوادم

1-2 يجب اعتماد صورة (Image) لإعدادات وتحصين أنظمة تشغيل الخوادم الخاصة بـجامعة حائل وحفظها في مكان آمن وفقاً للمعايير التقنية الأمنية المعتمدة.

2-2 يجب استخدام صورة (Image) معتمدة لتثبيت أنظمة تشغيل الخوادم أو تحديثها.

3-2 يجب اعتماد إعدادات وتحصين الخوادم، ومراجعتها وتحديثها دورياً، وكل ستة أشهر على الأقل بالنسبة لخوادم الأنظمة الحساسة (CSCC-6-1-3-2).

3- الوصول والإدارة

1-3 يجب تقييد الوصول إلى الخوادم الخاصة بـجامعة حائل بحيث يكون الوصول متاحاً للمستخدمين المصرح لهم وعند الحاجة فقط.

2-3 يجب تقييد الدخول إلى الخوادم وحصره على حسابات مشرفي الأنظمة ومراجعة الحسابات والصلاحيات الممنوحة للمشرفين بشكل دوري.

3-3 يجب تقييد الوصول إلى الخوادم الخاصة بالأنظمة الحساسة وحصره على الفريق التقني ذي الصلاحيات الهامة وذلك عن طريق أجهزة حاسب (Workstations)، كما يجب عزل هذه الأجهزة في شبكة خاصة لإدارة الأنظمة (Management Network)، ومنع ارتباطها بأي شبكة أو خدمة أخرى (مثل خدمة البريد الإلكتروني والإنترنت).

4-3 يجب استخدام التحقق من الهوية متعدد العناصر (Multi-Factor Authentication) للدخول إلى الخوادم الخاصة بالأنظمة الحساسة (CSCC-3-1-2-2).

5-3 يجب إيقاف الحسابات المصنعية والافتراضية أو تغييرها، وإيقاف الخدمات غير المستخدمة، ومنافذ الشبكة غير المستخدمة في نظام التشغيل (Operating System).

6-3 يجب حماية البيانات المخزنة على الخوادم وتشفيرها بالتوافق مع ضوابط التشفير المعتمدة بناءً على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة. (ECC-2-8-3-3).

4- حماية الخوادم

1-4 يجب أن تُمنَع الخوادم غير المحدّثة أو غير الموثوقة من الاتصال بشبكة جامعة حائل ووضعها في شبكة معزولة لأخذ التحديثات اللازمة لتقليل المخاطر السيبرانية ذات العلاقة والتي قد تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات.

2-4 يجب استخدام تقنيات وآليات الحماية الحديثة والمتقدمة للحماية من الفيروسات (Virus) والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) وإدارتها بشكل آمن.

3-4 يجب السماح فقط بقائمة محددة من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة (CSCC-2-3-1-1).

4-4 يجب تقييد استخدام وسائط التخزين الخارجية على الخوادم، ويجب الحصول على إذن مسبق من إدارة الأمن السيبراني قبل استخدامها، والتأكد من استخدامها بشكل آمن.

5-4 يجب تثبيت الخوادم في المنطقة المناسبة من مخطط/هيكل الشبكة حسب المتطلبات التشغيلية والتشريعية لها لضمان إدارتها وتطبيق الحماية اللازمة عليها بشكل فعّال.

5- المتطلبات التشغيلية لإدارة الخوادم

1-5 يجب إدارة الخوادم مركزياً في جامعة حائل لكشف المخاطر بصورة أسرع، وتسهيل إدارة ومراقبة الخوادم مثل تقييد الوصول وتثبيت حزم التحديثات وغيرها.

2-5 يجب توفير الحماية اللازمة للخوادم التي تعمل في بيئة الأنظمة الافتراضية (Virtual Environment) وإدارتها بشكل آمن حسب تقييم المخاطر.

3-5 يجب ضبط إعدادات الخوادم وتفعيل إرسال سجلات الأحداث إلى نظام السجلات والمراقبة (SIEM) وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

4-5 يجب مزامنة توقيت جميع الخوادم مركزياً (Clock Synchronization) من مصدر دقيق وموثوق ومعتمد.

5-5 يجب توفير المتطلبات اللازمة لتشغيل الخوادم بشكل آمن وملائم، مثل توفير بيئة مناسبة وآمنة وتقييد الوصول المادي إلى منطقة الخوادم للعاملين المصرح لهم فقط ومراقبته.

6-5 يجب على عمادة تقنية المعلومات والتعليم الالكتروني مراقبة مكونات الخوادم التشغيلية والتأكد من فعالية أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحو ذلك.

6- إدارة الثغرات واختبار الاختراق

1-6 يجب فحص الخوادم واكتشاف الثغرات الموجودة فيها ومعالجتها بناءً على تصنيف الثغرات المكتشفة والمخاطر السيبرانية المترتبة عليها دورياً، ومرة واحدة شهرياً على الأقل بالنسبة لخوادم الأنظمة الحساسة (CSCC-2-9-1-2).

2-6 يجب تنفيذ عمليات اختبار الاختراق على الخوادم دورياً، وكل ثلاثة أشهر على الأقل على خوادم الأنظمة الحساسة (CSCC-2-10-2).

3-6 يجب تثبيت حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات ورفع مستوى كفاءة الخوادم وأمنها، حسب سياسة إدارة التحديثات والإصلاحات.

7- الحماية المادية والبيئية للخوادم

1-7 يجب رصد ومراقبة الدخول والخروج من مرافق جامعة حائل، على سبيل المثال الأبواب والأقفال.

2-7 يجب رصد ومراقبة العوامل البيئية كالتدفئة وتكييف الهواء والدخان وأجهزة إنذار الحريق وأنظمة إخماد الحرائق.

3-7 يجب الالتزام بوضع الضوابط الأمنية المادية المناسبة (مثل كاميرات المراقبة داخل وخارج مركز بيانات جامعة حائل، وحراس الأمن، وتأمين الكابلات، وغيرها).

8- متطلبات أخرى

1-8 يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لحماية الخوادم.

2-8 يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة الخوادم سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن استخدام أجهزة المستخدمين (Workstations)، والأجهزة المحمولة (Mobile Devices)، والأجهزة الشخصية للعاملين (Bring Your Own Device "BYOD") داخل جامعة حائل، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات وسلامتها وتوافرها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضوابط رقم ٢-٣-١ و٢-٦-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية للعاملين داخل جامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- البنود العامة

1-1 يجب حماية البيانات والمعلومات المُخزّنة في أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) حسب تصنيفها باستخدام الضوابط الأمنية المناسبة لتقييد الوصول إلى هذه المعلومات، ومنع العاملين غير المصرّح لهم من الوصول لها أو الاطلاع عليها.

2-1 يجب تحديث برمجيات أجهزة المستخدمين والأجهزة المحمولة، بما في ذلك أنظمة التشغيل والبرامج والتطبيقات، وتزويدها بأحدث حزم التحديثات والإصلاحات وذلك وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في جامعة حائل.

3-1 يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة وفقاً لمعايير الأمن السيبراني.

4-1 يجب عدم منح العاملين صلاحيات هامة وحساسة (Privileged Access) على أجهزة المستخدمين والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.

5-1 يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.

6-1 يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين والأجهزة المحمولة.

7-1 يجب تزويد أجهزة المستخدمين والأجهزة المحمولة برسالة نصيّة (Banner) لإتاحة الاستخدام المصرّح به.

1-8 يجب السماح فقط بقائمة محددة من التطبيقات (Application Whitelisting) ومنع تسرّب البيانات (Data Leakage Prevention) واستخدام أنظمة مراقبة البيانات وغيرها.

1-9 يجب تشفير وسائط التخزين الخاصة بأجهزة المستخدمين والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة وفقاً لمعيار التشفير المعتمد في جامعة حائل.

1-10 يجب منع استخدام وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة الأمن السيبراني لامتلاك صلاحية استخدام وسائط التخزين الخارجية.

1-11 يجب عدم السماح لأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) المزوّدة ببرمجيات غير محدثة أو منتهية الصلاحية (بما في ذلك أنظمة التشغيل والبرامج والتطبيقات) بالاتصال بشبكة جامعة حائل لمنع التهديدات الأمنية الناشئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.

1-12 يجب أن تُمنَع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المزوّدة بأحدث برمجيات الحماية من الاتصال بشبكة جامعة حائل لتجنب حدوث المخاطر السيبرانية التي تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات. وتتضمّن برمجيات الحماية برامج إلزامية، مثل: برامج الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware)، وجدار الحماية للمستضيف (Host-Based Firewall)، وأنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Detection/Prevention)

1-13 يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة غير المستخدمة بحيث تعرض شاشة توقّف محمية بكلمة مرور في حال عدم استخدام الجهاز (Session Timeout) لمدة 3 دقائق.

1-14 يجب إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً من خلال خادم الدليل النشط (Active Directory) الخاص بنطاق جامعة حائل أو نظام إداري مركزي.

1-15 يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة بإدارة الوحدات التنظيمية المناسبة (Domain Controller) لتطبيق السياسات الملائمة وتثبيت الإعدادات البرمجية اللازمة.

1-16 يجب تنفيذ سياسات النطاق المناسبة (Group Policy) في جامعة حائل وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة لضمان التزام جامعة حائل بالضوابط التنظيمية والأمنية.

2- متطلبات الأمن السيبراني لأمن أجهزة المستخدمين

2-1 يجب تخصيص أجهزة المستخدمين للفريق التقني ذي الصلاحيات الهامة، وأن تكون معزولة في شبكة خاصة لإدارة الأنظمة (Management Network) ولا ترتبط بأي شبكة أو خدمة أخرى.

2-2 يجب ضبط إعدادات أجهزة المستخدمين الهامة والحساسة والتي لها صلاحيات متقدمة لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني، مع عدم إمكانية إيقافه عن طريق المستخدم.

2-3 يجب تأمين أجهزة المستخدمين مادياً داخل مباني جامعة حائل.

3- متطلبات الأمن السيبراني لأمن الأجهزة المحمولة

3-1 يجب منع وصول الأجهزة المحمولة إلى الأنظمة الحساسة إلا لفترة مؤقتة فقط، وذلك بعد إجراء تقييم المخاطر وأخذ الموافقات اللازمة من إدارة الأمن السيبراني. (CSCC-2-5-1-1)

2-3 يجب تشفير أقراص الأجهزة المحمولة التي تملك صلاحية الوصول للأنظمة الحساسة تشفيراً كاملاً (Full Disk Encryption). (CSCC-2-5-1-2)

4- متطلبات الأمن السيبراني لأمن الأجهزة الشخصية (BYOD)

1-4 يجب إدارة الأجهزة المحمولة مركزياً باستخدام نظام إدارة الأجهزة المحمولة (Mobile Device Management "MDM").

2-4 يجب فصل وتشفير البيانات والمعلومات الخاصة بـجامعة حائل المخزنة على الأجهزة الشخصية للعاملين (BYOD).

5- متطلبات أخرى

1-5 إجراء نسخ احتياطي دوري للبيانات المخزّنة على أجهزة المستخدمين والأجهزة المحمولة، وذلك وفقاً لسياسة النسخ الاحتياطية المعتمدة في جامعة حائل.

2-5 تُحذَف بيانات جامعة حائل المُخزّنة على الأجهزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية:

- فقدان الجهاز المحمول أو سرقته.
- انتهاء أو إنهاء العلاقة الوظيفية بين المستخدم وجامعة حائل.

3-5 يجب نشر الوعي الأمني للعاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول المعتمدة في جامعة حائل وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصلاحيات الهامة والحساسة.

4-5 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والأجهزة المحمولة.

5-5 يجب مراجعة سياسة أمن أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على عمادة تقنية المعلومات والتعليم الالكتروني و إدارة الأمن السيبراني في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة مراجعة وتدقيق الأمن السيبراني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متابع

قائمة المحتويات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لمراجعة وتدقيق ضوابط الأمن السيبراني لدى جامعة حائل والتأكد من تطبيقها وأنها تعمل وفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية الوطنية ذات العلاقة، والمتطلبات الدولية المقرة تنظيمياً على جامعة حائل.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-٨-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع ضوابط الأمن السيبراني في جامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- البنود العامة

1-1 يجب على إدارة الأمن السيبراني مراجعة تطبيق ضوابط الأمن السيبراني دورياً، ومراجعة مدى الالتزام بالضوابط الأساسية للأمن السيبراني (ECC:1-2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019) الصادرة من الهيئة الوطنية للأمن السيبراني.

2-1 يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني دورياً من قبل أطراف مستقلة عن إدارة الأمن السيبراني، مثل إدارة المراجعة الداخلية أو طرف خارجي.

3-1 يجب أن تتم مراجعة تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة مرة واحدة كل ثلاث سنوات على الأقل من قبل أطراف مستقلة عن إدارة الأمن السيبراني من داخل جامعة حائل.

4-1 يجب التأكد من تطبيق ضوابط الأمن السيبراني دورياً، ومرّة واحدة سنوياً على الأقل للأنظمة الحسّاسة للتأكد من مواءمتها مع الضوابط الأساسية للأمن السيبراني (ECC:1-2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019).

5-1 يجب تحديد إجراءات مراجعة وتدقيق الأمن السيبراني وتوثيقها.

6-1 يجب توثيق نتائج مراجعة وتدقيق الأمن السيبراني ومناقشتها مع الإدارات المعنية.

7-1 يجب عرض النتائج على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية، كما يجب أن تشمل النتائج نطاق المراجعة والتدقيق، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وتقييم المخاطر وخطة معالجة الملاحظات.

8-1 يجب اعتماد جدول المسؤوليات التالي (RACI Chart) في تنفيذ عمليات مراجعة وتدقيق الأمن السيبراني:

	المدقق الخارجي	التدقيق الداخلي	إدارة الأمن السيبراني	مدير إدارة الأمن السيبراني	مدير إدارة الأمن السيبراني	رئيس الجامعة
مراجعة الأمن السيبراني	R		R	A	I	I
تدقيق الأمن السيبراني	R	R	I	I	A	I
تنفيذ إجراءات تصحيحية	C/I	C/I	R	R	A	I

2- متطلبات أخرى

2-1 يجب أن تتخذ إدارة الأمن السيبراني إجراءات استباقية وتصحيحية خاصة بنتائج المراجعة والتدقيق.

2-2 يجب على إدارة الأمن السيبراني تحديد العوامل التي أدّت إلى هذه الملاحظات وتحليلها ومعرفة أسبابها والحد من تكرارها.

3-2 يجب مراجعة سياسة مراجعة وتدقيق الأمن السيبراني سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** إدارة المراجعة الداخلية.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة إدارة هويات الدخول والصلاحيات

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

`

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة هويات الدخول والصلاحيات على الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية، وذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- إدارة هويات الدخول والصلاحيات (Identity and Access Management)

1-1 إدارة الصلاحيات

1-1-1 توثيق واعتماد إجراء لإدارة الوصول يوضح آلية منح صلاحيات الوصول للأصول المعلوماتية والتقنية وتعديلها وإلغائها في جامعة حائل، ومراقبة هذه الآلية والتأكد من تطبيقها.

2-1-1 إنشاء هويات المستخدمين (User Identities) وفقاً للمتطلبات التشريعية والتنظيمية الخاصة بـجامعة حائل.

3-1-1 التحقق من هوية المستخدم (Authentication) والتحقق من صحتها قبل منح المستخدم صلاحية الوصول إلى الأصول المعلوماتية والتقنية.

4-1-1 توثيق واعتماد مصفوفة (Matrix) لإدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:

1-4-1-1 مبدأ الحاجة إلى المعرفة والاستخدام (Need-to-Know and Need-to-Use).

2-4-1-1 مبدأ فصل المهام (Segregation of Duties).

3-4-1-1 مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege).

5-1-1 تطبيق ضوابط التحقّق والصلاحيات على جميع الأصول التقنية والمعلوماتية في جامعة حائل من خلال نظام مركزي آلي للتحكّم في الوصول، مثل بروتوكول النفاذ إلى الدليل البسيط (Lightweight Directory Access Protocol "LDAP").

`

1-1-6 منع استخدام الحسابات المشتركة (Generic User) للوصول إلى الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل.

1-1-7 ضبط إعدادات الأنظمة ليتم إغلاقها تلقائياً بعد فترة زمنية محدّدة (Session Timeout)، (يوصى ألا تتجاوز الفترة 15 دقيقة).

1-1-8 تعطيل حسابات المستخدمين غير المستخدمة خلال فترة زمنية محدّدة (يوصى ألا تتجاوز الفترة 90 يوماً).

1-1-9 ضبط إعدادات جميع أنظمة إدارة الهويات والوصول لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

1-1-10 عدم منح المستخدمين صلاحيات الوصول أو التعامل المباشر مع قواعد البيانات للأنظمة الحساسة، حيث يكون ذلك من خلال التطبيقات فقط، ويستثنى من ذلك مشرفي قواعد البيانات (Database Administrators). [CSCC-2-2-1-7]

1-1-11 توثيق واعتماد إجراءات واضحة للتعامل مع حسابات الخدمات (Service Account) والتأكد من إدارتها بشكل آمن مابين التطبيقات والأنظمة، وتعطيل الدخول البشري التفاعلي (Interactive Login) من خلالها. (CSCC-2-2-1-7)

2-1 منح حق الدخول

1-2-1 متطلبات حق الدخول لحسابات المستخدمين

1-2-1-1 منح صلاحية الدخول بناءً على طلب المستخدم من خلال نموذج أو عن طريق النظام المعتمد من قبل مديره المباشر ومالك النظام (System Owner) يُحدّد فيه اسم النظام ونوع الطلب والصلاحية ومدتها (في حال كانت صلاحية الدخول مؤقتة).

1-2-1-2 منح المستخدم حق الوصول إلى الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل بما يتوافق مع الأدوار والمسؤوليات الخاصة به.

1-2-1-3 اتباع آلية موحدة لإنشاء هويات المستخدمين بطريقة تتيح تتبع النشاطات التي يتم أداؤها باستخدام "هوية المستخدم" (User ID) وربطها مع المستخدم، مثل كتابة <الحرف الأول من الاسم الأول> نقطة <الاسم الأخير>، أو كتابة رقم الموظف المعرف مسبقاً لدى الإدارة العامة للموارد البشرية.

1-2-1-4 تعطيل إمكانية تسجيل دخول المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت (Concurrent Logins).

2-2-1 متطلبات حق الوصول للحسابات الهامة والحسّاسة

بالإضافة إلى الضوابط المذكورة في قسم متطلبات حق الوصول لحسابات المستخدمين، يجب أن تُطبَق الضوابط المُوضّحة أدناه على الحسابات ذات الصلاحيات الهامة والحسّاسة:

`

1-2-2-1 تعيين حق وصول مستخدم فردي للمستخدمين الذين يطلبون الصلاحيات الهامة والحسّاسة (Administrator Privilege) ومنحهم هذا الحق بناءً على مهامهم الوظيفية، مع الأخذ بالاعتبار مبدأ فصل المهام.

2-2-2-1 يجب تفعيل سجل كلمة المرور (Password History) لتتبع عدد كلمات المرور التي تم تغييرها.

3-2-2-1 تغيير أسماء الحسابات الافتراضية، وخصوصاً الحسابات الحاصلة على صلاحيات هامة وحسّاسة مثل "الحساب الرئيسي" (Root) وحساب "مدير النظام" (Admin) وحساب "مُعرّف النظام الفريد" (Sys id).

4-2-2-1 منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في العمليات التشغيلية اليومية.

5-2-2-1 التحقّق من حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة على الأصول التقنية والمعلوماتية من خلال آلية التحقّق من الهوية متعدد العناصر (Multi-Factor Authentication "MFA") باستخدام طريقتين على الأقل من الطرق التالية:

- المعرفة (شيء يعرفه المستخدم "مثل كلمة المرور").
- الحيازة (شيء يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها "One-Time-Password").
- الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع").

6-2-2-1 يجب أن يتطلب الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها استخدام التحقق من الهوية متعدد العناصر (MFA) لجميع المستخدمين.

3-2-1 الدخول عن بُعد إلى شبكات جامعة حائل

1-3-2-1 منح صلاحية الدخول عن بعد للأصول المعلوماتية والتقنية بعد الحصول على إذن مسبق من إدارة الأمن السيبراني وتقييد الدخول باستخدام التحقق من الهوية متعدد العناصر (MFA).

2-3-2-1 حفظ سجلات الأحداث المتعلقة بجميع جلسات الدخول عن بُعد الخاصة ومراقبتها حسب حساسية الأصول المعلوماتية والتقنية.

3-1 إلغاء وتغيير حق الوصول

1-3-1 يجب على الإدارة العامة للموارد البشرية تبليغ عمادة تقنية المعلومات والتعليم الالكتروني لاتخاذ الإجراء اللازم عند انتقال المستخدم أو تغيير مهامه أو إنهاء/انتهاء العلاقة الوظيفية

`

بين المستخدم وجامعة حائل. وتقوم عمادة تقنية المعلومات والتعليم الالكتروني بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمستخدم بناءً على مهامه الوظيفية الجديدة.

2-3-1 في حال تم إيقاف صلاحيات المستخدم، يمنع حذف سجلات الأحداث الخاصة بالمستخدم ويتم حفظها وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

2- مراجعة هويات الدخول والصلاحيات

2-1 مراجعة هويات الدخول (User IDs) والتحقق من صلاحية الوصول إلى الأصول المعلوماتية والتقنية وفقاً للمهام الوظيفية للمستخدم بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة هويات الدخول على الأنظمة الحساسة مرة واحدة كل ثلاثة أشهر على الأقل.

2-2 مراجعة الصلاحيات الخاصة (User Profile) بالأصول المعلوماتية والتقنية بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة الصلاحيات الخاصة بالأنظمة الحساسة مرة واحدة سنوياً على الأقل.

2-3 يجب تسجيل وتوثيق جميع محاولات الوصول الفاشلة والناجحة ومراجعتها دورياً.

3- إدارة كلمات المرور

3-1 تطبيق سياسة آمنة لكلمة المرور ذات معايير عالية لجميع الحسابات داخل جامعة حائل، ويتضمّن الجدول أدناه أمثلة على ضوابط كلمات المرور لكل مستخدم:

ضوابط كلمات المرور	جميع المستخدمين (All Users)	حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة Privileged) (Users	حسابات الخدمات Service) (Account
الحدّ الأدنى لعدد أحرف كلمة المرور	8 أحرف أو أرقام أو رموز	12 حرفاً أو رقماً أو رمزاً	8 أحرف أو أرقام أو رموز
سجل كلمة المرور	تذكّر 5 كلمات مرور	تذكّر 5 كلمات مرور	تذكّر 5 كلمات مرور
الحد الأعلى لعمر كلمة المرور	45 يوماً	45 يوماً	45 يوماً
مدى تعقيد كلمة المرور	مُفعّل	مُفعّل	مُفعّل
مثال على تعقيد كلمة المرور	D_dyW5$_	R@rS%7qY#b!u	r?M4d5V=
مدة إغلاق الحساب	30 دقيقة أو حتى يقوم النظام بفك الإغلاق	30 دقيقة أو حتى يقوم النظام بفك الإغلاق	30 دقيقة أو حتى يقوم النظام بفك الإغلاق
حد إغلاق الحساب	5 محاولات غير صحيحة لتسجيل الدخول	5 محاولات غير صحيحة لتسجيل الدخول	لا توجد محاولات
إعادة ضبط عداد إغلاق الحساب بعد مرور فترة معينة	30 دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	30 دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	لا يوجد
استخدام التحقق متعدد العناصر	مُفعل على الدخول عن بعد فقط	مُفعل	غير مُفعل

2-3 معايير كلمات المرور

`

1-2-3 يجب أن تتضمّن كلمة المرور (8) أحرف على الأقل.

2-2-3 يجب أن تكون كلمة المرور معقّدة (Complex Password) وتتضمّن ثلاثة رموز من الرموز التالية على الأقل:

1-2-2-3 أحرف كبيرة (Upper Case Letters).

2-2-2-3 أحرف صغيرة (Lower Case Letters).

3-2-2-3 أرقام (1235).

4-2-2-3 رموز خاصّة (@#%*).

3-2-3 يجب إشعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية.

4-2-3 يجب ضبط إعدادات كافة الأصول المعلوماتية والتقنية لطلب تغيير كلمة المرور المؤقتة عند تسجيل المستخدم الدخول لأول مرة.

5-2-3 يجب تغيير جميع كلمات المرور الافتراضية لجميع الأصول المعلوماتية والتقنية قبل تثبيتها في بيئة الإنتاج.

6-2-3 يجب تغيير كلمات مرور السلاسل النصية (Community String) الافتراضية (مثل: «Public» و«Private» و«System») الخاصة ببروتوكول إدارة الشبكة البسيط (SNMP)، ويجب أن تكون مختلفة عن كلمات المرور المستخدمة لتسجيل الدخول في الأصول التقنية المعنية.

3-3 حماية كلمات المرور

1-3-3 يجب تشفير جميع كلمات المرور للأصول المعلوماتية والتقنية الخاصة بـجامعة حائل بصيغة غير قابلة للقراءة أثناء إدخالها ونقلها وتخزينها وذلك وفقاً لسياسة التشفير.

2-3-3 يجب إخفاء (Mask) كلمة المرور عند إدخالها على الشاشة.

3-3-3 يجب تعطيل خاصية "تذكّر كلمة المرور" (Remember Password) على الأنظمة والتطبيقات الخاصة بـجامعة حائل.

4-3-3 منع استخدام الكلمات المعروفة (Dictionary) في كلمة المرور كما هي.

5-3-3 يجب تسليم كلمة المرور الخاصة بالمستخدم بطريقة آمنة وموثوقة.

6-3-3 إذا طلب المستخدم إعادة تعيين كلمة المرور عن طريق الهاتف أو الإنترنت أو أي وسيلة أخرى، فلا بد من التحقّق من هوية المستخدم قبل إعادة تعيين كلمة المرور.

7-3-3 يجب حماية كلمات المرور الخاصة بحسابات الخدمة والحسابات ذات الصلاحيات الهامة والحسّاسة وتخزينها بشكل آمن في موقع مناسب (داخل مغلف مختوم في خزنة) أو استخدام التقنيات الخاصة بحفظ وإدارة الصلاحيات الهامة والحسّاسة (Privilege Access Management Solution).

`

4- متطلبات أخرى

4-1 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة هويات الدخول والصلاحيات.

4-2 يحب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات دورياً.

4-3 يجب مراجعة هذه السياسة سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني والإدارة العامة للموارد البشرية وإدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

`

جامعة حائل
University of Ha'il

سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني لضمان حماية الأصول المعلوماتية والتقنية في جامعة حائل من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية بما في ذلك خدمات الإسناد لتقنية المعلومات والخدمات المدارة وفقا للسياسات والإجراءات التنظيمية الخاصة بـجامعة حائل.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-١-٤ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تنطبق هذه السياسة على جميع الخدمات المقدمة من الأطراف الخارجية لـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- البنود العامة

1-1 يجب توثيق واعتماد إجراءات موحدة لإدارة علاقة جامعة حائل مع الأطراف الخارجية قبل وأثناء وبعد انتهاء العلاقة التعاقدية.

2-1 يجب تحديد واختيار الأطراف الخارجية المقدمة للخدمات بعناية ووفقاً للسياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب إجراء تقييم للمخاطر على الأطراف الخارجية والخدمات المقدمة والـتأكد من سلامتها، وذلك بمراجعة مشاريع الأطراف الخارجية داخل جامعة حائل ومراجعة سجلات الأحداث السيبرانية الخاص بخدمة الطرف الخارجي (إن أمكن) قبل وأثناء العلاقة وبشكل دوري.

4-1 يجب إعداد العقود والاتفاقيات مع الأطراف الخارجية بشكل يضمن التزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني لـجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

5-1 يجب مراجعة العقود والاتفاقيات مع الأطراف الخارجية من قبل الإدارة القانونية للتأكد من أن تكون بنود الاتفاقية ملزمة أثناء فترة العقد وبعد انتهاءها وأن مخالفتها يعرض الطرف الخارجي للمساءلة قانونياً.

6-1 يجب أن تشمل العقود والاتفاقيات على بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قِبَل الطرف الخارجي لبيانات جامعة حائل عند انتهاء الخدمة.

7-1 يجب مراجعة متطلبات الأمن السيبراني مع الأطراف الخارجية بشكل دوري.

8-1 يجب مراجعة سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية سنوياً، وتوثيق التغييرات واعتمادها.

2- متطلبات الأمن السيبراني الخاصة بخدمات الإسناد لتقنية المعلومات "Outsourcing" أو الخدمات المدارة "Managed Services" المقدمة من قبل الأطراف الخارجية

2-1 للحصول على خدمات إسناد لتقنية المعلومات أو خدمات مدارة، فإنه يجب اختيار الطرف الخارجي بعناية، ويجب أن يتم التحقق من الآتي:

2-1-1 إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة.

2-1-2 يجب أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة والتي تستخدم طريقة الوصول عن بعد موجودة بالكامل داخل المملكة. (ECC-4-1-3-2)

2-1-3 خدمات الإسناد على الأنظمة الحساسة يجب أن تكون عن طريق شركات وجهات وطنية، وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. (CSCC-4-1-1-2)

3- متطلبات الأمن السيبراني المتعلقة بموظفي الأطراف الخارجية

3-1 يجب أن يتم إجراء المسح الأمني (Screening or Vetting) لشركات خدمات الإسناد، ولموظفي خدمات الإسناد، والخدمات المدارة العاملين على الأنظمة الحساسة. (CSCC-4-1-1-1)

3-2 يجب تضمين مسؤوليات الأمن السيبراني وبنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) في عقود موظفي الأطراف الخارجية (لتشمل خلال وبعد انتهاء/ إنهاء العلاقة الوظيفية مع جامعة حائل).

4- التوثيق وضوابط الوصول

4-1 يجب أن تُطوّر الأطراف الخارجية وتتبع عملية رسمية وموثّقة بعناية لمنح وإلغاء حق الوصول إلى جميع الأنظمة المعلوماتية والتقنية التي تُعالِج أو تنقل أو تخزّن معلومات جامعة حائل بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بـ جامعة حائل.

4-2 يجب توفير إمكانية الوصول إلى معلومات جامعة حائل ومعالجتها بطريقة آمنة ومراقبة.

4-3 يجب تطبيق الضوابط المتعلّقة بكلمات المرور على جميع المستخدمين الذين يملكون حق الوصول إلى معلومات جامعة حائل بما يتماشى مع متطلّبات الأمن السيبراني وأهداف ضوابط الأمن السيبراني الخاصة بـ جامعة حائل.

4-4 يجب تطبيق نظام التحقّق من الهوية متعدّد العناصر على إمكانية الوصول إلى الأنظمة الحسّاسة التي تُعالج المعلومات الخاصة بـ جامعة حائل أو تنقلها أو تُخزّنها.

4-5 يجب إلغاء حقوق الوصول فور انتهاء/إنهاء خدمات أي موظف يعمل لدى الأطراف الخارجية ويملك حق الوصول إلى المعلومات أو الأصول المعلوماتية والتقنية الخاصة بـ جامعة حائل أو في حال تغيير دوره الوظيفي الذي لا يتطلّب استمرارية وصوله إليها.

4-6 يجب أن تقوم الأطراف الخارجية بمراجعة حقوق الوصول بوتيرة دورية وفقًا لسياسات الأمن السيبراني المعتمدة في جامعة حائل.

4-7 يجب تخزين كلّ سجلات التدقيق والحفاظ عليها وتوفيرها بناءً على طلب جامعة حائل.

5- متطلبات الأمن السيبراني المتعلقة بإدارة التغيير

1-5 يجب أن تتبع الأطراف الخارجية عملية إدارة التغيير الرسمية والمناسبة وفقاً لسياسات وإجراءات جامعة حائل وبما يتوافق مع متطلّبات الأمن السيبراني.

2-5 يجب مراجعة واختبار التغيير التي أجريت على الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل قبل تطبيقها على بيئة الإنتاج (Production Environment).

3-5 يجب إبلاغ الأطراف المعنية في جامعة حائل بالتغييرات الرئيسية التي مخطط إجراءها وكذلك التي أجريت على الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل.

6- متطلبات إدارة حوادث الأمن السيبراني واستمرارية الأعمال

1-6 يجب ان تتضمن بنود العقود والاتفاقيات مع الأطراف الخارجية على متطلبات متعلقة بالإبلاغ عن حوادث الأمن السيبراني وإبلاغ جامعة حائل في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني.

2-6 يجب تحديد وتوثيق إجراءات التواصل بين الطرف الخارجي و جامعة حائل في حال تعرض الطرف الخارجي إلى حادثة أمن سيبراني، ومراجعة وتحديث هذه الإجراءات بشكل دوري.

3-6 يجب وضع خطة مناسبة لاستمرارية الأعمال لتفادي عدم توافر الخدمات المقدمة لـجامعة حائل وفقاً لمتطلّبات خطّة استمرارية الأعمال والتعافي من الكوارث الخاصة بـجامعة حائل.

7- متطلبات حماية البيانات والمعلومات

1-7 يجب أن تقوم الأطراف الخارجية بمعالجة بيانات ومعلومات جامعة حائل وتخزينها وإتلافها وفقاً لسياسة ومعيار حماية البيانات والمعلومات المعتمدين في جامعة حائل.

2-7 يجب تطبيق ضوابط تشفير مناسبة لحماية بيانات ومعلومات جامعة حائل وضمان الحفاظ على سريّتها وسلامتها وتوافرها وفقاً لمعيار التشفير المعتمد في جامعة حائل.

3-7 يجب عمل نُسخ احتياطية من بيانات ومعلومات جامعة حائل بشكل دوري ووفقاً لسياسة إدارة النسخ الاحتياطية الخاصة بـجامعة حائل.

4-7 يجب عدم معالجة أو تخزين أو استخدام بيانات ومعلومات جامعة حائل الموجودة في الأنظمة الحسّاسة والبيانات الشخصية (Data privacy)، والتي تُعالجها الأطراف الخارجية - في بيئة الاختبار إلا بعد استخدام ضوابط مشددة لحماية تلك البيانات مثل: تقنيات تعتيم البيانات (Data Masking) أو تقنيات مزج البيانات (Data Scrambling) أو تقنيات إخفاء البيانات (Data Anonymization). (CSCC-2-6-1-1)

5-7 يجب عدم نقل بيانات ومعلومات جامعة حائل الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - خارج بيئة الإنتاج. (CSCC-2-6-1-5)

6-7 يجب تصنيف بيانات ومعلومات جامعة حائل الموجودة في الأنظمة الحسّاسة - والتي تُعالجها الأطراف الخارجية - وفقاً لسياسة تصنيف البيانات والمعلومات المعتمدة في جامعة حائل. (CSCC-2-6-1-2)

8- التدقيق

1-8 يجب أن تُجري جامعة حائل تدقيقًا للعمليات والأنظمة ذات الصلة متى كان ذلك ضرورياً أو مناسباً.

2-8 يجب أن تتعاون جميع مرافق الطرف الخارجي وموظفيه بصورة كاملة مع أنشطة مراجعة سجل الأحداث والتدقيق التي تقوم بها جامعة حائل بما يشمل المراجعات المُنفّذة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **تحديث السياسة ومراجعتها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني وعمادة تقنية المعلومات والتعليم الالكتروني والإدارة العامة للموارد البشرية و الإدارة القانونية و إدارة المشتريات والعقود.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.
2- يجب على جميع الإدارات المعنية بتنفيذ وتطبيق السياسة في جامعة حائل الالتزام بهذه السياسة.
3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة لإجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

نموذج سياسة الأمن السيبراني ضمن استمرارية الأعمال

مقيّد - داخلي

التاريخ:	2023\05\05
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير ضمن إدارة استمرارية الأعمال لضمان استمرارية أعمال جامعة حائل وحمايتها من المخاطر السيبرانية والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على هدف التوافر وهو من الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 3-1-1 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) والضابط رقم 3-1-1 من ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة إدارة استمرارية الأعمال الخاصة بالأمن السيبراني في جامعة حائل وتنطبق على جميع العاملين في جامعة حائل .

بنود السياسة

1- يجب التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني في جامعة حائل .

2- يجب إجراء تقييم للمخاطر التي قد تؤثر على استمرارية أعمال جامعة حائل .

3- يجب معالجة نقاط الضعف لتجنب الحوادث التي قد تؤثر على استمرارية أعمال جامعة حائل .

4- يجب تحديد المتطلبات التشريعية والتنظيمية الخاصة باستمرارية الأعمال لدى جامعة حائل .

5- يجب وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال جامعة حائل .

6- يجب وضع خطط التعافي من الكوارث (Disaster Recovery Plan).

7- يجب إدراج الأنظمة الحساسة لجامعة حائل ضمن خطط التعافي من الكوارث.

8- يجب إنشاء مركز للتعافي من الكوارث للأنظمة الحساسة.

9- يجب إجراء اختبارات دورية للتأكد من فعالية خطط التعافي من الكوارث للأنظمة الحساسة لـجامعة حائل مرة واحدة سنويًا على الأقل.

10- يجب إجراء اختبار دوري حي للتعافي من الكوارث (Live DR Test) للأنظمة الحساسة.

11- يجب تضمين حوادث الأمن السيبراني عالية الخطورة ضمن الأسباب الموجبة لتفعيل خطة استمرارية الأعمال في جامعة حائل .

12- يجب إجراء تحليل التأثير على الأعمال (Business Impact Analysis) لتحديد الأنظمة الحساسة في جامعة حائل ونسخها إلى موقع التعافي من الكوارث.

13- يجب تحديد متطلبات النسخ الدورية الخاصة بالأنظمة الحساسة لـجامعة حائل إلى مركز التعافي.

14- يجب تضمين خطط استمرارية سلاسل التوريد والإمداد ضمن خطط استمرارية أعمال جامعة حائل .

15- يجب تضمين طرق التواصل الخاصة بفريق الأمن السيبراني في جامعة حائل سواءً الداخلية أو الخارجية وتوثيقها.

16- يجب تحديد الأدوار والمسؤوليات للأطراف ذات العلاقة باستمرارية الأعمال في جامعة حائل .

17- يجب وضع خطط تنفيذ ومتابعة المسؤوليات والأعمال الخاصة بالأمن السيبراني خلال الكوارث ولحين عودة الأوضاع لطبيعتها.

18- يجب إدارة هويات الدخول والصلاحيات على جميع الأنظمة والبيانات المستضافة في موقع التعافي من الكوارث الخاص بـجامعة حائل لضمان عدم الوصول إليها من قبل الأشخاص غير المصرح لهم.

19- يجب تضمين متطلبات خطط التعافي من الكوارث في عقود واتفاقيات جامعة حائل مع الأطراف الخارجية ومقدمي الخدمات السحابية.

20- يجب ضمان تطبيق الضوابط الأساسية للأمن السيبراني (ECC-1:2018) في بيئة مركز التعافي من الكوارث التابع لـجامعة حائل مثل: الأمن المادي، أمن الشبكة والبنية التحتية، أمن البيانات والمعلومات، التشفير، إلخ.

21- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني الخاصة باستمرارية أعمال الأمن السيبراني.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني بجامعه حائل

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الإلكتروني و إدارة الأمن السيبراني

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.

2- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يُعرِض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل .

جـامـعـة حـائــل
University of Ha'il

نموذج معيار التشفير

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالتشفير الخاصة بـجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها. كما يجب أن تتوافق مع المعايير الوطنية للتشفير الصادرة من الهيئة الوطنية للأمن السيبراني كمرجع أساسي بأعلى أولوية لمتطلبات الأمن السيبراني الخاصة بالتشفير.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ١-٨-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الأنظمة والتطبيقات وأجهزة معالجة المعلومات الخاصة بـ جامعه حائل وتنطبق على جميع العاملين في جامعه حائل

المعايير

1	استخدام التشفير (Use of Cryptography)
الهدف	ضمان إدارة التشفير واستخدامه بصورة آمنة وملائمة عند الحاجة.
المخاطر المحتملة	يمكن أن يؤدي عدم استخدام التشفير بصورة ملائمة وعند الضرورة إلى مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-1	استخدام شهادات تشفير صحيحة لأمن طبقة النقل (TLS) وذلك لكافة المعلومات المحمية المنقولة أو المستخدمة بين العميل والخادم والخوادم الأخرى. Valid Transport Layer Security (TLS) certificates shall be used for all sensitive information in transit between the client, server and other servers.
2-1	استخدام شهادات تشفير أمن طبقة النقل (TLS) الصادرة عن جهة إصدار شهادات معترف بها لكافة خدمات الإنتاج في جامعه حائل . TLS certificates shall be obtained from a recognized Certificate Authority (CA) for all production services at Hail university.

3-1	إعداد متصفحات الإنترنت لتجنب البروتوكولات غير الآمنة (مثل "SSLv3" أو "SSLv2") وخوارزميات التشفير الضعيفة (مثل "DES" أو "MD5"). Internet browsers shall be configured to avoid insecure and weak protocols (e.g., SSLv3 or SSLv2), and weak ciphers (e.g., DES or MD5).
4-1	استخدام القنوات المشفرة لكافة عمليات المصادقة. Encrypted channels shall be used for all authentication.
5-1	ضمان حماية النسخ الاحتياطية بصورة ملائمة عن طريق الأمن المادي والتشفير عند تخزينها ونقلها عبر الشبكة، ويشمل هذا النسخ الاحتياطية عن بعد والخدمات السحابية. It shall be ensured that backups are properly protected via physical security and encryption when they are stored and moved across the network. Such backups shall include remote backups and cloud services.
6-1	إدارة كافة أجهزة الشبكة باستخدام جلسات مشفرة. All network devices shall be managed using encrypted sessions.
7-1	في حال اكتشاف خطأ في المعلومات المستلمة خلال عملية التشفير، وطلب المتلقي أن تكون المعلومات صحيحة بالكامل (على سبيل المثال، عندما لا يكون المتلقي قادراً على متابعة أعماله عند وجود خطأ في المعلومات)، يجب تنفيذ الآتي: • عدم استخدام المعلومات. • إعادة إرسال المعلومات بناءً على طلب المتلقي (على أن تكون إعادة إرسالها مقتصرة على عدد محدد من المرات). • تخزين المعلومات المتعلقة بالحادثة في سجل التدقيق لتحديد مصدر الخطأ لاحقاً. During a cryptographic process, if an error is detected in the received information, and the receiver requires that the information be entirely correct (e.g., the receiver cannot proceed when the information is in error), then the following shall be performed: • The information shall not be used. • The recipient may request that the information be resent (retransmissions shall be limited to a predetermined maximum number of times).

	• Information related to the incident shall be stored in an audit log to later identify the source of the error.
2	إدارة مفاتيح التشفير (Cryptographic Key Management)
الهدف	ضمان إدارة مفاتيح التشفير بصورة آمنة خلال دورة إدارة مفاتيح التشفير الكاملة.
المخاطر المحتملة	تنطوي إدارة مفاتيح التشفير غير الآمنة على مخاطر شديدة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-2	يجب إدارة مفاتيح التشفير وفقاً لعمليات إدارة مفاتيح التشفير المعتمدة في جامعة حائل وإجراءاتها وإرشاداتها، ويشمل ذلك إصدار المفاتيح وتخزينها ونسخها احتياطياً واستعادتها وغيرها من العمليات. Cryptographic keys shall be managed in accordance with Hail university's cryptographic key management processes, procedures, and guidelines. This shall include key generation, key storage, key backup, key recovery, etc.
2-2	يجب تحديد فئات مفاتيح التشفير وفقاً لتصنيفها (عامة، أو خاصة، أو متماثلة) واستخدامها. Cryptographic keys shall be categorized according to their classification (public, private, or symmetric) and use.
3-2	يجب حماية مفاتيح التشفير وفقاً لنوعها. Cryptographic keys shall be protected according to their type and the required protection.
4-2	يجب حماية الخصائص المشتركة لمفاتيح التشفير وفقاً لنوعها. Associations for the cryptographic keys shall be protected according to their type.
5-2	يجب الحصول على ضمان بشأن صلاحية المفاتيح العامة للتأكد من أن مفاتيح التشفير صحيحة حسابياً، وذلك من خلال إحدى الطرق التالية: • الحصول على ضمان من الجهة المسؤولة عن المفتاح أو الجهة المسؤولة عن التحقق من المفتاح أو طرف خارجي موثوق. • التحقق المباشر من المفاتيح العامة اعتماداً على الخوارزميات المستخدمة.

An assurance of public-key validity shall be obtained to ensure that the cryptographic key is arithmetically correct, through one of the following methods: • Assurance from the key owner, key verifier, or trusted third party. • Explicit public key validation depending on the algorithm used.	
يجب استخدام خوارزميات توفر ضماناً بشأن ملكية المفتاح العام أو الحصول على هذا الضمان مباشرة للتأكد من أن الجهة الخارجية (أي الطرف الخارجي) التي توفر المفتاح العام تملك فعلياً المفتاح الخاص المصاحب للمفتاح العام. Algorithms that provide an assurance of private-key possession shall be used. Alternatively, such assurance shall be obtained explicitly to ensure that the external entity (i.e., third party) providing a public key actually possesses the associated private key.	6-2
يجب توفير الحماية الأمنية الواردة في الضابط 2-2 لفترة زمنية معينة وفقاً لنوع مفتاح التشفير. The security protections highlighted in control 2-2 shall be provided for a period of time as per the cryptographic key type.	7-2
يجب تعيين مدة تشفير لمفاتيح التشفير. Cryptoperiods shall be assigned to the cryptographic keys.	8-2
يجب إتلاف كافة المفاتيح المتماثلة والمفاتيح الخاصة في نهاية فترة حمايتها كما هو مبين في الضابط 2-6. All symmetric keys and all private keys shall be destroyed at the end of their period of protection as highlighted in control 2-6.	9-2
يجب استخدام أطوال مفاتيح التشفير التي لا تقل عن 128 بت في جميع خوارزميات المفاتيح المتماثلة. Cryptographic key lengths that are at least 128 bits shall be used in all symmetric key algorithms.	10-2
يجب استخدام مفاتيح نظام التشفير غير المتماثلة ذات الطول الكافي لكي تكون بنفس درجة قوة أطوال المفاتيح المتماثلة.	11-2

	Asymmetric cryptosystem keys that are of sufficient length shall be used to yield equivalent strength to symmetric key lengths.
12-2	بالنسبة للأنظمة الحساسة، من المستحسن استخدام أطوال مفاتيح تشفير متماثلة لا تقل عن 256 بت، وأطوال مفاتيح تشفير غير متماثلة (Elliptic Curve Cryptography ECC) لا تقل عن 512 بت. For critical systems, it is recommended to employ symmetric cryptographic key lengths that are at least 256 bits, and asymmetric Elliptic Curve Cryptography ECC key lengths that are at least 512 bits.
3	تشفير البيانات والمعلومات (Data and Information Encryption)
الهدف	ضمان تشفير البيانات والمعلومات عند الضرورة.
المخاطر المحتملة	تنطوي البيانات والمعلومات غير المشفرة على مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-3	يجب استخدام برنامج تشفير القرص الكامل المعتمد لتشفير القرص الصلب في كافة الأجهزة المحمولة. Approved whole disk encryption software shall be used to encrypt the hard drive of all mobile devices.
2-3	يجب فك تشفير كافة أنواع حركة بيانات الشبكة المشفرة عند الخادم الوكيل على حدود الشبكة قبل تحليل المحتوى. ويمكن لـجامعة حائل استخدام قائمة محددة من التطبيقات لمواقع مسموحة يمكن الوصول إليها عبر خادم وكيل دون فك تشفير حركة البيانات. All encrypted network traffic shall be decrypted at the boundary proxy prior to analyzing the content. However, Hail university may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
3-3	يجب على كافة عمليات الوصول وتسجيل الدخول عن بعد إلى شبكة جامعة حائل تشفير البيانات قيد الاستخدام والنقل، واستخدام التحقّق من الهوية متعدّد العناصر. All remote login access to Hail university's network shall be required to encrypt data in transit and use multi-factor authentication.

4-3	يجب مراقبة كافة أنواع الحركة التي تخرج من جامعة حائل وكشف أي استخدام غير مصرح به للتشفير. All traffic leaving Hail university shall be monitored, and any unauthorized use of encryption shall be detected.
5-3	إذا كانت أجهزة التخزين (USB) مطلوبة، يجب تشفير البيانات المخزنة بناءً على تصنيفها على هذه الأجهزة. If USB storage devices are required, data stored on such devices shall be encrypted while at rest, based on the data classification.
6-3	يجب تشفير جميع المعلومات المحمية أثناء الاستخدام والنقل. All protected information in transit shall be encrypted.
7-3	يجب تشفير جميع المعلومات المحمية أثناء التخزين باستخدام أداة تتطلب آلية تحقق ثانوية غير مدمجة في نظام التشغيل من أجل الوصول إلى المعلومات. All protected information at rest shall be encrypted using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.
8-3	يجب تشفير جميع البيانات اللاسلكية أثناء الاستخدام والنقل. All wireless data in transit shall be encrypted.
9-3	يجب تشفير أو اختزال كافة بيانات الاعتماد باستخدام بيانات عشوائية عند تخزينها. All authentication credentials shall be encrypted or hashed with a salt when stored.
10-3	يجب ضمان أن جميع أسماء المستخدمين وبيانات التحقق الخاصة بالحسابات تُنقل عبر الشبكات باستخدام قنوات مشفرة. It shall be ensured that all account usernames and authentication credentials are transmitted across networks using encrypted channels.
4	المعلومات الأخرى ذات العلاقة بالتشفير (Other Cryptographic Related Information)
الهدف	ضمان إدارة البيانات والمعلومات المستخدمة مع مفاتيح التشفير بصورة آمنة.

المخاطر المحتملة	قد تؤدي الإدارة غير الآمنة للبيانات والمعلومات المستخدمة مع مفاتيح التشفير إلى مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-4	يجب حماية كافة المعلومات المستخدمة مع خوارزميات التشفير ومفاتيح التشفير. All information used in conjunction with cryptographic algorithms and cryptographic keys shall be protected.
2-4	يجب حماية الخصائص المشتركة لمعلومات التشفير وفقاً لنوعها. Associations for cryptographic information shall be protected according to their type.
3-4	يجب الحصول على ضمان بشأن صلاحية "معيار النطاق" لكافة خوارزميات المفاتيح العامة الخاصة بالدخول المنفصل لضمان صحة معايير النطاق حسابياً. وذلك من خلال إحدى الطرق التالية: • الحصول على ضمان من الجهة المسؤولة عن المفتاح أو الجهة المسؤولة عن التحقق من المفتاح أو طرف خارجي موثوق. • التحقق من المفاتيح العامة اعتماداً على الخوارزميات المستخدمة. An assurance of domain parameter validity shall be obtained for all discrete log public key algorithms to ensure that the domain parameters are arithmetically correct, using one of the following methods: • Assurance from the key owner, key verifier, or trusted third party • Explicit validation depending on the algorithm used
4-4	يجب توفير الحماية الأمنية الواردة في الضابط 2-2 لفترة زمنية معينة وفقاً لنوع معلومات التشفير. The security protections highlighted in control 2-2 shall be provided for a period of time.

5-4	يجب إدراج آليات لا تعتمد على التشفير في أنظمة الاتصالات لضمان توافر المعلومات المشفرة المنقولة بعد استلامها بنجاح، بدلاً من الاعتماد على إعادة إرسالها من قبل المرسل الأصلي لغايات توافرها مستقبلاً. Non-cryptographic mechanisms shall be incorporated in communication systems to ensure the availability of transmitted cryptographic information after it has been successfully received, rather than relying on retransmission by the original sender for future availability.
5	بروتوكولات التشفير وخوارزميات التشفير المدعومة (Encryption Protocols and Cipher Suites)
الهدف	ضمان استخدام خوارزميات التشفير المعتمدة والآمنة عند التشفير.
المخاطر المحتملة	ينطوي استخدام خوارزميات التشفير غير الآمنة أو غير المعتمدة على مخاطر كبيرة قد تتسبب بسرقة المعلومات أو الكشف عنها أو الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-5	يجب استخدام خوارزميات دوال الاختزال المشفرة فقط بحيث لا يكون من الممكن العثور على نص له نتيجة اختزال معينة (مقاومة عكس الخوارزمية)، أو العثور على نصين لهما نفس نتيجة الاختزال (مقاومة التصادم). Only cryptographic hash functions shall be used to ensure that it is not feasible to find a message that produces a given hash value (Pre-image Resistance), or find two messages that produce the same hash value (Collision Resistance).
2-5	يجب استخدام خوارزميات دوال اختزال مشفرة وفقاً لمعايير الخوارزميات ذات العلاقة. Cryptographic hash functions shall be used as directed by the relevant algorithm standards.
3-5	يجب استخدام أطوال مفاتيح التشفير التي لا تقل عن 128 بت في جميع خوارزميات المفاتيح المتماثلة. Cryptographic key lengths that are at least 128 bits shall be used in all symmetric key algorithms.
4-5	يجب استخدام شفرة التحقق من الرسائل (MAC) لضمان سلامة البيانات والتأكد من قيام الجهة المتوقعة بحساب شفرة التحقق من الرسائل (MAC).

Message Authentication Codes (MACs) shall be used to provide assurance of the data's integrity, and that the MAC was computed by the expected entity.	
يجب استخدام خوارزميات شفرة التحقق من الرسائل (MAC) بناءً على خوارزميات التشفير الكتلي (Block Cipher)، (مثل شفرة التحقق من الرسائل باستخدام التشفير "CMAC" أو شفرة غاليوس للتحقق من الرسائل "GMAC")، أو بناءً على خوارزميات حساب ملخص النص المميز (شفرة التحقق من الرسائل المجزأة "HMAC"). Only MAC algorithms shall be used based on block cipher algorithms (CMAC or GMAC) or based on hash functions (HMAC).	5-5
يجب عدم استخدام نفس المفتاح لغايات التشفير واحتساب شفرة التحقق من الرسائل (MAC) في حال استخدام نفس خوارزمية التشفير الكتلي (Block Cipher). The same key shall not be used if the same block cipher algorithm is used for both encryption and MAC computation.	6-5
يجب استخدام خوارزميات التواقيع الرقمية المعتمدة لتوفير التحقق الآمن والتحقق من سلامة المعلومات ودعم عدم إنكار صحة البيانات. Approved digital signature algorithms shall be used to provide source authentication, integrity authentication, and support for non-repudiation.	7-5
يجب استخدام خوارزميات التواقيع الرقمية التالية مع أطوال المفاتيح المعتمدة لكل من: • خوارزمية التوقيع الرقمي (خوارزمية "DSA"). • خوارزمية ريفست وشامير وإديلمان (خوارزمية "RSA"). • خوارزمية التوقيع الرقمي للمنحنى الإهليلجي (خوارزمية "ECDSA"). Only the following digital signature algorithms shall be used with the approved key sizes for each of the following: • Digital Signature Algorithm (DSA) • RSA Algorithm • ECDSA Algorithm	8-5
يجب إصدار التواقيع الرقمية باستخدام مفاتيح تلبي أو تتجاوز أطوال المفاتيح المعتمدة للخوارزمية. Digital signatures shall be generated using keys that meet or exceed the approved key sizes of the algorithm.	9-5

10-5	يجب استخدام طرق تبادل المفاتيح المعتمدة التالية لإعداد المفاتيح بين الجهات التي تقوم بالاتصالات: • نقل المفاتيح: يجب نقل مواد صياغة المفاتيح من جهة إلى أخرى باستخدام خوارزمية متماثلة (أي باستخدام مفاتيح تشفير المفاتيح) أو باستخدام خوارزمية غير متماثلة. • الاتفاق على المفاتيح: يجب أن تتعاون الجهات في إنشاء مواد صياغة المفاتيح المشتركة باستخدام خوارزميات متماثلة أو غير متماثلة. Only the following approved key-exchange scheme types shall be used to set up keys between communicating entities: • Key Transport: The keying material shall be transported from one entity to another using a symmetric algorithm (i.e., using a key-wrapping key), or using an asymmetric algorithm. • Key Agreement: Entities shall co-create shared keying material using symmetric or asymmetric algorithms.
11-5	يجب استخدام طرق تبادل المفاتيح المعتمدة باستخدام أطوال المفاتيح المعتمدة. وتشمل هذه الطرق خوارزمية ديفي- هيلمان (خوارزمية "DH") وخوارزمية "RSA". Approved key-exchange schemes with approved key sizes shall be used. These schemes include Diffie-Hellman (DH) and RSA algorithms.
12-5	يجب استخدام درجة قوة لا تقل عن 256 بت لخوارزميات التشفير المستخدمة للأنظمة الحساسة حسب ما تصدره الهيئة الوطنية للأمن السيبراني في هذا الخصوص. Security strengths of at least 256 bits shall be employed for cryptographic algorithms used for critical systems following what the NCA issues in this regards.
13-5	يجب استخدام درجات قوة لا تقل عن 256 بت لخوارزميات حساب ملخص النص المميز المستخدمة للأنظمة الحساسة. Security strengths of at least 256 bits shall be employed for hash functions used for critical systems.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني.

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الإلكتروني

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذا المعيار باستمرار.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعه حائل .

جامعة حائل
University of Ha'il

نموذج سياسة الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية الأصول المعلوماتية والتقنية الخاصة بجامعة حائل على خدمات الحوسبة السحابية والاستضافة (Cloud Computing Services and Hosting). وذلك، لضمان معالجة المخاطر السيبرانية أو تقليلها من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٢-٤ من الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية، وتنطبق هذه السياسة على جميع العاملين في جامعه حائل

بنود السياسة

1- البنود العامة

1-1 تُطبَق جميع متطلبات الأمن السيبراني الخاصة بالأطراف الخارجية في سياسة الأمن السيبراني المتعلّق بالأطراف الخارجية على جميع مقدمي خدمات الحوسبة السحابية والاستضافة.

2-1 يجب على إدارة الأمن السيبراني التحقق من كفاءة وموثوقية مقدم خدمات الحوسبة السحابية والاستضافة بالإضافة إلى حصوله على ترخيص ووجود سجل رسمي له داخل المملكة العربية السعودية.

3-1 يجب تطبيق متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة وفقاً للسياسات والإجراءات التنظيمية الخاصة بجامعة حائل والمتطلبات التشريعية والتنظيمية ذات العلاقة.

4-1 يجب على جامعة حائل إجراء تقييم لمخاطر الأمن السيبراني المترتبة على استضافة التطبيقات أو الخدمات في الحوسبة السحابية قبل اختيار مقدم خدمات الحوسبة السحابية والاستضافة.

5-1 يجب أن يكون موقع استضافة الأنظمة الحساسة، أو أي جزء من مكوناتها التقنية، داخل جامعه حائل أو في خدمات الحوسبة السحابية المقدمة من قبل جهة حكومية، أو شركة وطنية محققة لضوابط الهيئة الوطنية للأمن السيبراني المتعلقة بخدمات الحوسبة السحابية والاستضافة، مع مراعاة تصنيف البيانات المستضافة. (CSCC-4-2-1-1)

6-1 يجب على إدارة الأمن السيبراني تطوير وتوثيق واعتماد إجراءات خاصة باستخدام الخدمات السحابية.

7-1 يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة بحد أدنى ما يلي:

1-7-1 متطلبات الأمن السيبراني وبنود اتفاقية مستوى الخدمة (Service Level Agreement "SLA").

2-7-1 بنود المحافظة على سرية المعلومات (Non-disclosure Clauses) بما في ذلك حذف البيانات وإتلافها بالاتفاق بين مقدم الخدمة وجامعة حائل بناء على تصنيف تلك البيانات ومع مراعاة سياسة تصنيف البيانات.

3-7-1 متطلبات استمرارية الأعمال والتعافي من الكوارث.

4-7-1 يجب أن تتضمن عقود مقدمي خدمات الحوسبة السحابية والاستضافة إمكانية جامعة حائل إنهاء الخدمة دون مبرر أو اشتراطات .

8-1 يجب مراجعة تطبيق متطلبات الأمن السيبراني مع مقدمي خدمات الحوسبة السحابية والاستضافة دورياً، مرة واحدة في السنة، على الأقل.

2- متطلبات الأمن السيبراني المتعلقة باستضافة/تخزين البيانات

1-2 يجب تصنيف البيانات قبل استضافتها/تخزينها لدى مقدمي خدمات الحوسبة السحابية والاستضافة. (ECC-4-2-3-1)

2-2 يجب على مقدمي خدمات الحوسبة السحابية والاستضافة إعادة البيانات (بصيغة قابلة للاستخدام) وحذفها بشكل غير قابل للاسترجاع عند إنهاء/انتهاء الخدمة. (ECC-4-2-3-1)

3-2 يجب أن يكون موقع واستضافة وتخزين معلومات جامعة حائل داخل المملكة العربية السعودية (ECC-4-2-3-3) مع مراعاة التنظيمات والجوانب التشريعية بعدم خضوع تلك البيانات لأي قوانين دول أخرى.

4-2 يجب على إدارة الأمن السيبراني التأكد من فصل البيئة الخاصة بجامعة حائل(ويشمل ذلك الخوادم الافتراضية، والشبكات وقواعد البيانات) عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية. (ECC-4-2-3-2)

5-2 يجب الحصول على موافقة إدارة الأمن السيبراني لاستضافة الأنظمة الحساسة أو أي جزء من مكوناتها التقنية.

6-2 يجب على جامعة حائل التأكد من تطبيق متطلبات خصوصية البيانات على البيانات المستضافة في الحوسبة السحابية.

7-2 يجب تشفير البيانات والمعلومات المنقولة إلى الخدمات السحابية، أو المخزنة فيها، أو المنقولة منها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة في جامعه حائل

8-2 يجب على جامعة حائل التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة يقوم بعمل النسخ الاحتياطي دورياً وحماية النسخ الاحتياطية وفقاً لسياسة النسخ الاحتياطية المعتمدة في جامعه حائل

9-2 يجب على جامعة حائل التأكد من أن مقدم خدمات الحوسبة السحابية والاستضافة لا يمكنه الاطلاع على البيانات المخزنة وأن صلاحية الوصول الخاصة بمقدم الخدمة محدودة بالصلاحيات اللازمة للقيام بأنشطة إدارة خدمة الاستضافة وصيانتها، أو حسب متطلبات الأعمال.

2-10 يجب على مقدم خدمات الحوسبة السحابية والاستضافة تقييد الدخول إلى الخدمات السحابية الخاصة بجامعة حائل على المستخدمين المصرح لهم فقط وباستخدام وسائل التحقق من هوية المستخدم وفقاً لسياسة إدارة هويات الدخول والصلاحيات المعتمدة في جامعه حائل

2-11 يجب على مقدم خدمات الحوسبة السحابية والاستضافة توفير التقنيات والأدوات اللازمة لجامعة حائل لإدارة ومراقبة خدماتها السحابية.

2-12 يجب على إدارة الأمن السيبراني وإدارة الشؤون القانونية تضمين بنود متطلبات الأمن السيبراني المتعلقة باستضافة البيانات في العقد مع مقدم خدمة الحوسبة السحابية.

3- متطلبات أخرى

3-1 يجب على جامعة حائل التأكد من تفعيل سجلات الأحداث على الأصول المعلوماتية المستضافة.

3-2 يجب على جامعة حائل مراقبة سجلات الأحداث الخاصة بالأمن السيبراني دورياً.

3-3 يجب على جامعة حائل التأكد من مزامنة التوقيت (Clock Synchronization) الخاص بالبنية التحتية للخدمة السحابية مع التوقيت الخاص بـجامعه حائل

3-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية الأصول المعلوماتية والتقنية على خدمات الحوسبة السحابية.

3-5 يجب مراجعة متطلبات الأمن السيبراني الخاصة بخدمات الحوسبة السحابية والاستضافة دورياً.

3-6 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الامن السيبراني

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني

3- **تنفيذ وتطبيق السياسة:** عمادة تقنية المعلومات والتعليم الإلكتروني و إدارة الأمن السيبراني

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعه حائل

جامعة حائل
University of Ha'il

نموذج معيار أمن الشبكات اللاسلكية

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية أمن الشبكات اللاسلكية الخاصة بجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية، وهي: سرية المعلومات، وسلامتها، وتوافرها.

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أنظمة الشبكات التقنية اللاسلكية الخاصة بجامعة حائل وينطبق على جميع العاملين في جامعة حائل

المعايير

1	الوصول الآمن (Secure Access)
الهدف	ضمان تطبيق الإعدادات الصحيحة للوصول إلى واجهات إدارة أمن الشبكات اللاسلكية من أجل حمايتها بشكل فعال من الهجمات السيبرانية.
المخاطر المحتملة	تؤدي الإعدادات غير الكافية لحلول واجهات إدارة أمن الشبكات اللاسلكية إلى تعرضها داخل بيئة جامعة حائل إلى هجمات أو انتهاكات أمنية.
الإجراءات المطلوبة	
1-1	إعداد قوائم الوصول بصورة تسمح بالتحكم بالوصول إلى أجهزة اتصالات الشبكة اللاسلكية بحيث يمكن للأشخاص المصرح لهم فقط الوصول إلى هذه الأجهزة. Access lists shall be configured to control access to wireless network communication devices and ensure that these devices are accessible to authorized users only.
2-1	استخدام آلية تحقق مركزية للتحقق من جميع المستخدمين التفاعليين الذين يقومون بعمل تغييرات على كافة أجهزة الشبكة اللاسلكية. كما يجب أن تكون أنظمة التحقق بأقل عدد ممكن. Centralized user-level authentication shall be deployed to authenticate all interactive users making changes to all

wireless network devices. Additionally, authentication systems shall be as few as possible.	
أن يقتصر وصول مشرفي إدارة مكونات الشبكة اللاسلكية عبر استخدام أجهزة حاسب مخصصة ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs) أو خوادم الوصول إلى المناطق الآمنة (Jump Servers) الموجودة على واجهات إدارة مستقلة على شبكة مفصولة عن شبكة جامعة حائل ومعزولة عن الإنترنت، ومنع وصولهم لاسلكياً. Restrict wireless network administrators' access to use dedicated Privileged Access Workstations (PAWs) or jump servers placed in an out-of-band management network, segmented from Hail university's network and isolated from the internet, and not wirelessly.	3-1
تطبيق التحقّق من هوية الوصول متعدّد العناصر لمشرفي الأنظمة اللاسلكية، واستخدام الجلسات المشفرة لإدارة وإعداد مكونات أجهزة الشبكات اللاسلكية. Multi-Factor Authentication shall be implemented and encrypted sessions shall be used to manage (or administrate) all wireless network devices by administrators.	4-1
تقييد استخدام كلمة المرور الاساسية بتعليمات وإجراءات معتمدة، وحصره على مشرفين محددين فقط بحسب ما هو ضروري لغايات غير تشغيلية، أو لغرض استعادة أجهزة الشبكة اللاسلكية التي تم فصلها عن الشبكة. The use of hard-coded passwords shall be limited to relevant administrators only as necessary for non-interactive purposes, as well as to recover wireless network devices that have become disconnected from the network.	5-1
إعداد أجهزة الشبكة اللاسلكية لعرض رسالة نصية تنبيهية عند تسجيل الدخول. ويجب ألا تُظهر هذه الرسالة النصية الخصائص الأساسية للشبكة. Wireless network devices shall be configured to display an alert banner at login. This banner text shall not provide the underlying characteristics of the network.	6-1
فصل الشبكة اللاسلكية (Wireless Network Segregation)	2
ضمان حماية تصميم وبنية الشبكة اللاسلكية وحماية الأجزاء الشبكية وفقاً لمستوى الأمن الخاص بها.	الهدف

المخاطر المحتملة	تتشارك الشبكات اللاسلكية غير المفصولة في نفس نطاق البث وتكون الأجهزة قادرة على التواصل دون مراقبة أو ضبط حركة البيانات، وبالتالي يمكن أن يؤدي أي هجوم على النظام إلى تهديدات داخلية خطيرة وهجمات على معظم أنظمة الشبكة، مما يسهل حركة البيانات الجانبية ضمن الشبكة.
الإجراءات المطلوبة	
1-2	تصميم وتطبيق شبكة لاسلكية معزولة منطقياً و/أو مادياً مع الأخذ بعين الاعتبار احتياجات الأعمال والمعمارية المؤسسية وذلك بالاستناد إلى الدفاع الأمني متعدد المراحل والمعمارية متعددة المستويات. A logically and/or physically segmented wireless network shall be designed and implemented, taking into consideration business needs and enterprise architecture, and based on the principles of defense-in-depth and multi-tier architecture.
2-2	تطبيق المستوى الملائم من ضوابط الأمن السيبراني على الأجزاء الشبكية المختلفة بناءً على قيمة وتصنيف المعلومات المعالجة في الشبكة اللاسلكية ومستويات الموثوقية والتأثير على الأعمال والمخاطر المرافقة. Appropriate level of security controls shall be applied to different network segments based on the value and classification of information processed in the wireless network, levels of trust, business impact and associated risks.
3-2	تصميم وإعداد الشبكات اللاسلكية لتصفية مرور البيانات بين مختلف الأجزاء وحجب الوصول غير المصرح به. Wireless networks shall be designed and configured to filter traffic between different segments and block any unauthorized access.
4-2	إعداد جدران الحماية والموجّهات (Routers) لمنع أي اتصالات غير مصرح بها بين الشبكات اللاسلكية غير الموثوقة Firewalls and routers shall be configured to prevent any unauthorized connections between untrusted wireless networks
5-2	منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية.

	Critical systems shall be prevented from connecting to the wireless network.
6-2	مراجعة الإعدادات والقواعد والسياسات والملفات التعريفية الأمنية لجدران الحماية والموجهات (Routers) بشكل دوري. Security configurations, rules, policies and profiles for firewalls and routers shall be reviewed in regular bases.
3	تأمين الحدود (Boundary Defense)
الهدف	حماية حدود الشبكة اللاسلكية من التهديدات.
المخاطر المحتملة	في حال تم ترك حدود الشبكة اللاسلكية من دون الحماية التي توفرها الضوابط الأمنية المناسبة، سيتمكن المهاجمون من اختراق الشبكة اللاسلكية بسهولة وفرض المزيد من التهديدات الخطيرة.
الإجراءات المطلوبة	
1-3	الاحتفاظ بقائمة جرد محدثة لكافة حدود الشبكة اللاسلكية في جامعة حائل An up-to-date inventory of all of Hail university's wireless network boundaries shall be maintained.
2-3	حظر الاتصالات مع عناوين بروتوكولات الإنترنت الضارة أو غير المستخدمة وحصر الوصول بمجالات عنوان بروتوكولات الإنترنت الموثوقة والضرورية عند كل حد من حدود الشبكة اللاسلكية لجامعة حائل Communications with known malicious or unused Internet IP addresses shall be denied, and access shall be limited to trusted and necessary IP address ranges at each of Hail university's wireless network boundaries.
3-3	حظر الاتصالات عبر منافذ بروتوكول التحكم بالنقل (TCP) أو بروتوكول حزم بيانات المستخدم (UDP) أو حركة التطبيقات لضمان السماح فقط للبروتوكولات المصرح لها بالدخول أو الخروج من الشبكة اللاسلكية عند كل حد من حدود الشبكة اللاسلكية جامعة حائل Communication over unauthorized TCP or UDP ports or application traffic shall be denied to ensure that only authorized protocols are allowed to cross the network boundary in or out of the wireless network at each of Hail university's network boundaries.

4-3	إعداد أنظمة المراقبة لتسجيل حزم بيانات الشبكة التي تمر عبر الحدود عند كل حد من حدود الشبكة اللاسلكية لـ جامعة حائل Monitoring systems shall be configured to record network packets passing through the boundary at each of Hail university's wireless network boundaries.
5-3	تفعيل أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات على حدود الشبكة اللاسلكية لكشف أي حركة بيانات خبيثة على الشبكة عند كل حد من حدود شبكة جامعة حائل Network-based Intrusion Prevention Systems (IPS) shall be deployed to block malicious network traffic at each of Hail university's wireless network boundaries.
6-3	تثبيت تقنيات كشف/منع التهديدات المتقدمة المستمرة (APT) على الشبكة لكشف أو حجب الهجمات على الشبكة والهجمات غير المعروفة مسبقاً عند كل حد من حدود شبكة جامعة حائل Network-based Advanced Persistent Threat (APT) detection/prevention systems shall be deployed to detect or block malicious network attacks and zero-day attacks at each of Hail university's network boundaries.
7-3	تمكين جمع معلومات حركة البيانات عبر الشبكة (NetFlow) وتسجيل البيانات على كافة أجهزة حدود الشبكة اللاسلكية. The collection of NetFlow and logging data shall be enabled on all wireless network boundary devices.
8-3	ضمان أن كافة أشكال حركة البيانات عبر الشبكة اللاسلكية من أو إلى الإنترنت تمر عبر خادم وكيل طبقة التطبيقات المعتمدة والمجهز لتصفية الاتصالات غير المصرح بها. All wireless network traffic to/from the Internet shall pass through an authenticated application layer proxy that is configured to filter unauthorized connections.
9-3	تمكين تسجيل الاستفسارات على نظام أسماء النطاقات لكشف وتحديد اسم المستضيف للنطاقات الخبيثة المعروفة. Domain Name System (DNS) query logging shall be enabled to detect hostname lookups for known malicious domains.

10-3	ضمان التحديث المنتظم لكافة خدمات الاشتراك وفئات العناوين (URL) ومصادر المعلومات الاستباقية والقوائم المحددة من التطبيقات الممنوعة (Blacklists) والإشارات المعرفة المسبقة. All subscription services, URL categories, threat feeds, blacklists, and signatures shall be up-to-date and updated regularly.
5	الارتباط اللاسلكي (Wireless Access)
الهدف	ضبط استخدام الشبكات اللاسلكية وحمايتها.
المخاطر المحتملة	في حال تم ترك الشبكات اللاسلكية من دون حماية، ستتعرض جامعة حائل لمخاطر الاتصال غير المصرح به بالشبكة أو كشف البيانات.
الإجراءات المطلوبة	
1-5	إجراء تقييم مخاطر شامل لتقييم مخاطر اتصال الشبكات اللاسلكية بالشبكة الداخلية. A comprehensive risk assessment exercise shall be conducted to evaluate the risks of connecting wireless networks to the internal network.
2-5	الاحتفاظ بقائمة جرد بنقاط الوصول اللاسلكية المصرح بها والمتصلة بالشبكة السلكية. An inventory of authorized wireless access points connected to the wired network shall be maintained.
3-5	إعداد أدوات مسح الثغرات الأمنية في الشبكة لكشف أو منع أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده. Network vulnerability scanning tools shall be configured to detect and alert on unauthorized wireless access points connected to the wired network.
4-5	استخدام نظام كشف التسلل اللاسلكي (WIDS) لكشف أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده. Wireless Intrusion Detection System (WIDS) shall be used to detect/prevent and alert on unauthorized wireless access points connected to the wired network.
5-5	إلغاء تفعيل الوصول اللاسلكي على الأجهزة التي لا تقتضي طبيعة عملها ذلك.

Wireless access on devices that do not have a business purpose for wireless access shall be disabled.	
إعداد الوصول اللاسلكي على أجهزة المتصلين التي لا تحتاج لذلك لغايات العمل بحيث يتم السماح بالوصول إلى الشبكات اللاسلكية المصرح بها فقط وتقييد الوصول إلى الشبكات اللاسلكية الأخرى. Wireless access on client machines that do not have a business need for wireless access shall be configured to allow access to authorized wireless networks only, and to restrict access to other wireless networks.	6-5
إلغاء تفعيل قدرات الشبكة اللاسلكية (المخصصة) لمشاركة الملفات بين الأجهزة مباشرة على الشبكات اللاسلكية لدى المتصلين. Peer-to-peer (ad hoc) wireless network capabilities shall be disabled on wireless clients.	7-5
إعداد نقاط الوصول اللاسلكية والأجهزة اللاسلكية للاتصال بالشبكة اللاسلكية باستخدام بروتوكولات آمنه مثل (WPA2) أو (WPA3). Wireless access points and wireless devices shall be configured to connect to the wireless network using secure protocol such as WPA2 or WPA3.	8-5
ضمان استخدام الشبكات اللاسلكية لبروتوكولات التحقق مثل بروتوكول المصادقة القابل للامتداد-أمن طبقة النقل (EAP/TLS) الذي يقتضي استخدام التحقّق من الهوية متعدّد العناصر بشكل متبادل. Wireless networks shall use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual Multi-Factor Authentication.	9-5
إلغاء تفعيل الوصول اللاسلكي للأجهزة الطرفية الموجودة على الأجهزة (مثل تقنية بلوتوث "Bluetooth" والاتصال قريب المدى "NFC") ما لم تقتضي طبيعة العمل ذلك. Wireless access of peripheral devices (such as Bluetooth and NFC) shall be disabled unless such access is required for a business purpose.	10-5

11-5	إيجاد شبكات لاسلكية منفصلة للأجهزة الشخصية أو غير الموثوقة، والتعامل مع هذه الشبكات بحذر واعتبارها مصادراً غير موثوقة مما يستدعي مراقبتها وتصفيتها بشكل مستمر. A separate wireless network shall be created for personal or untrusted devices. Enterprise access from this network shall be treated as untrusted and shall be filtered and audited accordingly.
7	الأمن المادي (Physical Security)
الهدف	ضمان حماية جميع أجهزة الشبكة اللاسلكية المطلوبة لاتصالات الشبكة من العبث أو التعديل أو أي هجمات مادية أخرى.
المخاطر المحتملة	يمكن أن يؤدي الهجوم المادي على أجهزة الشبكة اللاسلكية التي تحفظ عمليات الاتصالات إلى الإضرار بالأصول المعلوماتية والتقنية الخاصة بجامعة حائل وبالتالي التأثير على سير أعمالها المعتاد. في حال تلف الجهاز أو العبث به أو تعديله مادياً، لا يمكن لجامعة حائل الوثوق بالمعلومات المرسلة عبره وسيرتفع مستوى المخاطر التي قد تهدد أمن الشبكة.
الإجراءات المطلوبة	
1-7	تطبيق ضوابط الوصول المادي على كافة أجهزة الشبكة اللاسلكية All network devices that are required for network communications shall be placed in a secured area with physical access controls implemented.
8	التسجيل والمراقبة (Logging and Monitoring)
الهدف	ضمان مراقبة وتخزين كافة الأحداث الحساسة المتعلقة بأمن الشبكة اللاسلكية من أجل الاكتشاف الاستباقية للهجمات السيبرانية وإدارة المخاطر بفعالية لمنع أو تقليل الآثار المترتبة على أعمال جامعة حائل
المخاطر المحتملة	لضمان سلامة الشبكة اللاسلكية، يجب مراقبة كافة أجهزة الشبكة بشكل منتظم وضمان إمكانية الوصول إليها من قبل فرق الأمن السيبراني في جامعة حائل دون القدرة على مراقبة وتسجيل الأحداث في الشبكة، لن تتمكن جامعة حائل من التحقيق في الهجمات التي يتعرض لها أمن الشبكة اللاسلكية مما يؤدي إلى زيادة تكرار تلك الهجمات.
الإجراءات المطلوبة	

1-8	إعداد كافة أجهزة الأمن والشبكة اللاسلكية لتسجيل سجلات الأحداث والتدقيق في نظام إدارة الأحداث والسجلات المركزي لأغراض التحليل والربط والتنبيه وفقاً لمعيار إدارة ومراقبة سجل الأحداث المعتمد في جامعة حائل All wireless network and security devices shall be configured to log events and audit logs to the central event and log management system for analysis, correlation and alerting as per Hail university's Event Log Management and Monitoring Standard.
2-8	ضمان اتساق كافة سجلات الأجهزة مع متطلبات معيار إدارة ومراقبة سجل الأحداث المعتمد في جامعة حائل All device logs shall be consistent with the requirements of Hail university's Event Log Management and Monitoring Standard.
3-8	إعداد أجهزة الشبكة اللاسلكية لإرسال الأحداث المتعلقة بمحاولات الدخول الناجحة وغير الناجحة إلى واجهات الإدارة إلى نظام إدارة الأحداث والسجلات المركزي لأغراض التحليل والربط والتنبيه. Wireless network devices shall be configured to send events related to failed and successful login to administration interfaces to the central event and log management system for analysis, correlation and alerting.
9	الإعدادات والتحصين (Secure Configuration)
الهدف	لضمان إيجاد ومعالجة الثغرات في أجهزة الشبكة والتحصين الامن لها.
المخاطر المحتملة	لضمان سلامة الشبكة اللاسلكية جامعة حائل يجب عمل اختبارات أمنية، وتطبيق التحديثات وتحصين الاعدادات والتحديث المستمر لمعالجة المخاطر والتهديدات.
الإجراءات المطلوبة	
1-9	إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في جامعة حائل Regular security testing, such as vulnerability assessments and penetration testing, shall be performed as per Hail university's Vulnerability Management Policy.

2-9	إجراء التحديثات والإصلاحات على أجهزة الشبكات اللاسلكية بشكل منتظم وفقاً لسياسة إدارة التحديثات والإصلاحات في جامعة حائل لضمان تحديث جميع البرامج الثابتة على الأجهزة وتطبيق التحديثات والإصلاحات. Network devices shall be regularly patched and updated as per Hail university's Patch Management Policy to ensure all devices firmware is up-to-date and all patches are applied.
3-9	إزالة/إلغاء تفعيل الخدمات غير الضرورية أو غير اللازمة على أجهزة الشبكة مثل: بروتوكول النقل الآمن (FTP) أو بروتوكول تل نت (Telnet) أو غيرها. Unnecessary/unrequired services on network devices, such as FTP, Telnet, etc., shall be removed/disabled.
4-9	إعداد وضبط كافة أجهزة الشبكة ليتزامن وقتها مع ثلاث خوادم زمنية إضافية على الأقل. All network devices shall be configured to synchronize clock with at least three centralized time sources.
5-9	التحديث المستمر لبرامج تشغيل الموجهات Keep the router's Firmware Up to Date
10	التحقق من سلامة البرمجيات والمعدات (Hardware and Software Integrity Validation)
الهدف	ضمان أن جميع برامج ومعدات الشبكة اللاسلكية تأتي من مصادر شرعية وأنه لم يتم العبث بها والتحقق من ذلك.
المخاطر المحتملة	تعتبر الاختراقات في سلسلة الإمداد فرصة لتركيب وتثبيت البرامج والمعدات الخبيثة ضمن شبكة جامعة حائل اللاسلكية، وقد تؤثر البرامج والمعدات التي تتعرض لانتهاك أمني على أداء الشبكة وتهدد سرية وسلامة وتوافر المعلومات الخاصة بجامعة حائل ونتيجة لذلك، سيصبح من الممكن تحميل البرمجيات غير المصرح بها أو الخبيثة على الجهاز بعد تشغيلها.
الإجراءات المطلوبة	
1-10	فحص كافة أجهزة الشبكة اللاسلكية المادية بحثاً عن أي علامات لوجود عبث عند التركيب. All physical wireless network devices shall be scanned for signs of tampering upon installation.

2-10	الحصول على البرمجيات وتحديثات النظام وحزم التحديثات والإصلاحات والترقيات الخاصة بمكونات الشبكة اللاسلكية من مصادر الشركة المصنعة. Software, updates, patches, and upgrades to wireless network components shall be obtained from validated sources.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الإلكتروني

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذا المعيار دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل

جامعة حائل
University of Ha'il

نموذج سياسة الأمن السيبراني المتعلق بالأمن المادي

مقيّد - داخلي

التاريخ:	05\04\2023
الإصدار:	3:0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالأمن المادي في جامعة حائل تطبق بفعالية.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني. حيث يلزم الجهات حماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرّح به والفقدان والسرقة والتخريب، وبما يحقق سلامة وتوافر وحماية بيانات ومعلومات الفعالية.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة والأصول المعلوماتية والمعدات والأجهزة الخاصة بـجامعة حائل وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية الأصول المعلوماتية والتقنية من الوصول المادي غير المصرّح به، على أن تشمل بحد أدنى ما يلي:

1-1 التحكم بالوصول للأماكن الحساسة مثل (مراكز البيانات، مراكز التعافي، أماكن معالجة المعلومات، مراكز المراقبة، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والمكونات التقنية).

2-1 مراقبة ومراجعة سجلات الدخول والخروج مثل (الدوائر التلفزيونية المغلقة CCTV).

3-1 حماية السجلات ومصادر المعلومات من الوصول غير المصرّح به.

4-1 أمن واتلاف وإعادة استخدام الأصول المادية التي تحتوي على معلومات مصنّفة وتشمل (الوثائق الورقية ووسائط التخزين والحفظ).

5-1 أمن الأجهزة والمعدات داخل المباني وخارجها.

6-1 تطوير وتطبيق إجراءات الاستجابة للطوارئ وخطط الإخلاء لمباني ومرافق الجهة في حال الاشتباه أو وقوع أي حوادث مادية أو بيئية.

7-1 منع دخول السوائل والمواد الخطرة للأماكن الحساسة.

8-1 التحكم بدرجة حرارة الأماكن الحساسة للحفاظ على كفاءة أداء الأنظمة.

9-1 منع دخول الأفراد غير المصرّح لهم دخول القاعات والغرف المصنّفة والحصول على تصريح مسبق استناداً على مبدأ "الحاجة إلى المعرفة " و "الحاجة إلى الوصول" و "الحد الأدنى من الصلاحيات".

10-1صيانة المعدات والأجهزة داخل المباني وخارجها بشكل دوري.

2- يجب تنفيذ ضوابط لحماية الكابلات الصوتية والاتصالات والشبكة والطاقة ضد الأضرار المادية، بعد دراسة المخاطر المحتملة. كما يجب أن تغطي هذه الضوابط بحد أدنى ما يلي:

2-1 حماية كابلات الاتصالات وشبكة البيانات من زراعه أجهزه تنصت (Wiretapping).

2-2 عدم تمديد كابلات الاتصالات وشبكة البيانات في مناطق تمكن أطراف خارجية من الوصول إليها.

2-3 حماية وعزل كابلات الاتصالات وشبكة البيانات بكفاءة من الضرر أو الاعتراض غير المصرح به، وضمان تمديدها عبر مناطق آمنة ومحمية.

2-4 عزل كابلات الكهرباء والطاقة عن كابلات الاتصالات وشبكة البيانات.

2-5 استخدام مصادر طاقة متعددة وغير منقطعة لدعم التشغيل المستمر للأنظمة والمرافق الحساسة (مثل مراكز البيانات)

3- تنفيذ تقييم لمخاطر الأمن المادي من قبل الجهات المسؤولة عن الأمن المادي عبر تحليل البيئة المادية والمناطق المحيطة لرصد التهديدات الأمنية وتهديدات السلامة ومعرفة مواطن الضعف ومعالجتها لحماية الأصول المعلوماتية من التعرض لهذه التهديدات.

4- على إدارة الأمن والسلامة تطوير واعتماد لائحة وإجراءات الأمن المادي والسلامة الخاصة بـجامعة حائل أو بأي حدث أو فعالية تشارك في تنظيمها. بحيث تشمل تحديداً دقيقاً للواجبات، والمهام، لتكون بمثابة إطار عام لخدمة السلامة، والوقاية، والإنقاذ، ومكافحة الحريق، والإسعاف، ودليلاً مرشداً في سبيل حماية الأرواح والأصول والمعلومات.

5- تنفيذ المسح الأمني وتفتيش الحضور للاجتماعات المصنّفة، على أن يتم توفير أجهزة الكشف عن المعادن والمواد الخطيرة.

6- تصنيف جميع مرافق الجهة استناداً على تصنيف المعلومات التي يتم تداولها ومعالجتها فيها.

7- عدم منح الأطراف الخارجية صلاحية وصول مادي لمرافق الجهة إلا بعد تحقيق اشتراطات أمنية، على أن يتم مراقبة وصولهم ومرافقتهم في الأماكن التي تتطلب ذلك.

8- يجب أن تقتصر صلاحية إدارة نظام الوصول المادي على أشخاص بامتيازات محددة يمكن تدقيقها ومراجعتها.

9- مراجعة وتحديث صلاحيات الوصول المادي للمناطق الحساسة بشكل دوري.

10- توعية منسوبي الجهة حول أفضل الممارسات المتعلقة بالأمن المادي مثل سياسة المكتب النظيف وضمان التزامهم بها.

11- يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لمتطلبات الأمن السيبراني المتعلق بالأمن المادي.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني بجامعه حائل.

3- **تنفيذ السياسة وتطبيقها:** مدير إدارة الأمن والسلامة .

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على جميع العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة حائل .

جامعة حائل
University of Ha'il

سياسة إدارة حوادث وتهديدات الأمن السيبراني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حوادث وتهديدات الأمن السيبراني الخاصة بـجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل، وتنطبق هذه السياسة على جميع العاملين في جامعة حائل.

بنود السياسة

1- المتطلبات العامة

1-1 يجب على جامعة حائل توفير التقنيات اللازمة لتحديد حوادث الأمن السيبراني واكتشافها في الوقت المناسب أو من خلال استلام البلاغات من العاملين أو المستفيدين من خدمات جامعة حائل وإدارتها بشكل فعال.

2-1 يجب على جامعة حائل التعامل مع تهديدات الأمن السيبراني استباقياً باعتماد وسائل دفاع وقائية من أجل منع أو تقليل الآثار المترتبة على سرية المعلومات أو سلامتها أو توافرها.

3-1 تشمل حوادث الأمن السيبراني على سبيل المثال لا الحصر ما يلي:

1-3-1 التغييرات غير المصرح بها في إعدادات أجهزة المستخدمين المكتبية و/أو المحمولة، والتغييرات في إعدادات الخوادم.

2-3-1 الإصابة بالبرمجيات الضارة.

3-3-1 التغييرات في التطبيقات من حيث المظهر (المظهر غير الاعتيادي) والتعديلات على صلاحيات المستخدم مثل رفع مستوى الوصول.

4-3-1 الوصول غير المصرح به إلى البيانات، و/أو تعديلها دون تصاريح أو صلاحيات المستخدمين.

5-3-1 محاولات الحصول على معلومات يمكن استخدامها في تنفيذ الهجمات، مثل فحص منافذ الشبكة (Port Scans)، والهندسة الاجتماعية (Attacks Social Engineering)، وفحص مجال شبكة محددة (Targeted Scans Across IP Range)، وغيرها.

6-3-1 التفعيل غير المصرح به لحسابات مستخدمين موقوفة أو محذوفة.

4-1 يجب توثيق واعتماد خطة استجابة للحوادث توضح إجراءات التعامل مع حوادث الأمن السيبراني، والأدوار والمسؤوليات الخاصة بفريق الاستجابة، وصلاحيات اتخاذ القرارات الهامة، وآلية التواصل مع الجهات الداخلية والخارجية وكذلك آليات التصعيد. (ECC-2-13-3-1)

5-1 في حال اكتشاف حادثة أمن سيبراني في جامعة حائل، يجب على فريق الاستجابة للحوادث اتخاذ الخطوات اللازمة للتعامل مع الحادثة التي تم اكتشافها فوراً والتي تشمل تحليل بيانات الحادثة وتحديد أثرها.

6-1 في حال اكتشاف حادثة أمن سيبراني، يجب تحليل المعلومات المتاحة ذات العلاقة مثل سجلات النظام والشبكة، والسجلات الصادرة من المنتجات الأمنية ذات الصلة (مثل السجلات الصادرة من حلول الحماية من البرمجيات الضارة، ومن جدار الحماية، ومن أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات).

7-1 يجب معالجة الأدلة اللازمة (على سبيل المثال، جمع الأدلة وفقاً للقيود القانونية وحمايتها من التلاعب) وينبغي توثيقها وحفظها بصورة محمية حتى لا تفقد جدواها في التحليل، ثم تحليلها دون تدميرها أو تعديل صورتها الأصلية.

8-1 في حال وقوع حادثة أمن سيبراني، يجب التحقيق في أسباب حدوثها والاستعانة بالمختصين مثل خبراء التحليل الجنائي الرقمي (Digital Forensics Analysts) وفرق الاستجابة للحوادث السيبرانية.

9-1 يجب مراجعة خطة الاستجابة للحوادث مرة واحدة في السنة؛ على الأقل.

10-1 يجب تصنيف حوادث الأمن السيبراني بناءً على مستوى خطورتها ومدى تأثيرها على أعمال جامعة حائل. (ECC-2-13-3-2)

11-1 يتم تصنيف حوادث الأمن السيبراني وفقاً للجدول أدناه:

جدول 1: تصنيف حوادث الأمن السيبراني

مستوى الخطورة	الوصف	الوقت المستهدف للاستجابة	الوقت المستهدف لحل الحادثة
مرتفع جداً	ضرر جسيم يؤثر بشكل مباشر على سمعة جامعة حائل ومصداقيتها، أو يؤثر على العديد من وحدات الأعمال الوظيفية فيها أو موقع الأعمال بصورة كبيرة، مما يستدعي تفعيل إجراءات استمرارية الأعمال.	فوراً	بدء الشروع بحل المشكلة فور حدوثها
مرتفع	انقطاع كبير يؤثر على وحدات الأعمال الوظيفية أو الخدمات الرئيسية أو الموقع.	فورًا	بدء الشروع بحل المشكلة فور حدوثها
متوسط	تأثير متوسط في سير عمل وحدات الأعمال الوظيفية أو المواقع أو أصول تقنية المعلومات، إضافة إلى تأثير يتراوح	3-2 ساعات	8 -9 ساعات

مستوى الخطورة	الوصف	الوقت المستهدف للاستجابة	الوقت المستهدف لحل الحادثة
	ما بين المتوسط والمرتفع على وحدات الأعمال غير الهامة في جامعة حائل.		
منخفض	تأثير بسيط على عدد قليل من الموارد، ويمكن تحمل الحادثة لفترة معينة من الزمن.	3-2 ساعات	24 ساعة

2- الإبلاغ عن حوادث الأمن السيبراني

1-2 يجب رفع الوعي الأمني للعاملين في جامعة حائل وتوضيح مسؤولياتهم تجاه حوادث الأمن السيبراني أو التهديدات، وذلك للإبلاغ فوراً عن أي حوادث أو تهديدات متعلقة بالأمن السيبراني.

2-2 يجب على جامعة حائل تحديد جهة اتصال داخلية للإبلاغ عن الحوادث سواءً عن طريق الهاتف أو البريد الإلكتروني.

3-2 يجب أن تحدد جامعة حائل الحوادث والتهديدات التي يجب الإبلاغ عنها ووقت الإبلاغ عنها والأطراف التي يجب إبلاغها، مثل معالي رئيس الجامعة والمشرف على إدارة الأمن السيبراني وفرق الاستجابة للحوادث داخل جامعة حائل والإدارات المسؤولة عن الأصول المعلوماتية والتقنية.

4-2 قبل الإفصاح عن أي معلومات متعلقة بالحوادث الأمنية إلى أطراف خارجية، يجب الحصول على الموافقات اللازمة بما يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

5-2 يجب إبلاغ الهيئة الوطنية للأمن السيبراني عن حوادث الأمن السيبراني. (ECC-2-13-3-3)

6-2 يجب على جامعة حائل إطلاع الهيئة الوطنية للأمن السيبراني على تبليغات الحوادث ومؤشرات وتقارير الانتهاكات. (ECC-2-13-3-4)

3- الاستجابة للحوادث والتعافي من حوادث الأمن السيبراني

1-3 يجب على فريق الاستجابة للحوادث في إدارة الأمن السيبراني كتابة تقرير مفصل عن حوادث الأمن السيبراني، ويجب أن يشمل التقرير نوع الحادثة وفئتها والعاملين الذين أبلغوا عن الحادثة أو الأدوات المستخدمة في اكتشافها، والخدمات أو الأصول أو المعلومات المتأثرة بها، وكيفية اكتشاف الحادثة، وأي وثائق أو موارد أخرى متعلقة بالحادثة.

2-3 يجب أن يتم إشراك الموردين في حل الحوادث أو استعادة الخدمات عند الحاجة.

3-3 يجب أن تتضمن إجراءات التعافي من حوادث الأمن السيبراني تحديد الثغرات التي تم استغلالها خلال الحادثة ومعالجتها بالتدابير الفنية والإدارية اللازمة، على سبيل المثال:

1-3-3 تطبيق الضوابط الأمنية الإضافية (Compensating Controls).

2-3-3 تنصيب حزم التحديثات والإصلاحات المحدثة.

3-3-3 استعادة النسخ الاحتياطية للنظام.

4-3-3 إعادة ضبط إعدادات الأنظمة الأمنية، مثل نظام جدار الحماية وأنظمة الكشف عن الاختراق.

4-3 يجب على إدارة الأمن السيبراني حفظ تقارير الحادثة (التي تتضمن معلومات حول الاختراقات الأمنية والحوادث مثل المعلومات المتعلقة بالأفراد والإدارات وأنظمة معينة و/أو منهجية الهجمات) بمكان آمن وتقييد الوصول إليها.

5-3 يجب تصعيد الحادثة، في حال عدم حلها في الوقت الزمني المحدد، وفقاً لتصنيف الحوادث وإجراءات التعامل معها وآلية التصعيد المعتمدة.

6-3 في حال تطلبت معالجة حادثة سيبرانية إجراء تغييرات على المكونات التقنية، يجب الالتزام بإجراءات إدارة التغيير المعتمدة لدى جامعة حائل.

7-3 بعد التعامل مع الحادثة، يجب على فريق الاستجابة للحوادث في إدارة الأمن السيبراني عقد اجتماعات لمناقشة الدروس المستفادة (Lessons Learned) مع الإدارات ذات العلاقة لتحسين طرق التعامل مع حوادث الأمن السيبراني في المستقبل، وكذلك التعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال جامعة حائل.

4- المعلومات الاستباقية بشأن التهديدات

1-4 يجب الاشتراك مع مقدمي المعلومات الاستباقية (Threat Intelligence) للاطلاع المستمر على الحوادث والتهديدات المتعلقة بالأمن السيبراني والتعامل مع تلك المعلومات بشكل مباشر. (ECC-2-13-3-5)

2-4 يجب حفظ المعلومات الاستباقية بشأن التهديدات وتنظيمها في قاعدة بيانات مرنة وملائمة لصياغة ملاحظات العمل والبيانات الوصفية للمؤشرات، مثل قاعدة المعرفة (Knowledge Base).

3-4 يجب تحديث أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات (Intrusion Prevention and Detection Systems) بالمعلومات الاستباقية المتعلقة بالتهديدات والتأكد من إمكانية تلك الأنظمة من اكتشاف التهديدات والتعامل معها بشكل فعال.

5- متطلبات أخرى

1-5 يجب مراجعة متطلبات الأمن السيبراني الخاصة بإدارة حوادث وتهديدات الأمن السيبراني دورياً. (ECC-2-13-4)

2-5 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة حوادث وتهديدات الأمن السيبراني.

3-5 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني .

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الإلكتروني وإدارة الأمن السيبراني

الالتزام بالسياسة

1- يجب على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل مستمر.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

معيار حماية البريد الإلكتروني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

يهدف هذا المعيار إلى توفير متطلبات الأمن السيبراني التقنية المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية الناتجة عن استخدام جامعة حائل للبريد الإلكتروني وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي:

- سرية معلومات البريد الإلكتروني.
- سلامة معلومات البريد الإلكتروني.
- توافر خدمة البريد الإلكتروني.

يتبع هذا المعيار المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهو متطلب تشريعي في الضابط رقم ١-٣-٣ والضابط رقم ٢-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل

يغطي هذا المعيار جميع أنظمة البريد الإلكتروني الخاصة بـجامعة حائل، وينطبق على جميع مستخدمي البريد الإلكتروني في جامعة حائل.

المعايير

1	تصفية المحتوى وتحليله (Content Filtering and Analysis)
الهدف	ضمان حماية عناوين البريد الإلكتروني من الرسائل الاقتحامية (Spam Emails) والتصيّد الإلكتروني (Phishing Emails) وروابط الإنترنت الضارة والمشبوهة (Malicious URLs) وأي نوع آخر من المحتوى الضار.
المخاطر المحتملة	يُمكن أن ينخدع المستخدم برسائل البريد الإلكتروني التي تحتوي على محتوى ضار ومشبوه، وقد تتعرّض جامعة حائل لهجمات سيبرانية في حال عدم فحص رسائل البريد الإلكتروني والتأكد من سلامتها.
الإجراءات المطلوبة	
1-1	فحص جميع رسائل البريد الإلكتروني الواردة والصادرة الخاصة بـجامعة حائل من المحتوى الضار والمشبوه (Malicious Content). All Hail university's inbound and outbound emails shall be scanned for malicious and suspicious content.
2-1	ترميز أو وضع علامة (Tag/Label) على جميع رسائل البريد الإلكتروني الواردة والصادرة الخاصة بـجامعة حائل بالترميزات الوقائية المناسبة بما يعكس مستوى الحساسية والسريّة بناءً على مستوى تصنيف البيانات ووفقاً لنتيجة تحليل المحتوى، أو استخدام إجراء الترميز المعياري (Tagging/Labeling Standard) المطبّق في جامعة حائل وفقاً لسياسة أمن البريد

	الإلكتروني المتّبعة فيها. من الأمثلة على الترميزات أو العلامات: محتوى ضار، ومُرسِل غير مصرّح له، وغير لائق، ورسالة اقتحامية، ورسالة اقتحامية مشتبهة (Suspected SPAM)، وآمن، وحسّاس، وغيرها. All Hail university's inbound and outbound emails shall be tagged/labeled with appropriate protective tagging/labeling reflecting the sensitivity and confidentiality levels based on the data classification level and as per Hail university's Data Classification Policy and the results of content analysis. Alternatively, Hail university's applicable Tagging/Labeling Standard shall be used as per Hail university 's Email Protection Policy. Some examples of tags and labels are malicious, bad sender, inappropriate, spam, suspected spam, safe, sensitive, etc.
3-1	حجب جميع رسائل البريد الإلكتروني الواردة بترميزات أو علامات وقائية تُشير إلى المحتوى غير المسموح به وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في جامعة حائل، على سبيل المثال: • حجب الرسائل الخبيثة وغير المصرّح بها والاقتحامية. • حجر الرسائل الاقتحامية المشتبهة. • السماح بالرسائل الآمنة. All inbound emails shall be blocked and tagged/labeled to reflect disallowed content as per Hail university's Email Protection Policy. For example: • **Block** malicious, blacklisted and spam emails. • **Quarantine** suspected spam emails. • **Allow** safe emails.
4-1	حجب جميع رسائل البريد الإلكتروني الصادرة والمصنفة، بناءً على ترميزات أو علامات وقائية تُشير إلى مستوى سريّة رسالة البريد الإلكتروني وذلك وفقاً لسياسة أمن البريد الإلكتروني المتّبعة وسياسة تصنيف البيانات في جامعة حائل، على سبيل المثال: • حجب الرسائل الحسّاسة والسريّة. • السماح بالرسائل العامة والخاصة. All outbound classified emails shall be blocked based on the protective tags/labels reflecting the email classification level as per Hail university's Email Protection Policy. For example: • **Block** sensitive and confidential emails. • **Allow** public and restricted emails.
5-1	حجب رسائل البريد الإلكتروني الاقتحامية التي تتضمّن درجات غير مسموح بها من المخاطر الاقتحامية وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في جامعة حائل، على سبيل المثال: • حجب الرسائل شديدة المخاطر. • حجر الرسائل متوسطة المخاطر. • السماح بالرسائل منخفضة ومعدومة المخاطر.

	Spam emails reflecting unacceptable spam risk scores shall be blocked as per Hail university's Email Protection Policy. For example: • **Block** high risk emails. • **Quarantine** medium risk emails. • **Allow** low risk and no-risk emails.
6-1	حجب رسائل البريد الإلكتروني الواردة التي تحتوي على روابط إنترنت ونطاقات ضارة ومشبوهة (Malicious URLs and Domains) ومحاولات تصيّد وما إلى ذلك. Inbound emails containing malicious URLs, phishing attempts, malicious domains, etc. shall be blocked.
7-1	استبدال عناوين الويب النشطة (Active Web Addresses) المُدرجة في نص رسالة البريد الإلكتروني بعناوين أخرى. Active Web Addresses in emails shall be replaced with other addresses.
8-1	حجب رسائل البريد الإلكتروني الواردة التي تحتوي على محتوى تفاعلي (Active Content) في نص الرسالة الإلكترونية أو حذفه منها. Inbound emails containing active content shall be blocked. Alternatively, the active content in the email's body shall be removed.
9-1	حجب رسائل البريد الإلكتروني الواردة والصادرة التي تحتوي على ملفات أو محتويات حجمها أكبر من الحجم المسموح حسب سياسات جامعة حائل، أو تأجيلها حتى يتم التحقق من الملف من قبل الموظف المسؤول أو وفقاً للسياسة المتبعة. Inbound and outbound emails with extra-large files or content shall be blocked or delayed until the files are verified by the responsible employee or as per the enforced policy.
10-1	حجب رسائل البريد الإلكتروني المُرسلة إلى قائمة غير معرّفة من عناوين البريد الإلكتروني. Outbound emails to unknown distribution lists shall be blocked.
2	حماية المصادقة (Secure Authentication)
الهدف	ضمان حماية استخدام البريد الإلكتروني من خارج جامعة حائل من الوصول غير المصرّح به من خلال صفحة موقع البريد الإلكتروني (Webmail) أو برنامج قارئ البريد الإلكتروني الخارجي (Email Client).
المخاطر المحتملة	يُعرّض الوصول غير المصرّح به إلى البريد الإلكتروني جامعة حائل إلى مخاطر كبيرة قد تؤدي إلى سرقة المعلومات وانتحال الشخصيات مما يتيح استخدامها في تنفيذ المزيد من الهجمات السيبرانية ضد جامعة حائل وبنيتها التحتية.

	الإجراءات المطلوبة
1-2	تطبيق آليات التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication "MFA") على إمكانية وصول المستخدمين للبريد من خارج الشبكة خلال برنامج قارئ البريد الإلكتروني الخارجي (Email Client) وصفحة موقع البريد الإلكتروني (Webmail)، (مثل: Outlook Web Access "OWA") وفقاً للضابط رقم ٢-٤-٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018). Multi-Factor Authentication (MFA) shall be implemented for remote email client access and webmail access by users (e.g., Outlook Web Access "OWA") as per ECC-2-4-3-2.
2-2	بالإضافة إلى ضرورة إدخال اسم المستخدم وكلمة المرور، يجب على المستخدم استعمال آليات أخرى للتحقّق من الهوية عند الدخول من خارج الشبكة، مثل: الخصائص الحيوية (Biometrics)، أو جهاز توليد الأرقام العشوائية (Hardware Keys)، أو الرسائل القصيرة المؤقتة لتسجيل الدخول (One-Time-Password)، أو البطاقات الذكية (Smartcards) أو شهادات التشفير (Certificates)، أو غيرها. Besides a user/password combination, users shall implement other authentication mechanisms when accessing emails from outside the network (e.g., biometrics, hardware keys, one-time passwords, smart cards, encryption certificates, etc.).
3-2	ضبط متطلبّات إعدادات كلمات المرور المعقدة للبريد الإلكتروني وفقاً لسياسة إدارة هويات الدخول والصلاحيات المتّبعة في جامعة حائل. Complex email password requirements shall be configured as per Hail university's Identity and Access Management Policy.
4-2	تطبيق تقنيات التشفير، مثل: «أمن مستوى النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks)، لحماية آليات التحقّق من الهوية خلال إرسالها. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suites) المُوصى بها. يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة حائل. Encryption methods, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), shall be implemented to protect authentication mechanisms during transmission. Recommended next generation encryption protocols and cipher suites (such as cipher suite B) shall be used. Refer to Hail university's Cryptography Standard.

3	حماية محتوى البريد الإلكتروني (Content Protection)
الهدف	ضمان حماية رسائل البريد الإلكتروني التي تحتوي على مرفقات من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقاً وأي نوع آخر من المرفقات الخبيثة.
المخاطر المحتملة	يُمكن أن ينخدع المستخدم برسائل البريد الإلكتروني التي تحتوي على مرفقات خبيثة حيث قد تتعرض جامعة حائل لاختراق بياناتها أو الوصول إليها بشكل غير مصرّح به أو كشفها في حال عدم فحص مرفقات البريد الإلكتروني.
الإجراءات المطلوبة	
1-3	تطبيق وتفعيل تصنيفين لمرفقات البريد الإلكتروني: التصنيف الأول وفقاً لنوع الملف، والتصنيف الثاني وفقاً لمحتوى الملف. Two types of email attachment classification shall be configured; based on file type and based on file content.
2-3	ترميز المرفقات حسب أنواع المرفقات وصيغتها. على سبيل المثال: • **اللائحة السوداء:** جميع أنواع نسخ البرمجيات القابلة للتنفيذ من ويندوز (Windows PE) وأوامر ماكرو أوفيس (Office Macros) والبرمجيات أو الأوامر النصية (Scripts)، وغيره. • **اللائحة الرمادية:** الأرشيفات متعدّدة المستويات (Multi-Layer Archives) وملفات حماية كلمة المرور وملفات التشفير والملفات التي يزيد حجمها عن الحد الأقصى، وغيرها من الملفات ضمن قائمة الحجر (Quarantine-list) • **اللائحة البيضاء:** ملفات برامج أوفيس القياسية (مثل: docx وpptx وxlsx) وملفات pdf وtxt، والملفات الأرشيفية، وغيرها. • **لائحة المرفقات غير المعروفة:** أنواع وصيغ الملفات غير المعروفة والتي يتعذّر التحقّق منها. Attachments based on file types and formats shall be tagged. For example: • **Blacklist:** All forms of Windows PE, Office macros, scripts, etc. • **Graylist (quarantine-list):** Multi-layer archives, password protection files, encryption files, files exceeding the maximum size, etc. • **Whitelist:** Standard Microsoft Office extensions (docx, pptx, xlsx, etc.), pdf, txt, archives, etc. • **Unknown:** Unknown file type/format, or unable to detect.
3-3	ترميز جميع المرفقات بعد فحصها من البرمجيات الضارة بإدراج نتائج الفحص، على سبيل المثال: • **ضارة:** تحتوي على فيروس أو برنامج ضار أو تهديد متقدّم مستمر أو غيره. • **آمنة:** تحتوي على ملف مرفق آمن.

	• **غير معروفة:** أي تعذّر فحصها. All malware-scanned attachments shall be tagged with scan results. For example: • **Malicious:** Contains virus, malware, APT, etc. • **Safe:** Malware-free attachment. • **Unknown:** Unable to scan.
4-3	تحديد أنواع الملفات باستخدام محتواها مثل ترويسة وتذييل الملف (Footer and Header) وليس من خلال صيغها. File types shall be determined using file content (file header and footer), not extensions.
5-3	فحص جميع المرفقات المسموحة والتي تمت تصفيتها للتأكد من خلوها من الملفات الضارة، مثل: الفيروسات والبرمجيات الضارة وأي نوع آخر من الملفات المشبوهة. All whitelisted and filtered attachments shall be scanned for malicious files including viruses, malware and any other form of suspicious files.
6-3	فحص جميع أنظمة وخوادم البريد للتحقّق من عدم وجود أي برمجيات ضارة أو مشبوهة في المكونات التقنية للبريد الإلكتروني وبوابة البريد (Mail Gateway) وخاصية ترحيل البريد (Mail Relay) أو خادم البريد (Mail Server) قبل أن تصل إلى برنامج قارئ البريد (Email Client). Malware scanning shall be performed on Mail Gateway, Mail Relay or Mail Server before it reaches the Email Client.
7-3	إجراء فحص للتحقّق من عدم وجود أي برمجيات ضارة أو مشبوهة عبر برامج قراءة البريد (Email Clients) باستخدام حل يُقدّمه مورّد أو مزوّد مختلف عن الموجود في البند 3-6 مثل إضافة أدوات للحماية من الفيروسات إلى برنامج قارئ البريد. Malware scanning shall be performed on email clients using a solution from a vendor or provider different from the one mentioned in clause 3-6 (e.g., AV plug-ins added to outlook client)
8-3	فحص جميع المرفقات المسموحة والتي تمت تصفيتها عبر إجراء تحليل ديناميكي للمرفقات باستخدام تقنية الحماية المعزولة (Sandbox) للتحقّق من التهديدات المتقدّمة المستمرة (APT) والبرمجيات الضارة غير المعروفة مسبقاً. Allowed attachments, on which dynamic analysis was performed in sandbox, shall be scanned to detect Advanced Persistent Threats (APTs) and zero-day malware.
9-3	حجب (أي عدم السماح لها بالمرور إلى بريد المستخدم) أو تجريد جميع رسائل البريد الإلكتروني التي تحتوي على ملفات مرفقة ضارة أو مصنفة ضمن اللائحة السوداء وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في جامعة حائل ثمّ إضافة عنوان المرسل والنطاق إلى اللائحة السوداء.

	All emails with blacklisted or malicious attachments shall be blocked/stripped as per Hail university's Email Protection Policy. Sender's email address and domain shall be added to the blacklist.
10-3	حجر (أي إيقاف وصولها إلى بريد المستخدم إلى حين التأكد من سلامة محتواها) جميع رسائل البريد الإلكتروني التي تتضمّن ملفات ضمن اللائحة الرمادية إذا كانت آمنة. All emails with graylisted attachments shall be quarantined if they are malware-free.
11-3	حجر جميع رسائل البريد الإلكتروني التي تتضمّن ملفات مرفقة غير معروفة. All emails with **Unknown** attachments shall be quarantined.
12-3	قبول جميع رسائل البريد الإلكتروني التي تتضمّن ملفات مرفقة آمنة ومسموحة. All emails with whitelisted attachments shall be allowed if they are malware-free.
4	التحقّق من مرسل البريد الإلكتروني (Email Sender Verification)
الهدف	ضمان الحفاظ على سريّة بيانات البريد الإلكتروني والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.
المخاطر المحتملة	تحمي خاصية التأكّد من سلامة وموثوقية رسائل البريد الإلكتروني جامعة حائل من عمليات تزوير البريد الإلكتروني والرسائل الإلكترونية الضارة والكشف عن المعلومات المهمّة والحسّاسة والوصول غير المصرّح به إلى الرسائل الإلكترونية الخاصة بالمستخدم.
الإجراءات المطلوبة	
1-4	التحقّق من المُرسِل باختبار قاعدتين من بيانات سمعة المُرسِل (Sender Reputation) على الأقل. Sender shall be verified against at least two sender reputation databases.
2-4	التحقّق من عنوان المُرسِل مقابل قوائم الرسائل الاقتحامية (Email SPAM lists) المتواجدة على الإنترنت والتي تحدث يومياً. Sender email address shall be verified against sender spam lists that are available on the Internet and are updated daily.
3-4	التحقّق من بروتوكول الإنترنت (Internet Protocol "IP") الخاص بخادم بريد المُرسِل واسم النطاق بمقارنته مع القائمة اللحظية لعناوين الإنترنت العشوائية (Real-time Blackhole Lists).

	Sender email server **IP** and **domain name** shall be verified against Real-time Blackhole Lists (RBL).
5	التحقّق من سلسلة الثقة المتعلقة بالبريد الإلكتروني (Email Chain of Trust Verification)
الهدف	ضمان الحفاظ على سريّة بيانات البريد الإلكتروني والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.
المخاطر المحتملة	قد يؤدي عدم التأكد من سلامة وموثوقية رسائل البريد الإلكتروني إلى عمليات تزوير البريد الإلكتروني والرسائل الإلكترونية الخبيثة والكشف عن المعلومات المهمة والحسّاسة والوصول غير المصرّح به إلى الرسائل الإلكترونية الخاصة بالمستخدمين.
الإجراءات المطلوبة	
1-5	إنشاء وتسجيل إطار سياسة المُرسِل (Sender Policy Framework "SPF") والبريد المُعرَّف بمفاتيح النطاق (Domain Key Identified Mail "DKIM") ومصادقة الرسائل والإبلاغ عنها ومطابقتها استناداً إلى النطاق (Domain-based Message Authentication, Reporting and Conformance "DMARC"). Sender Policy Framework (SPF), Domain Key Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) shall be created and registered.
2-5	التحقّق من المُرسِل وفق نظام مصادقة هوية مُرسِل الرسائل (SenderID) وسجلات إطار سياسة المُرسِل (SPF) واتخاذ الإجراء المناسب وفقاً لسياسة أمن البريد الإلكتروني المتّبعة في جامعة حائل. • رفض الفشل الكامل (SPF Strict -Fail) في إطار سياسة المُرسِل. • حجر الفشل الجزئي (SPF Relaxed -Fail) في إطار سياسة المُرسِل. Senders shall be verified according to their SenderID/SPF records and actions shall be taken as per Hail university's Email Protection Policy. • **Reject** SPF hard-fail • **Quarantine** SPF soft-fail
3-5	التحقّق من المُرسِلين وفق البريد المُعرَّف بمفاتيح النطاق (DKIM) التي يستخدمونها. • رفض الفشل في البريد المُعرَّف بمفاتيح النطاق. Senders shall be verified according to their DKIM. • **Reject** DKIM fail.
4-5	ضبط إطار سياسة المُرسِل (SPF) على السجلات الخارجية المقابلة لنظام أسماء النطاقات (External DNS Records) لكل أسماء النطاقات التي تملكها جامعة حائل للسماح فقط بسجلات تبادل البريد (Mail Exchange Records) في الخوادم التي صرّحت لها جامعة حائل بإرسال الرسائل الإلكترونية نيابةً عنها.

	SPF on external records facing DNS shall be configured for each and every domain name owned by Hail university to allow only Mail Exchange Records (MX Records) of servers authorized by Hail university to send emails on its behalf.
5-5	ضبط سجلات البريد المُعرَّف بمفاتيح النطاق (DKIM) لتوقيع محتوى رسائل البريد الإلكتروني (Email Digital Signing) الخاصة بـجامعة حائل وذلك بتحديد مفاتيح عامة تشفيرية للتواقيع (Public Key Cryptography). DKIM records shall be configured to sign the content of Hail university's emails by specifying cryptographic public keys for signing.
6-5	ضبط «مصادقة الرسائل والإبلاغ عنها ومطابقتها استناداً إلى النطاق» (DMARC) لأتمتة تطبيق الإجراءات المناسبة بشأن الأخطاء المرصودة في نظام مصادقة هوية مُرسِل الرسائل وسجلات إطار سياسة المُرسِل والبريد المُعرّف بمفاتيح النطاق وفقاً لسياسة حماية البريد الإلكتروني المتبعة في <اسم الجهة>. على سبيل المثال: • **رفض/حجر** الفشل الجزئي (Relaxed Fail) في البريد المُعرَّف بمفاتيح النطاق (DKIM) وسجلات إطار سياسة المُرسِل (SPF). ملاحظة: الفشل الجزئي (Relaxed Fail) يسمح بمرور الرسائل الواردة من النطاقات الفرعية، والفشل الكامل (Strict Fail) يمنع ذلك. Domain-based Message Authentication, Reporting and Conformance (DMARC) shall be configured to automate the actions taken on SenderID/SPF fails and DKIM fails. For example: • **Reject/Quarantine** Relaxed Fail in DKIM and SPF. Note: Relaxed Fail allows emails received from sub-domains and Strict Fail blocks them.
6	حماية أنظمة البريد الإلكتروني (Email Systems Security)
الهدف	ضمان حماية وأمن البنية التحتية الأساسية لخدمة البريد الإلكتروني بما في ذلك خوادم البريد وبواباته وقواعد بياناته وحلوله الأمنية.
المخاطر المحتملة	من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية البنية التحتية لخدمة البريد الإلكتروني في جامعة حائل إلى استغلال المهاجمين لنقاط الضعف الكامنة في أنظمة البريد الإلكتروني واستغلال ثغراتها للوصول غير المصرّح به إلى شبكة جامعة حائل وبياناتها.
الإجراءات المطلوبة	
1-6	إجراء اختبارات أمنية دورية (مثل: فحص الثغرات الأمنية وتنفيذ عمليات اختبار الاختراق) وفقاً للسياسات والإجراءات ذات العلاقة في جامعة حائل.

Regular security testing (such as vulnerability assessments and penetration testing) shall be performed as per Hail university's relevant policies and procedures.	
مراجعة وتطبيق حزم التحديثات والإصلاحات دورياً على أنظمة البريد الإلكتروني وفقاً لسياسة إدارة التحديثات والإصلاحات المتّبعة في جامعة حائل، وضمان تحديث جميع الأنظمة. Email systems shall be regularly patched and updated as per Hail university's Patch Management Policy. Additionally, it shall be ensured that all systems are up-to-date.	2-6
حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من أنظمة البريد الإلكتروني، مثل: خدمات الطباعة وبروتوكول الاتصال عن بعد غير الآمن (Telnet) ، وغيرها. Unnecessary/unrequired applications and services on email systems, such as printing services, telnet, etc. shall be removed/disabled.	3-6
ضبط إعدادات وتحصين (Secure Configuration and Hardening) أنظمة البريد الإلكتروني على مستوى التطبيقات وقاعدة البيانات والتشغيل كل ثلاثة أشهر. يُرجى الرجوع إلى معيار أمن الخادم ومعيار أمن قاعدة البيانات المعتمدين في جامعة حائل. Secure Configuration and Hardening shall be applied every three months on applications, databases, and operating systems. Refer to Hail university's Server Security Standard and Database Security Standard.	4-6
تقييد الوصول (Restrict Access) إلى أنظمة البريد الإلكتروني ليكون مسموح به فقط لمديري أنظمة البريد الإلكتروني (Mail System Administrators). Access to email systems shall be restricted to email system administrators only.	5-6
حذف أو إلغاء تفعيل الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة. Default/non-interactive/unneeded accounts shall be removed/disabled.	6-6
إلزام مديري الأنظمة ومُشغّلي أنظمة البريد الإلكتروني باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى أنظمة البريد الإلكتروني. Email systems administrators and operators shall be obliged to use multi-factor authentication to access email systems.	7-6

8-6	استخدام مبدأ الحماية الذي يمنح مديري ومُشغّلي أنظمة البريد الإلكتروني (Email System Administrators and Operators) الحد الأدنى من صلاحيات الوصول (Least-Privilege Principle) إلى مختلف أنواع أنظمة البريد الإلكتروني. The least-privilege principle shall be used to provide access for email system administrators and operators to email systems.
9-6	تقييد الوصول الشبكي إلى أنظمة إدارة البريد الإلكتروني على المنطقة الشبكية التي تتواجد فيها والمنطقة الشبكية الخاصة بالإدارة (Management Zone). Network access to email management systems shall be restricted to Email System Zone and Management Zone.
10-6	حذف أو إلغاء تفعيل خصائص تطبيق البريد الإلكتروني وملفات الإعدادات غير الضرورية أو غير اللازمة. Unnecessary/unrequired email application features and configuration files shall be removed/disabled.
11-6	حجب إمكانية الوصول (Restrict Access) إلى مجلدات الشبكة (Network File Shares) والملفات غير الضرورية أو غير اللازمة. Access to unnecessary/unrequired network and file directories shall be blocked.
12-6	استخدام ضوابط الأجهزة الطرفية (Peripheral Device Controls) وحجب الوصول إلى وسائل التخزين القابلة للإزالة مثل الأقراص المتحركة (CD) والأقراص المدمجة (DVD) وذاكرة التخزين (USB). Peripheral device controls shall be used and access to removable media, such as CDs, DVDs, and USBs, shall be blocked.
13-6	تثبيت برامج أنظمة البريد الإلكتروني على خوادم استضافة مخصصة لها. Email systems software shall be installed on dedicated hosts.
14-6	ضبط رسائل خدمة برتوكولات نقل البريد (مثل: بروتوكول إرسال البريد البسيط "SMTP"، وبروتوكول مكتب البريد "POP"، وبروتوكول الوصول إلى رسائل الإنترنت "IMAP"، وغيرها) لمنع الكشف عن معلومات إصدار البرنامج أو نظام التشغيل (Exchange Version). The service banners of mail transport protocols (such as SMTP, POP, IMAP, etc.) shall be configured to prevent software/protocol version disclosure (Exchange version).
15-6	تفعيل أوامر البريد غير الخطرة فقط وذلك لتفادي الأوامر الخطرة مثل (VRFY وEXPN).

Safe email commands shall only be enabled to avoid risky email commands (such as VRFY and EXPN).	
تفعيل سجلات الأحداث (Event Logging) في أنظمة البريد الإلكتروني وسجل التدقيق (Audit Log) الواجب إرسالهما إلى نظام مركزي لإدارة سجلات الأحداث وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني في جامعة حائل. Email systems event logging and audit log to be forwarded to a centralized event logging system shall be configured as per Hail university's Cybersecurity Event Logs and Monitoring Management Policy and Standard.	16-6
إنشاء البنية التحتية لخدمة البريد الإلكتروني باستخدام مبدأ المعمارية متعددة المستويات (Multi-Tier Architecture) المحمية باستخدام طبقتين مختلفتين من جدار الحماية (Firewalls). وتحديداً، إدراج بوابة أمن البريد الإلكتروني (Mail Gateway) في منطقة الإنترنت المحايدة (DMZ)، وخوادم تطبيقات البريد الإلكتروني في منطقة الإنتاج (Production Zone)، وخوادم قواعد بيانات البريد الإلكتروني في المنطقة الموثوقة (Trusted Zone) أو منطقة قاعدة البيانات (Database Zone). A Multi-Tier architecture protected by a dual layer of firewalls shall be applied when creating the email service infrastructure, specifically, **Mail Gateway** in the Internet DMZ, **Email Application Servers** in the Production Zone, and **Email Database Servers** in the Trusted or Database zone.	17-6
حماية صفحة موقع البريد الإلكتروني خلف جدار حماية تطبيق الويب (Web Application Firewall "WAF"). The webmail page shall be protected behind a web application firewall (WAF).	18-6
تعطيل خاصية الترحيل المفتوح (Open Mail Relay). Open Mail Relay feature shall be disabled.	19-6
ضبط تشفير نقل البريد الإلكتروني باستخدام تقنيات التشفير، مثل: «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية رسائل البريد الإلكتروني خلال إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suites) المُوصى بها (مثل التشفير بمجموعة Suite B). يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة حائل. Email transport encryption shall be configured using encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), to protect emails during transmission. Recommended next generation encryption protocols and cipher	20-6

	suites (such as cipher suite B) should be used. Refer to Hail university's Cryptography Standard.
21-6	ضبط مجموعات مواصفات الارتداد لبيانات البريد (Mail Bounce Profiles)، على سبيل المثال: • الارتداد القوي لرسائل البريد الإلكتروني المرسلة إلى عناوين بريد غير موجودة أو منتهية الصلاحية أو غير مفعّلة. Mail bounce profiles shall be configured, for example: • **Hard Bounce** for emails sent to non-existing users or expired/disabled email addresses.
7	برنامج قارئ البريد الإلكتروني (Email Client Security)
الهدف	ضمان حماية استخدام البريد الإلكتروني من خلال صفحة موقع البريد الإلكتروني (Webmail) أو برنامج قارئ البريد الإلكتروني (Email Client).
المخاطر المحتملة	من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية برنامج قارئ البريد الإلكتروني إلى مخاطر كبيرة قد تؤدي إلى سرقة المعلومات وانتحال الشخصيات مما يتيح استخدامها في تنفيذ المزيد من الهجمات الضارة ضد موظفي جامعة حائل وبنيتها التحتية.
الإجراءات المطلوبة	
1-7	استخدام برنامج قارئ بريد إلكتروني مرخص وموثوق. Only fully supported and up-to-date email clients shall be used.
2-7	منع تشغيل صفحة موقع البريد الإلكتروني على المتصفحات غير المرخصة. Running the webmail on unsupported browsers shall be prohibited.
3-7	تعطيل التطبيقات الإضافية أو المكونات غير الضرورية أو غير المسموح بها لبرنامج قارئ البريد الإلكتروني. Unnecessary or not whitelisted email client plug-ins or add-ons applications shall be disabled.
4-7	منع تشغيل لغات البرمجة النصية في برنامج قارئ البريد الإلكتروني. Running scripting languages in email clients shall be prohibited.
5-7	ضبط تكامل برنامج قارئ البريد الإلكتروني مع أنظمة حماية الأجهزة كمضاد الفيروسات والبرمجيات الضارة. Email clients shall be integrated with endpoint security products (e.g., AV and Malware).
8	النسخ الاحتياطية والأرشفة (Backup and Archival)

الهدف	ضمان سلامة بيانات البريد الإلكتروني وتوافرها وقابلية استعادتها وحمايتها من فقدانها أو تخريبها.
المخاطر المحتملة	في حال حذف بيانات البريد الإلكتروني والرسائل الإلكترونية أو العبث بها أو فقدانها بالخطأ أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن جامعة حائل من استرداد بيانات بريدها الإلكتروني وسجل اتصالاتها مما يؤثّر على أنشطة أعمالها الاعتيادية.
الإجراءات المطلوبة	
1-8	إجراء عمليات نسخ احتياطية دورية كاملة لخوادم وقواعد بيانات البريد الإلكتروني وفقاً لسياسة إدارة النسخ الاحتياطية، ويشمل ذلك النسخ الاحتياطية لأنظمة تشغيل الخوادم وإعدادات تطبيق البريد وقاعدة البيانات بالإضافة إلى مجمل قواعد البيانات وصناديق البريد، وإضافة ترتيب تسلسلي للنسخ الاحتياطية لنظام البريد الإلكتروني ومحتويات البريد الخاصة بـجامعة حائل وتسجيل وقتها وتاريخها وجدولتها. Full backups for the email systems and underlying infrastructure shall be performed as per Hail university's Backup and Recovery Management Policy. The backups must include at a minimum email servers and email databases, including servers' operating system backup, email application configuration backup, database configuration backup, databases and mailboxes. Additionally, Hail university's email system and mailbox backups shall be serialized, time-dated and indexed.
2-8	إجراء عملية نسخ احتياطي إضافية يومياً أو وفقاً لسياسة إدارة النسخ الاحتياطية لمحتويات بريد المستخدمين. Incremental backup for user mailboxes shall be performed daily or as per Hail university's Backup and Recovery Management Policy.
3-8	تشفير النسخ الاحتياطية لنظام البريد الإلكتروني ومحتويات البريد وفقاً لسياسة التشفير المعتمدة في جامعة حائل. Hail university's email system and mailbox backups shall be encrypted.
4-8	تخزين النسخ الاحتياطية لنظام البريد الإلكتروني ومحتويات البريد الخاصة بـجامعة حائل في موقعين محميّين منفصلين على الأقل وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة حائل. Hail university's email system and mailbox backups shall be stored in, at least, two geographically distinct protected off-sites.
5-8	تطبيق إجراءات توثيق وسلامة (Integrity Verification) النسخ الاحتياطية لضمان نسخ بيانات البريد الإلكتروني أو أرشفتها بطريقة صحيحة.

Backup and integrity verification mechanisms shall be employed to ensure that email data is being correctly backed up or archived.	
تجربة استعادة جميع أنواع النسخ الاحتياطية دورياً لضمان سلامة عملية النسخ الاحتياطي وفقاً لسياسة إدارة النسخ الاحتياطية. Backup recovery shall be regularly tested to verify the safety of the backup process as per Hail university's Backup and Recovery Management Policy.	6-8

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الامن السيبراني.

2- **مراجعة المعيار وتحديثه:** إدارة الامن السيبراني.

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الالكتروني.

جامعة حائل
University of Ha'il

نموذج معيار أمن أجهزة المستخدمين

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة أجهزة المستخدمين (Workstations) الخاصة بـجامعه حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة عن الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أجهزة المستخدمين المكتبية الخاصة بـجامعه حائل وينطبق على جميع العاملين في جامعه حائل

المعايير

1	الوصول الآمن (Secure Access)
الهدف	ضمان حماية أجهزة المستخدمين ووظائفها من الوصول غير المصرح به.
المخاطر المحتملة	ينطوي على الوصول غير المصرّح به إلى أجهزة المستخدمين مخاطر كبيرة قد تؤدي إلى سرقة المعلومات ووقوع انتهاكات أمنية تُمكن منفذيها من شن المزيد من الهجمات الضارة ضد موظفي جامعه حائل وبنيتها التحتية أو ضد أي هدف خارجي آخر.
الإجراءات المطلوبة	
1-1	تقييد الوصول إلى أجهزة المستخدمين وحصره على حساب المستخدم للجهاز. Access to workstations shall be limited to the accounts of the individual users of the workstations only.
2-1	تطبيق مبدأ الحد الأدنى من الصلاحيات والامتيازات عند منح الصلاحيات على أجهزة المستخدمين. Least Privilege principle shall be applied to provide access to users' workstations.
3-1	إلغاء أو إعادة تسمية الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة.

	Default/non-interactive/unneeded accounts shall be disabled or renamed.
4-1	إلى جانب استخدام تركيبة اسم المستخدم/كلمة المرور، إلزام المستخدم باستخدام آليات المصادقة أو التحقّق من الهوية متعدّد العناصر (MFA)، مثل الخصائص الحيوية والمفاتيح المادية وكلمات المرور المؤقتة والبطاقات الذكية وشهادات التشفير وغيرها، على أجهزة المستخدمين في البيئات فائقة الحماية مثل مركز العمليات الأمنية (SOC). In addition to a user/password combination, users shall be required to use other authentication mechanisms or Multi-Factor Authentication (MFA), such as biometrics, hardware keys, one-time passwords, smart cards, certificates, etc., on workstations of highly protected environment, such as Security Operations Center (SOC).
5-1	إعداد متطلبات تعقيد كلمة المرور الخاصة بجهاز المستخدم وفقاً لسياسة إدارة هويات الدخول والصلاحيات في جامعه حائل Workstation password complexity requirements shall be configured in accordance with Hail University's Identity and Access Management Policy.
6-1	ضبط وإعداد حد الإغلاق بعد عدد معين من محاولات تسجيل الدخول غير الناجحة وانتهاء وقت الجلسة وتسجيل الخروج في حال عدم الاستخدام بالنسبة لحالات الوصول المحلية والوصول إلى النطاقات وفقاً لسياسة إدارة هويات الدخول والصلاحيات في جامعه حائل Login attempts lockout, session timeout and session idle logout for local access and domain access shall be configured in accordance with Hail University's Identity and Access Management Policy.
7-1	ضبط وإعداد كلمات مرور مُحمِّل التشغيل (Bootloader) لنظام الإدخال/الإخراج الأساسي (BIOS). BIOS bootloader passwords shall be configured.
2	مراجعة الإعدادات والتحصين (Secure Hardening Configuration)
الهدف	تحديد متطلبات الأمن الأساسية لأجهزة المستخدمين لضمان تصميم أجهزة المستخدمين وإعدادها وتشغيلها بطريقة آمنة.

المخاطر المحتملة	يمكن أن يؤدي الإعداد الخاطئ والتصميم غير الآمن لأجهزة المستخدمين إلى ثغرات أمنية يمكن استغلالها لتهديد سرية وسلامة وتوافر بيانات جامعه حائل وسير عملها.
الإجراءات المطلوبة	
1-2	إجراء اختبارات أمنية منتظمة (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في جامعه حائل Regular security testing (such as vulnerability assessments and penetration testing) shall be conducted in accordance with Hail University's Vulnerability Management Policy.
2-2	إجراء التحديثات والإصلاحات على أجهزة المستخدمين بانتظام وفقاً لسياسة أمن أجهزة المستخدمين وسياسة إدارة التحديثات والإصلاحات في جامعه حائل لضمان تحديث جميع أنظمة التشغيل وبرمجيات التطبيقات على أجهزة المستخدمين. Workstations shall be regularly patched and updated in accordance with Hail University's Workstation Security Policy and Patch Management Policy to ensure that all workstation Operating Systems (OS) and application software are up-to-date.
3-2	حذف التطبيقات والخدمات غير الضرورية أو غير اللازمة أو إلغاء تفعيلها على أجهزة المستخدمين مثل بروتوكول تل نت (Telnet)، ولوحة المفاتيح باللمس، والسجل عن بعد (إذا لم يكن ضرورياً)، وغيرها. Unnecessary/unrequired applications and services, such as Telnet Protocol, touch keyboard, remote registry (if not needed), etc., shall be removed/disabled on workstations.
4-2	حذف/تعطيل خصائص نظام التشغيل والتطبيق وملفات الإعدادات غير الضرورية أو غير اللازمة أو إلغاء تفعيلها. Unnecessary/unrequired OS and application features and configuration files shall be removed/disabled.
5-2	حجب إمكانية الوصول إلى أدلة الشبكة والملفات غير الضرورية أو غير اللازمة. Access to unnecessary/unrequired network and file directories shall be blocked.
6-2	استخدام الضوابط المادية وحظر الوصول إلى الوسائط القابلة للإزالة عند الضرورة أو وفقاً لسياسة الاستخدام المقبول في جامعه حائل

	Hardware controls shall be used and access to removable media shall be blocked where necessary or as per Hail University's Acceptable Usage Policy.
7-2	تطبيق الإعدادات والتحصين لأجهزة المستخدمين بما في ذلك التحصين على مستوى البرمجيات وأنظمة التشغيل وفقاً لسياسة الإعدادات والتحصين في جامعه حائل Workstation configuration hardening, including software and operating system level hardening, shall be implemented in accordance with Hail University's Secure Configuration and Hardening Policy.
8-2	إنشاء نسخ وقوالب آمنة لأجهزة المستخدمين بناءً على معايير الإعدادات المعتمدة ووفقاً لسياسة الإعدادات والتحصين في جامعه حائل وإعادة نسخ الأجهزة باستخدام أحد قوالب نسخ أجهزة المستخدمين في حال تعرضها لانتهاك أمني. Secure workstation images or templates shall be created for all workstations based on the approved configuration standards and as per Hail University's Secure Configuration and Hardening Policy. Compromised workstations shall be reimaged using one of the workstation image templates.
9-2	تخزين نسخ أجهزة المستخدمين في بيئة آمنة على نسخ احتياطية أو بيئة تخزين معدة بصورة آمنة وغير مرتبطة بالشبكة والتحقق بانتظام من هذه النسخ باستخدام أدوات مراقبة سلامة المعلومات. Workstation images shall be stored in a secure environment on securely configured offline backups or storage environment, and they shall be validated regularly using integrity monitoring tools.
3	النسخ الاحتياطي والأرشفة (Backup and Archiving)
الهدف	ضمان سلامة بيانات أجهزة المستخدمين من العبث بها أو فقدانها بالخطأ أو تخريبها والتأكد من توافرها وإمكانية استعادتها.
المخاطر المحتملة	في حال حذف بيانات أجهزة المستخدمين بالخطأ أو العبث بها أو فقدانها أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن جامعه حائل من استعادة البيانات، مما سيؤثّر في أنشطة أعمالها الاعتيادية.
الإجراءات المطلوبة	

1-3	عمل نسخ احتياطية كاملة وتزايدية لأجهزة المستخدمين وفقاً لسياسة إدارة النسخ الاحتياطي المعتمدة في جامعه حائل ويجب أن تشمل النسخ الاحتياطية على الأقل نسخاً احتياطية لنظام تشغيل أجهزة المستخدمين، ونسخاً احتياطية لإعدادات البرمجيات، ونسخاً احتياطية للبيانات. Full and incremental backup of workstations shall be performed in accordance with Hail University's Backup and Recovery Management Policy. The backups must include, at minimum, workstations operating system backups, software configuration backups, and data backups.
2-3	تخزين النسخ الاحتياطية لثلاث فترات متتالية بما في ذلك الفترة الحالية. فعلى سبيل المثال، إذا تم عمل النسخ الاحتياطية شهرياً، يجب تخزين النسخ الاحتياطية للشهر الحالي ولشهرين سابقين فقط. Three generations of backups shall be stored including the backups for the current period. For example, if backup is performed monthly, backups of the current month and the two previous months shall be stored only.
3-3	تشفير النسخ الاحتياطية لأجهزة المستخدمين الخاصة بـجامعه حائل Hail University's workstation backups shall be encrypted.
4-3	ترتيب النسخ الاحتياطية الخاصة بأجهزة مستخدمي جامعه حائلتسلسلياً وتسجيل وقتها وتاريخها وجدولتها. Hail University's workstation backups shall be serialized, time-dated and indexed.
5-3	اختبار إمكانية استرجاع النسخة الاحتياطية كل ثلاثة أشهر وفقاً لسياسة إدارة النسخ الاحتياطي المعتمدة في جامعه حائل Backup recovery shall be tested every quarter or as per Hail University's Backup and Recovery Management Policy.
6-3	تطبيق آليات توثيق النسخ الاحتياطي وسلامتها لضمان نسخ بيانات أجهزة المستخدمين أو أرشفتها بطريقة صحيحة. Backup verification and integrity mechanisms shall be employed to ensure that data is being correctly backed up or archived.

4	برمجيات حماية الأجهزة الطرفية (Endpoint Protection Software)
الهدف	ضمان حماية أجهزة المستخدمين من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقاً وأي نوع آخر من الهجمات الخبيثة.
المخاطر المحتملة	يمكن أن تؤدي الهجمات الخبيثة الناجحة على أجهزة المستخدمين إلى تعريض جامعه حائل لاختراق أمني أو الوصول غير المصرح به أو الكشف عن بياناتها في حال تركت أجهزة المستخدمين دون حماية.
الإجراءات المطلوبة	
1-4	ضبط وإعداد حد إغلاق نظام التشغيل ووظائف التطبيقات عن طريق الحد الأدنى من الصلاحيات والامتيازات المطلوبة للتشغيل في الظروف الاعتيادية، مثل إلغاء تفعيل تغيير وقت النظام يدوياً، وتعديل ملفات النظام، وإنشاء الملفات أو تعديلها أو حذفها، وغيره. OS and application functionality lockout shall be configured with the least privilege required to operate in normal conditions. For example, changing system time manually, editing system files, creating/modifying/deleting files, etc., shall be disabled.
2-4	تطبيق خاصية السماح بقائمة محددة من التطبيقات على أجهزة المستخدمين لتمكين عمل تطبيقات وبرمجيات محددة فقط وفقاً للحاجة. Application whitelisting shall be implemented on workstations to allow only specific applications and software to run based on need.
3-4	تطبيق خاصية السماح بقائمة محددة من التطبيقات لاستخدام خاصيتين لتحديد التطبيق، بما في ذلك على سبيل المثال وليس الحصر، قواعد التجزئة المشفرة أو قواعد شهادات الناشر أو قواعد المسار للسماح باستخدام التطبيقات أو منعها. Application whitelisting shall be implemented to use two features of identifying the application, including but not limited to cryptographic hash rules, publisher certificate rules or path rules to allow or restrict the use of applications.
4-4	ضبط إعدادات أنظمة السماح بقائمة محددة من التطبيقات بحيث لا يمكن للمستخدمين إلغاء تفعيل الأنظمة باستثناء المديرين عند أدائهم لمهام إدارية معينة تقتضي إلغاء تفعيل السماح بقائمة محددة من التطبيقات مؤقتاً.

Application whitelisting agents shall be configured so that users cannot disable the agents with the exception of administrators when performing specific administrative tasks that require disabling application whitelisting temporarily.	
فيما يخص خاصية السماح بقائمة محددة من التطبيقات، يجب تعريف الملفات التنفيذية المعتمدة (exe, com, pif, وغيرها) ومكتبات البرمجيات (dll, ocx, وغيرها) والنصوص (ps1, bat, vbs, وغيرها) وبرامج التثبيت (msi, msp, وغيرها) من أجل تنفيذ الملفات من القائمة المعتمدة فقط. For application whitelisting, a list of approved executable files (exe, com, pif, etc.), software libraries (dll, ocx, etc.), scripts (ps1, bat, vbs, etc.), and installers (msi, msp, etc.) shall be defined to allow files from the approved list to be executed only.	5-4
تطبيق نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Prevention System "HIPS") على جميع أجهزة المستخدمين. Host-based Intrusion Prevention System (HIPS) shall be implemented on all workstations.	6-4
تطبيق جدار حماية من البرمجيات المستضافة على جميع أجهزة المستخدمين. Software host firewall shall be implemented on all workstations.	7-4
تطبيق برامج مكافحة الفيروسات على جميع أجهزة المستخدمين. Antivirus shall be implemented on all workstations.	8-4
تطبيق برامج مكافحة البرامج الضارة على جميع أجهزة المستخدمين. Antimalware shall be implemented on all workstations.	9-4
تطبيق برامج الحماية من التهديدات المتقدمة المستمرة (APT) على جميع أجهزة المستخدمين. Host Advanced Persistent Threat (APT) agents shall be implemented on all workstations.	10-4

11-4	تطبيق برامج اكتشاف أجهزة النهاية الطرفية والاستجابة لها على جميع أجهزة المستخدمين. Endpoint Detection and Response shall be implemented on all workstations.
12-4	تطبيق برمجيات التحكم بأجهزة النهاية الطرفية على كافة أجهزة المستخدمين لمنع أي دخول من أجهزة خارجية غير مصرحة. Endpoint Device Control software shall be implemented on all workstations to prevent the use of unauthorized peripheral devices.
13-4	تطبيق منع تسّرب البيانات (DLP) حيثما كان ذلك لازماً وفقاً للسياسات والإجراءات ذات العلاقة في جامعه حائل Data Leakage Prevention (DLP) shall be implemented where deemed necessary by Hail University's relevant policies and procedures.
5	تسجيل الأحداث وسجل التدقيق (Event and Audit Logging)
الهدف	التأكّد من توثيق وتسجيل الأحداث الأمنية والأنشطة غير المصرّح بها التي تشهدها أجهزة المستخدمين.
المخاطر المحتملة	قد يؤدي عدم تفعيل وتسجيل الأحداث الأساسية التي تُنفذ في أجهزة المستخدمين والتي حدّدتها متطلّبات الضابط إلى صعوبة اكتشاف ومنع الهجمات السيبرانية، أو إساءة استخدام الصلاحيات الهامة والحساسة، مما قد يؤثّر على أعمال جامعه حائل
الإجراءات المطلوبة	
1-5	ضبط وإعداد سجل أجهزة المستخدمين وسجل التدقيق ليتم ترحيلهما إلى نظام تسجيل مركزي وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني في جامعه حائل Workstation logging and audit trail shall be configured to be forwarded to a centralized logging system as per Hail University's Cybersecurity Event Logs and Monitoring Management Policy and Standard.
2-5	إعداد أجهزة المستخدمين ليتزامن توقيتها مع توقيت ثلاثة أجهزة تزامن مركزية على الأقل مما يسمح بتزامن توقيت سجلات الأحداث.

	Workstations shall be configured to synchronize clock to at least three redundant central time workstations to ensure that timestamps in logs are consistent.
3-5	ضبط إعدادات أجهزة المستخدمين وذلك بحفظ سجلات الأحداث المحلية، وسجلات التدقيق والسجلات الأمنية، بحيث تشمل جميع مستويات السجلات. Local logging, as well as audit trail and security logs, shall be configured with all levels of logging.
6	التشفير (Cryptography)
الهدف	ضمان الحفاظ على سريّة بيانات المستخدمين والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.
المخاطر المحتملة	قد يؤدي عدم وجود التقنيات الأمنية المناسبة لضمان تشفير بيانات أجهزة المستخدمين إلى تعرض بيانات جامعه حائل لمخاطر سيبرانية عالية نتيجة الوصول غير المصرح به إلى هذه البيانات.
الإجراءات المطلوبة	
1-6	تطبيق تقنيات التشفير مثل أمن طبقة النقل (TLS) والشبكات الخاصة الافتراضية (VPN) لحماية آليات التحقّق من الهوية أثناء إرسال الرسائل، واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) المُوصى بها. للمزيد من التفاصيل، يُرجى الرجوع إلى معيار التشفير المعتمد في جامعه حائل Encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Network (VPN), shall be implemented to protect authentication mechanisms during transmission. In addition, recommended next generation encryption protocols and cipher suites shall be used. For more details, refer to Hail University's Cryptography Standard.
2-6	تشفير وسائط التخزين في أجهزة المستخدمين بما في ذلك الأقراص الصلبة حيثما كان ذلك ضرورياً وفقاً للسياسات والإجراءات ذات العلاقة في جامعه حائل Workstations storage media, including hard disks, shall be encrypted where deemed necessary by Hail University's relevant policies and procedures.
3-6	استخدام بروتوكول إدارة أجهزة المستخدمين الذي يدعم التشفير أو يقوم بضبط إعدادات التشفير لبروتوكولات إدارة أجهزة المستخدمين مثل: بروتوكول النفاذ إلى الدليل البسيط

	(LDAP) على أمن طبقة النقل (TLS)، والنسخة الثالثة من بروتوكول إدارة الشبكة البسيط (SNMPv3) لغايات المصادقة والخصوصية، وبروتوكول كيربيروس (Kerberos) مع أمن طبقة النقل (TLS)، وسجل النظام المشفر، وغيرها. Workstation management protocol that supports or configures encryption for workstation management protocols, such as LDAP over TLS, SNMPv3 with authentication and privacy, Kerberos with TLS, encrypted syslog, etc., shall be used.
7	الإدارة المركزية (Central Management)
الهدف	تحديد المتطلبات الأمنية لإدارة أجهزة المستخدمين لضمان تشغيل أجهزة المستخدمين وإداراتها مركزياً وبطريقة آمنة وضمان تطبيق جميع المتطلبات الأمنية وتنفيذها.
المخاطر المحتملة	يؤدي الافتقار إلى الإدارة الآمنة وعدم تطبيق المتطلبات الأمنية على أجهزة المستخدمين إلى زيادة احتمالية التعرض للهجمات، ويزيد من فرص وجود ثغرات ونقاط ضعف في بيئة جامعه حائل يمكن استغلالها في الهجمات أو الاختراقات الخبيثة، مما يعرض أجهزة المستخدمين والبيانات في جامعه حائل إلى انتهاكات أمنية.
الإجراءات المطلوبة	
1-7	ضبط إعدادات خادم الإدارة المركزية أو خادم النطاق ليطبق سياسة أمن الخوادم في جامعه حائلعلى جميع أجهزة المستخدمين. The central management server or domain server shall be configured to enforce Hail University‘s policies on all workstations.
2-7	تثبيت أدوات إدارة إعدادات النظام التي تنفذ إعدادات الضبط والتهيئة لأجهزة المستخدمين وتعيد تثبيتها تلقائياً في فترات زمنية محددة ومنتظمة. للمزيد من التفاصيل، يرجى الرجوع إلى سياسة الإعدادات والتحصين في جامعه حائل System configuration management tools that automatically enforce and redeploy configuration settings to workstations at regularly scheduled intervals shall be deployed. For more details, refer to the Hail University‘s Secure Configuration and Hardening Policy.
3-7	تطبيق نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة محتوى الأمن (Security Content Automation Protocol "SCAP") للتأكد من عناصر الإعدادات الأمنية كافة وجدولة الاستثناءات المعتمدة والإبلاغ عن حدوث أي تغييرات غير مصرّح بها.

	A Security Content Automation Protocol (SCAP) compliant configuration monitoring system shall be implemented to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.
8	أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (Privileged Access Workstations “PAW”)
الهدف	تحديد المتطلبات الأمنية الإضافية لحماية أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs) المستخدمة في الوصول إلى الأنظمة ومناطق الشبكة الهامة.
المخاطر المحتملة	يمكن أن تؤدي الهجمات الخبيثة الناجحة على أجهزة المستخدمين ذات الصلاحيات الهامة والحساسة إلى تعريض جامعه حائل لاختراقات خطيرة وانتهاكات أمنية لأهم أصولها الحساسة مما يؤدي إلى أضرار جسيمة.
الإجراءات المطلوبة	
1-8	فرض استخدام التحقّق من الهوية متعدّد العناصر من أجل الوصول إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) التي يستخدمها مديرو النظام. Use of multi-factor authentication shall be required for accessing PAWs used by system administrators.
2-8	تقييد الوصول إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) وحصره على المشرفين والمشغلين المصرح لهم فقط. Access to PAWs shall be restricted to only authorized administrators and operators.
3-8	وضع أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) في منطقة الإدارة في الشبكة. PAWs shall be placed in the network management zone.
4-8	تشفير جميع أنواع الحركة المنقولة من أو إلى أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW) بما في ذلك حركة الوصول الإداري والتحكم (مثل بروتوكول النقل الآمن "SSH"، وبروتوكول التحكم بسطح المكتب عن بعد "RDP")، وحركة البيانات باستخدام آليات التشفير (مثل أمن طبقة النقل "TLS") وفقاً لمعيار التشفير المعتمد في جامعه حائل All traffic transmitted to or out of PAWs, including administrative access and control traffic (such as Secure Shell

	“SSH” and Remote Desktop Protocol “RDP”), and data traffic using cryptographic mechanisms (such as Transport Layer Security “TLS”), shall be encrypted as per Hail University’s Cryptography Standard.
5-8	إلغاء تفعيل خاصية الوصول إلى الإنترنت على أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW). Internet access on PAWs shall be disabled.
6-8	إلغاء تفعيل الخدمات الخطرة وغير اللازمة (مثل إرسال رسائل البريد الإلكتروني واستلامها) على أجهزة المستخدمين ذات الصلاحيات والامتيازات الهامة والحساسة (PAW). Unnecessary and risky services (such as sending and receiving emails) shall be disabled on PAWs.
7-8	تفعيل جميع مستويات التسجيل، إلى جانب سجل التدقيق والسجلات الأمنية، محلياً وعلى نظام تسجيل أحداث مركزي. All levels of logging, as well as audit trail and security logs, shall be enabled locally and to a centralized event logging system.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني

2- **مراجعة المعيار وتحديثه:** أدارة الأمن السيبراني

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الألكتروني

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعه حائل بهذا المعيار دورياً.

2- يجب على كافة العاملين في جامعه حائل الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعه حائل

جامعة حائل
University of Ha'il

نموذج معيار أمن الأجهزة المحمولة

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

يهدف هذا المعيار إلى توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر الناتجة عن استخدام أجهزة جامعه حائل المحمولة (Mobile Devices) والأجهزة الشخصية للعاملين (مبدأ "Bring Your Own Device "BYOD) وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

يتبع هذا المعيار المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهو متطلب تشريعي في الضابط رقم ١-٣-٣ والضابط رقم ٢-٦-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل

يغطي هذا المعيار أنظمة إدارة الأجهزة المحمولة في جامعه حائل ، وينطبق على الأجهزة المحمولة (Devices Mobile) الخاصة بـجامعه حائل والأجهزة الشخصية للعاملين (BYOD).

المعايير

1	منع الوصول إلى الجهاز (Device Access Locking)
الهدف	ضمان عدم وصول المستخدمين غير المصرّح لهم إلى الأجهزة غير المراقبة و/أو المفقودة و/أو المسروقة.
المخاطر المحتملة	في حال منح حق وصول غير مصرّح به إلى جهاز محمول تملكه جامعه حائل ويحتوي على بيانات خاصة بـجامعه حائل أو منح صلاحيات هامة للدخول إلى بيئة تقنية المعلومات الخاصة بـجامعه حائل فقد يؤثّر أي اختراق محتمل متعلّق بالعمل في الإدارة حسب شدّة الحادث.
الإجراءات المطلوبة	
1-1	إعداد رموز مرور (Passcodes) معقّدة لقفل الأجهزة. ويُنصَح بشدة عدم استخدام رموز المرور السهلة المكوّنة من أحرف أو أرقام متتالية أو متسلسلة (مثل: 0000، أو 1234، أو 9876)، كما يُنصَح باستخدام رموز مرور مكوّنة من مجموعات إضافية من الأحرف أو الأرقام أو استخدام رموز مرور طويلة. Passcodes consisting of complex characters shall be set up. Simple passcodes consisting of consecutive or sequential characters) e.g., 0000, 1234, 9876, etc.) are strongly discouraged. Passcodes consisting of additional character sets or greater lengths are recommended.

2-1	إضافة عنصر تحقّق (Factor of Authentication) آخر لقفل الجهاز (كاستخدام تقنية التعرّف على الوجه، أو نمط التمرير السريع على الشاشة "Swiping Pattern"، أو بصمة الأصبع، وغيرها) إن سمحت خصائص الجهاز المحمول بذلك. If the mobile device allows for it, an additional factor of authentication to lock the device (e.g., facial recognition, swiping pattern, fingerprint, etc.) shall be implemented.
3-1	تغيير رمز المرور لقفل الجهاز المحمول دورياً، أو كل ثلاثة أشهر على الأقل. The passcode for the mobile device shall be changed periodically or at least every three months.
4-1	منع المستخدمين من تعديل أو إلغاء آلية القفل الآمن للجهاز. Users shall be prohibited from modifying or disabling security locking mechanisms.
5-1	يجب ضبط آليات القفل التلقائي للجهاز عندما لا يكون الجهاز قيد الاستعمال لمدة لا تزيد عن 90 ثانية أو وفقًا لمتطلبات جامعه حائل The device auto-lock mechanism shall be set to lock the device when it is idle and not being used for no more than 90 seconds or as per Hail University's requirements.
2	سلامة المعلومات المخزنة في الجهاز المحمول (Device Contents Integrity)
الهدف	تطبيق آلية قياسية لمنع إجراء تعديلات غير مقصودة أو ضارة على محتويات البيانات المُخزّنة في الجهاز.
المخاطر المحتملة	في حال تعرّض البيانات المُخزّنة في الجهاز للعبث أو التلف أو التعديل، فإنه لا يمكن اعتبار الجهاز بعد ذلك من الأصول الموثوقة التي يُسمَح باستخدامها داخل بيئة تقنية المعلومات الخاصة بجامعه حائل
الإجراءات المطلوبة	
1-2	تفعيل التشفير الكامل لمحتويات الجهاز إن كان الجهاز المحمول يدعم هذا الخيار. If the mobile device supports it, full device contents encryption shall be enabled.
2-2	تفعيل وتطبيق خاصية فصل البيانات بين المعلومات الشخصية والبيانات الخاصة بجامعه حائل وذلك في الأجهزة الشخصية للعاملين (مبدأ BYOD) إن كانت تدعم هذه الخاصية. كما يجب تشفير البيانات بعد فصلها.

If supported by personal mobile devices (BYOD), data segregation between personal information and data owned by the Hail University shall be enabled and enforced. Additionally, segregated data shall be encrypted.	
ضبط وإعداد كلمات مرور مُحمِّل التشغيل (Bootloader) لنظام الإدخال/الإخراج الأساسي (BIOS). BIOS bootloader passwords shall be configured.	3-2
تفعيل إغلاق «مُحمِّل تشغيل» (Bootloader) إن كان الجهاز المحمول يدعم هذا الخيار. If the mobile device supports it, locking Bootloader shall be enabled.	4-2
ضبط وتطبيق التشفير على أي من وسائط التخزين القابلة للإزالة (مثل: بطاقات التخزين الآمنة "SD Cards" أو وسائط التخزين الخارجية "USB") التي تصل إليها الأجهزة المحمولة. Encryption shall be configured and enforced on any removable storage (e.g., SD cards or USB) that can be accessed by mobile devices.	5-2
ضبط إعدادات الجهاز لإجراء قفل تلقائي بعد القيام بخمس محاولات خاطئة لإدخال رمز المرور، وإجراء مسح تلقائي للبيانات بعد القيام بعشر محاولات خاطئة لإدخال رمز المرور أو وفقاً لعدد المحاولات التي يدعمها نظام تشغيل الجهاز. The device shall be set up to perform automatic lockout after five failed passcode entry attempts, and to perform data wiping after ten failed passcode entry attempts or as supported by the device operating system.	6-2
تفعيل إمكانية مسح البيانات عن بُعد من الأجهزة المفقودة أو المسروقة. Wiping data remotely from lost/stolen devices shall be enabled.	7-2
منع المستخدمين من تعديل أو إلغاء آلية إغلاق «مُحمِّل التشغيل» (Bootloader). Modifying or disabling Bootloader locking by users shall be prohibited.	8-2

9-2	منع إجراء أي عمليات تجاوز القيود التي تفرضها الشركات المصنّعة للجهاز (مثل Rooting أو Jailbreaking) على أي جهاز محمول، ومنع استخدام الأجهزة التي تم إجراء هاتين العمليتين عليها داخل بيئة تقنية المعلومات الخاصة بـجامعه حائل Rooting or jailbreaking a mobile device shall be prohibited, and the use of rooted or jailbroken devices within Hail University's IT environment shall also be prohibited.
3	أمن نظام تشغيل وتطبيقات الجهاز (Device OS and Applications Security)
الهدف	ضمان تحديث وضبط نظام التشغيل والتطبيقات المثبّتة في الجهاز المحمول بطريقة مناسبة قبل استخدامه.
المخاطر المحتملة	عدم الكشف عن استخدام التطبيقات غير المصرّح بها أو الملغيّة أو غير المزوّدة بالتحديثات والإصلاحات أو البرمجيات الضارة سيمنع جامعه حائل من مراقبة الاستخدام الآمن للأجهزة المحمولة.
الإجراءات المطلوبة	
1-3	إتاحة تثبيت التطبيقات المقدّمة فقط من المتاجر المعتمدة الخاصة بالمورّد أو الجهة. Application installation shall be allowed only from Vendor/Entity approved stores.
2-3	تقييد الأذونات الممنوحة للتطبيقات المثبّتة على الجهاز المحمول بحيث تُطبّق المبدأ الأساسي القائم على الحدّ الأدنى من الصلاحيات. The permissions assigned to applications installed on a mobile device shall be restricted, and the principle of Least Privilege shall be applied.
3-3	تعطيل الكاميرا والميكروفون بشكل افتراضي وتحديد التطبيقات المصرح لها باستخدامها حسب حاجة العمل. Camera and Microphone shall be disabled by default and access to them should be allowed based on need.
4-3	التأكّد من التواقيع الرقمية للتطبيقات قبل تثبيتها. Application digital signatures shall be verified before installation.
5-3	التأكّد من تزويد الجهاز المحمول بأحدث نسخة رسمية من إصدار/نسخة نظام التشغيل من خلال مورّد الجهاز. وإذا تعذّر تزويد أي جهاز بنسخة أحدث من نظام التشغيل، وتوقّف المورّد عن تقديم حزم الإصلاحات والتحديثات الأمنية للجهاز في العامين الماضيين، يجب عندها التوقف عن استخدام الجهاز واستبداله.

The mobile device shall be updated to last Operating Systems (OS) versions/releases provided by the device vendor. If a device cannot be further updated to a newer OS, and the vendor has not provided security patches for the device in the last two years, the mobile device shall be decommissioned and replaced.	
تطبيق نظام مراقبة الإعدادات المتوافقة مع «بروتوكول أتمتة محتوى الأمن» (Security Content Automation Protocol) لتدقيق عناصر الإعدادات الأمنية كافة والتأكّد منها في الأجهزة المحمولة وجدولة الاستثناءات المعتمدة والإبلاغ عن حدوث أي تغييرات غير مصرّح بها. Security Content Automation Protocol (SCAP) shall be utilized to audit and verify all security configuration elements within the mobile devices, catalog approved exceptions, and report any unauthorized changes.	6-3
منع المستخدمين من تعديل أو إلغاء أي إعدادات أمنية للجهاز المحمول. Users shall not be able to modify or remove any secure configurations on the mobile device.	7-3
تعطيل أو إزالة الحسابات الافتراضية، وتقييد الوصول إلى الحسابات ذات الصلاحية العالية على الأجهزة المحمولة بالتوافق مع سياسة إدارة هويات الوصول والصلاحيات. Disabling or removal of virtual accounts, and limiting access to accounts with high privilege based on Identity and Access Management Policy.	8-3
تطوير المعايير الأمنية الأساسية للأجهزة المحمولة وتنفيذها ومراقبتها دورياً. A Minimum-Security Baseline for mobile devices shall be developed, implemented and regularly monitored.	9-3
إجراء نسخ احتياطي كامل ومنتظم للبيانات المخزنة على الأجهزة المحمولة وفقاً لسياسة النسخ الاحتياطية الخاصة بـجامعه حائل A regular full backup of data stored on the mobile devices shall be performed as per Hail University's Backup Policy.	10-3
إجراء التحديثات والإصلاحات على أجهزة المستخدمين المحمولة بشكل منتظم وفقاً لسياسة أمن أجهزة المستخدمين وسياسة إدارة التحديثات والإصلاحات في جامعه حائل لضمان تحديث جميع أنظمة التشغيل وبرمجيات التطبيقات على أجهزة المستخدمين المحمولة.	11-3

Mobile devices shall be regularly patched and updated as per Hail University's Workstation and Mobile Device Security Policy and Patch Management Policy to ensure that all OS and application software is up-to-date.	
استخدام عناصر التحكم في الأجهزة وحظر الوصول إلى الوسائط القابلة للإزالة عند الضرورة أو وفقاً لسياسة الاستخدام المقبول في جامعه حائل Hardware controls shall be implemented and access to removable media shall be blocked where necessary or as per Hail University's Acceptable Use Policy.	12-3
تثبيت برمجيات التحكم بأجهزة المستخدمين المحمولة على كافة الأجهزة لمنع الاستخدام غير المصرح به لأدوات اتصال الشبكة (Wi-Fi, Bluetooth, etc.) والأجهزة الطرفية. Device control software shall be implemented on all mobile devices to prevent unauthorized use of network communication tools (Wi-Fi, Bluetooth, etc.) or peripheral devices.	13-3
تعطيل كافة خصائص تبادل البيانات أو الملفات مثل (Airdrop, NFC, Bluetooth .etc) Disabling all information and file sharing features such s (Airdrop, NFC, and Bluetooth, etc.).	14-3
تثبيت برمجيات الحماية على أجهزة المستخدمين المحمولة بما في ذلك مضاد الفيروسات، والبرامج التي تسمح لقائمة محددة فقط من التطبيقات، وبرامج منع تسرب المعلومات والبيانات على كافة الأجهزة المحمولة. Protection software including antivirus, antimalware, application whitelisting and data leakage prevention software shall be installed on all mobile devices.	15-3
تطبيق الإعدادات والتحصين لأجهزة المستخدمين بما في ذلك التحصين على مستوى البرمجيات وأنظمة التشغيل وفقاً لسياسة الإعدادات والتحصين في جامعه حائل Workstation configuration hardening, including software and operating system level hardening, shall be implemented in accordance with Hail University's Secure Configuration and Hardening Policy.	16-3

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني بجامعه حائل

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الإلكتروني و إدارة الأمن السيبراني

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني بجامعه حائل ضمان التزام جامعه حائل بهذا المعيار دورياً.

2- يجب على كافة العاملين في جامعه حائل الالتزام بهذا المعيار.

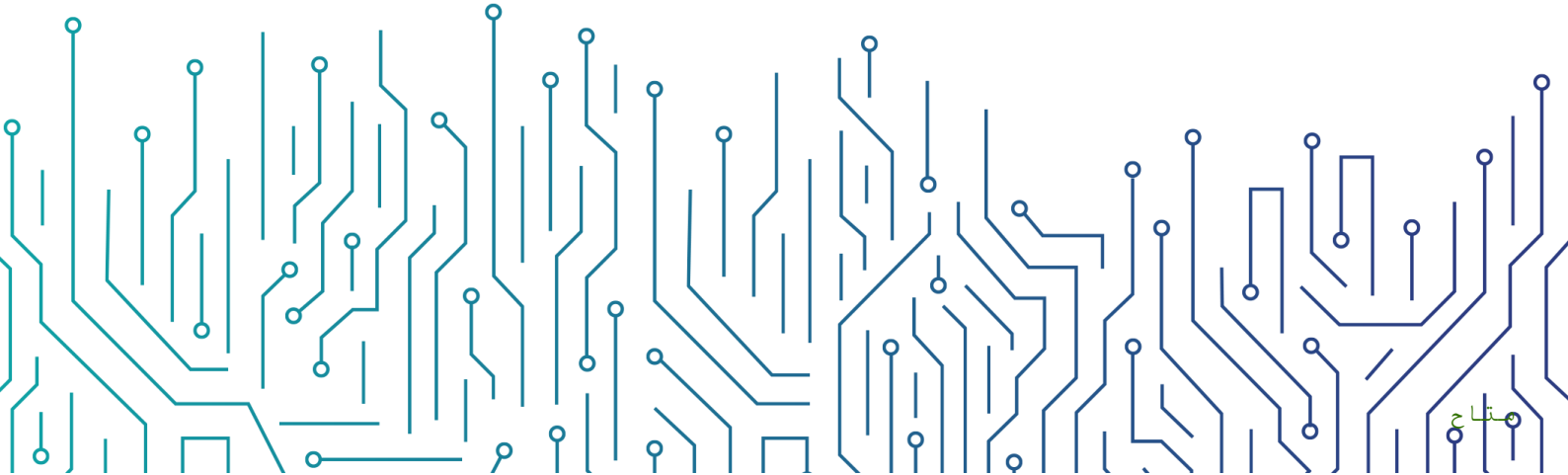
3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعه حائل

جامعة حائل
University of Ha'il

نموذج معيار التطوير الآمن للتطبيقات

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني



متاح

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتطوير البرمجيات والتطبيقات وحمايتها من التهديدات الداخلية والخارجية في جامعه حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ١-٣-٦-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018).

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار كافة أنشطة ومشاريع وممارسات تطوير البرمجيات والتطبيقات والأصول المعلوماتية والتقنية الخاصة بها في جامعه حائل وتنطبق على جميع العاملين في جامعه حائل

المعايير

1	التطوير الآمن للتطبيقات (Secure Code Development)
الهدف	توفير متطلبات الأمن السيبراني لضمان حماية أنشطة تطوير البرمجيات والتطبيقات وضوابط الأمن السيبراني لحماية البرمجيات التي يتم تطويرها.
المخاطر المحتملة	يمكن أن يؤدي تطوير التطبيقات غير الآمن إلى إيجاد ثغرات أمنية يمكن استغلالها لتهديد سرية بيانات جامعه حائل وسلامتها وتوافرها، والتأثير في سير عملها.
الإجراءات المطلوبة	
1-1	تطوير عملية دورة حياة تطوير البرمجيات الآمنة (SSDLC) وتطبيقها. A Secure Software Development Life Cycle (SSDLC) process Shall be developed and implemented.
2-1	تطوير منهجية وعملية "التطوير والأمن والعمليات" (DevSecOps) واتباعها. A DevSecOps methodology and process shall be developed and adopted.
3-1	ضمان توفير متطلبات الأمن السيبراني في المراحل الأولية من تطوير البرمجيات ودمجها في دورة حياة تطوير البرمجيات الآمنة (SSDLC).

Cybersecurity requirements shall be provided in the initial phases of software development and incorporated in the SSDLC process.	
ضمان اختبار الأمن السيبراني في مراحل اختبار تطوير البرمجيات ودمجه في دورة حياة تطوير البرمجيات الآمنة (SSDLC). Cybersecurity testing shall be conducted in the testing phases of software development and incorporated in the SSDLC process.	4-1
تصميم وإعداد بيئة آمنة لغايات التطوير والاختبار وضمان الجودة. A secure environment shall be designed and configured for development, testing and quality assurance purposes.	5-1
تطبيق إرشادات تطوير التطبيقات الآمن وفقاً للجدول (أ). The secure coding guidelines under Table (A) shall be implemented.	6-1
تطبيق إجراءات التخفيف على أعلى 10 مخاطر تهدد أمن تطبيقات الويب وفقاً للمشروع المفتوح لأمن تطبيقات الويب (OWASP) فيما يخص الأنظمة والتطبيقات الحساسة. Mitigations to the Open Web Application Security Project (OWASP) Top 10 Application Security Risks shall be implemented for critical systems and applications.	7-1
تطبيق آليات لتقييد صلاحيات التعديل على الشفرة المصدرية أو بيانات بيئات الإنتاج. Mechanisms to restrict modification of production source code or production data shall be implemented.	8-1
إلزام الموردين الخارجيين بالالتزام بسياسات ومعايير الأمن السيبراني المعتمدة في جامعه حائل Third party vendors shall be required to adhere to Hail University's cybersecurity policies and standards.	9-1
الحصول علىيجب استخدام المصادر الحديثة والموثوق بها والمرخصة فقط لأدوات تطوير البرمجيات والمكتبات والمكونات Only up-to-date, trusted and licensed sources of software development tools, libraries and components shall be used.	10-1

11-1	ضمان تطبيق ضوابط حماية تطبيقات الويب وفقاً لسياسة ومعيار حماية تطبيقات الويب المعتمدين في جامعه حائل Web application security controls shall be implemented as per Hail University's Web Application Security Policy and Standard.
12-1	استخدام خوارزميات تشفير موحدة ومراجعة بدقة وفقاً للمعايير والإجراءات ذات العلاقة. Standardized and extensively reviewed encryption algorithms shall be used only as per relevant standards and procedures.
13-1	التحقق من أن إصدارات كافة البرمجيات التي تم شراؤها من خارج جامعه حائل مدعومة من المطور ومحصنة بصورة ملائمة بناءً على التوصيات الأمنية للمطور. All versions of all software acquired from outside Hail University shall be verified to be still supported by the developer and appropriately hardened based on the developer's security recommendations.
14-1	تدريب جميع العاملين في تطوير البرمجيات على كتابة الشفرات المصدرية المناسبة للغة البرمجة وبيئة التطوير المستخدمة. Conduct training on writing secure code appropriate to the programming language and development environment being used for all software development personnel.
2	مستودع الشفرة المصدرية (Source Code Repository)
الهدف	توفير ضوابط الأمن السيبراني لضمان حماية الشفرة المصدرية والمكتبات ومستودع الشفرة المصدرية.
المخاطر المحتملة	في حال عدم توفير حماية كافية ومناسبة للشفرة المصدرية والمكتبات، يمكن أن تتعرض الشفرة المصدرية في جامعه حائل للخطر أو يتم التلاعب بها أو الوصول غير المصرح به لها.
الإجراءات المطلوبة	
1-2	استخدام مستودع شفرة مصدرية آمن يمتاز بتطبيق إجراءات التحقق من الهوية والإصدار والرقابة وتسجيل الدخول.

A secure source code repository that has authentication, version control, and logging enabled shall be used.	
تطبيق إجراءات منع وصول أي شخص إلى الشفرة المصدرية ومستودع الشفرة المصدرية باستثناء مطوري التطبيقات والجهات المسؤولة عنها. Deny access to source code and source code repository for anyone except application developers and owners.	2-2
استخدام خطة ترقيم موحدة لضوابط الإصدار بحيث تبين تاريخ تثبيت الإصدارات المحدثة من البرمجيات. A unified version control numbering scheme shall be used to reflect when updated versions of the software are installed.	3-2
أرشفة الإصدارات القديمة من الشفرة المصدرية دورياً. Outdated versions of source code shall be archived periodically.	4-2
فصل الشفرة المصدرية للتطبيقات قيد التطوير عن الشفرة المصدرية للتطبيقات في بيئة الإنتاج. Source code for applications under development shall be segregated from source code for applications in production.	5-2
أرشفة الشفرة المصدرية للتطبيقات التي انتهت صلاحيتها بحيث يمكن استرجاعها عند الحاجة. The source code of end of life applications shall be archived to ensure that it can still be retrieved if needed.	6-2
الحصول على نسخة من الشفرة المصدرية لكافة التطبيقات التي طورتها أطراف خارجية لـجامعه حائل وتخزينها في مستودع الشفرة المصدرية. A copy of the source code for all applications developed by third parties specifically for Hail University shall be acquired and stored in a secure source code repository.	7-2
تطوير معايير تحصين وأمن الحاويات والنسخ الافتراضية للنظام (Docker) وإرشادات الممارسات الأمنية المثلى وتطبيقها.	8-2

	Container and docker security hardening standards and security best practices guidelines shall be developed and implemented.
9-2	تثبيت آليات إدارة الأسرار وذلك من أجل إدارة الأسرار والمفاتيح والشهادات ومنع تخزين الأسرار في الحاويات. Secret management mechanisms shall be deployed to manage secrets, keys and certifications and prevent storing secrets in containers.
10-2	استخدام نسخ الحاويات من مصادر موثوقة أو معتمدة. Container images shall be used from trusted or approved sources.
11-2	استخدام سجل حاويات خاص لضمان تنزيل نسخ الحاويات المعتمدة والآمنة فقط على النظام بحيث يمكن فحص كل نسخة بحثاً عن الثغرات المعروفة والشائعة. A private container registry shall be used to ensure only verified and safe container images are downloaded to Hail University's system, and that every image is scanned for common known vulnerabilities.
12-2	عدم إدارة الحاويات من خلال حسابات المستخدمين عالية الصلاحية والامتيازات. Containers shall not be run with superuser accounts.
3	مراجعة واختبار الشفرة المصدرية (Secure Code Review and Testing)
الهدف	توفير ضمان بشأن تطبيق ضوابط الأمن السيبراني على تطوير التطبيقات الآمن وكشف نقاط الضعف والثغرات والمشكلات في البرمجيات.
المخاطر المحتملة	يمكن أن تتعرض جامعه حائل إلى مخاطر أمنية كبيرة في حال عدم اختبار الشفرة المصدرية وأنشطة تطوير الشفرات ومراجعتها بانتظام لغايات الكشف عن الثغرات الأمنية والإعدادات الخاطئة ونقاط الضعف، يمكن أن تتعرض جامعه حائل إلى مخاطر أمنية كبيرة.
الإجراءات المطلوبة	
1-3	إجراء عملية مراجعة الشفرة المصدرية بانتظام لتطبيقات الويب المطورة داخلياً. A secure code review process shall be conducted regularly for internally developed web applications.

2-3	تطبيق أدوات التحليل الثابتة والديناميكية للتحقق من الالتزام بممارسات تطوير التطبيقات الآمن بالنسبة للبرمجيات المطورة داخلياً. Static and dynamic analysis tools shall be applied to verify that secure coding practices are being adhered to for internally developed software.
3-3	القيام بمراجعة أمنية الشفرة المصدرية بانتظام لكافة التطبيقات المطورة لـجامعه حائل من قبل أطراف خارجية. Conduct a secure code review process regularly for all applications developed by third parties specifically for Hail University.
4-3	مراجعة واعتماد الضوابط الأمنية للتطبيقات المطورة داخلياً قبل تثبيتها في بيئة الإنتاج. Security controls of new internally developed applications shall be reviewed and approved prior to application deployment into the production environment.
5-3	إعادة تقييم التطبيقات الحالية المطورة داخلياً وإعادة اعتمادها بعد إجراء تغيير رئيسي عليها أو بعد مرور فترة زمنية محددة. Existing internally developed applications shall be re-evaluated and re-approved after a significant change is made to the application, or after a predetermined period.
6-3	إجراء تقييم المخاطر لكافة التطبيقات قيد التطوير أو التي يتم شراؤها لتحديد الضوابط المطلوبة لتقليل مخاطر التطبيقات إلى مستويات مقبولة قبل التثبيت في بيئة الإنتاج (يرجى الرجوع إلى سياسة إدارة المخاطر المعتمدة في جامعه حائل) Risk assessments for all applications under development, or which are purchased, shall be conduced to determine the controls required to mitigate application risks to acceptable limits prior to deployment into production environment (refer to Hail University's Risk Management Policy).
7-3	إجراء اختبار الالتزام بالأمن السيبراني للبرمجيات بناءً على سياسات الأمن السيبراني المعتمدة في جامعه حائل قبل التثبيت في بيئة الإنتاج. Cybersecurity compliance testing shall be conducted for software against Hail University's cybersecurity policies and standards prior to deployment into production environment.

8-3	استخدام معيار التحقق من حماية التطبيقات الصادر عن المشروع المفتوح لأمن تطبيقات الويب (OWASP) كدليل إرشادي لتحديد المتطلبات الأمنية وعمل حالات اختبار لمراجعة الأنظمة والتطبيقات الحساسة. OWASP Application Security Verification Standard shall be employed as a guide to define security requirements and generate test cases to review critical systems and applications.
9-3	إجراء مراجعة لإعدادات البرمجيات بما في ذلك مراجعة الإعدادات والتحصين وحزم التحديثات قبل التثبيت في بيئة الإنتاج. Configurations review of software, including secure configuration hardening and patching, shall be conducted prior to deployment into production environment.
10-3	إجراء اختبارات الأمن السيبراني، بما في ذلك تقييم الثغرات واختبار الاختراق ومراجعة تطويرالتطبيقات الآمن، قبل التثبيت في بيئة الإنتاج. Cybersecurity testing; including vulnerability assessment, penetrating testing and secure code review; shall be conducted prior to deployment into production environment.
11-3	إجراء اختبارات الأمن السيبراني، بما في ذلك تقييم الثغرات واختبار الاختراق، بعد التثبيت في بيئة الإنتاج. Cybersecurity testing, including vulnerability assessment and penetrating testing, shall be conducted after deployment into production environment.
12-3	معالجة كافة المشاكل الأمنية في التطبيقات المطورة التي يتم اكتشافها خلال مراجعة تطوير التطبيقات الآمن قبل التثبيت في بيئة الإنتاج. All developed application security issues discovered during the secure code review shall be remediated prior to implementation into production environment.
13-3	اختبار التطبيقات المطورة لضمان تطبيق ضوابط فصل المهام بالصورة الملائمة. Developed applications shall be tested to ensure that Segregation of duties controls are appropriately implemented.

14-3	إلغاء حسابات الاختبار الموجودة في بيئة غير بيئة الإنتاج قبل نقل التطبيقات إلى بيئة الإنتاج. Test accounts that are used in non-production environments shall be removed before the application is moved into production.
15-3	فصل بيئة الاختبار والتطوير منطقياً عن بيئة الإنتاج والبيئات الأخرى باستخدام محددات الشبكة عن طريق إعداد وتثبيت قوائم التحكّم بالوصول (ACL) والسياسات الأمنية على جدران الحماية. Test and development environment shall be logically separated from production and other environments using network restrictions by configuring Access-Control Lists (ACLs) and security policies on firewalls.
16-3	إجراء مراجعة النظير للشفرة المصدرية من قبل مطور لم يشارك في كتابة أي شفرة قبل التثبيت في بيئة الإنتاج في جامعه حائل Source code peer-review shall be conducted by a developer who did not write any of the code prior to its deployment into Hail University's production environment.
17-3	استخدام الشفرة المصدرية وأدوات تقييم أمن البرمجيات المعتمدة والمرخصة. Only approved and licensed source code and software security assessment tools shall be used.
18-3	إجراء الاختبارات الأمنية للتطبيقات المطورة في كافة مراحل اختبار دورة حياة تطوير البرمجيات (SDLC)، بما في ذلك الاختبارات غير الوظيفية، واختبار الوحدات (UT) واختبار تكامل الأنظمة (SIT)، واختبار قبول المستخدم (UAT). Security testing for developed applications shall be performed in all testing phases of SDLC including non-functional testing, Unit Testing (UT), System Integration Testing (SIT), and User Acceptance Testing (UAT).
19-3	استحداث عملية لإدارة العيوب البرمجية في البرمجيات والثغرات والمشكلات الأمنية ووضع سجل خاص بها ومتابعتهما. A process and registry shall be developed and maintained to manage software bugs, vulnerabilities and security issues.
20-3	إدراج الاختبارات كجزء من عمليات التحسين المستمر والتطوير المستمر (CI/CD).

Testing shall be embedded as part of the Continuous Improvement/Continuous Development (CI/CD) pipeline.	

الجدول أ - إرشادات تطوير التطبيقات الآمن

1	علميات التحقق من الهوية (OWASP:A2:2017 - إجراءات التحقق من الهوية غير الآمنة) Authentication (OWASP:A2:2017 – Broken Authentication)
1-1	التحقق من أن كافة الصفحات والمصادر تقتضي التحقق من الهوية باستثناء المحددة خصوصاً لتكون عامة (مبدأ التحقق التام والمتكامل). It shall be verified that all pages and resources require authentication except those specifically intended to be public (Principle of Complete Mediation).
2-1	التحقق من أن حقول كلمات المرور لا تُظهر كلمات مرور المستخدمين عند إدخالها وأن خاصية الإكمال التلقائي في حقول كلمات المرور (أو الأشكال التي تتضمنها) غير مفعلة. It shall be verified that all password fields do not show users' passwords when entered, and that password fields (or the forms that contain them) have autocomplete disabled.
3-1	التحقق من أن كافة ضوابط التحقق من الهوية تخفق بصورة آمنة لضمان عدم قدرة الجهات المهاجمة على تسجيل الدخول. It shall be verified that all authentication controls fail securely to ensure that attackers cannot log in.
4-1	التحقق من أن بيانات الاعتماد وكافة معلومات الهوية الأخرى التي يتعامل معها التطبيق لا تمر عبر روابط غير مشفرة أو مشفرة بصورة غير آمنة. It shall be verified that credentials and all other identity information handled by the application do not traverse unencrypted or through weakly encrypted links.
5-1	التحقق من أن مسار "نسيت كلمة المرور" ومسارات الاستعادة الأخرى لا ترسل كلمات المرور الحالية أو الجديدة من غير تشفير.

It shall be verified that forgot password and other recovery paths do not send the existing or new passwords in clear text to the user.	
التحقق من أن تنفيذ هجمات تعداد اسم المستخدم (User Enumeration) غير ممكن عن طريق وظائف "تسجيل الدخول" أو "إعادة ضبط كلمة المرور" أو "نسيت الحساب". It shall be verified that performing username enumeration is not possible via login, password reset, or forgot account functionalities.	6-1
التحقق من عدم وجود كلمات مرور افتراضية قيد الاستخدام لإطار عمل التطبيق أو أي مكونات مستخدمة من قبل التطبيق (مثل "admin/password"). It shall be verified that there are no default passwords in use for the application framework or any components used by the application (such as “admin/password”).	7-1
التحقق من وجود ضابط مصادر (Resource Governor) لتوفير الحماية من الهجوم التخميني العمودي (Vertical Brute Forcing) (وهو هجوم يحاول اختراق حساب واحد باستخدام كافة كلمات المرور المحتملة) والهجوم التخميني الأفقي (Horizontal Brute Forcing) (وهو هجوم يحاول اختراق جميع الحسابات باستخدام كلمة مرور واحدة مثل "Password1"). ويجب ألا يكون هناك تأخير في إدخال بيانات الاعتماد الصحيحة. فعلى سبيل المثال، يجب ضبط إعدادات عنوان بروتوكول الإنترنت لمصدر الهجوم التخميني بحيث يتم إغلاقه بعد 60 دقيقة، ويتم إغلاق الحساب بعد 15 دقيقة. ويجب أن تكون آليتا الضبط فاعلتين بشكل متزامن للحماية من الهجمات التشخيصية والموزعة. It shall be verified that a resource governor is in place to protect against vertical brute forcing (i.e., when a single account is tested against all possible passwords) and horizontal brute forcing (i.e., when all accounts are tested with the same password, such as “Password1”). A correct credential entry shall incur no delay. For example, brute force source IP address lockout shall be configured to 60 minutes and account lockout to 15 minutes. Both these governor mechanisms shall be active simultaneously to protect against diagonal and distributed attacks.	8-1
التحقق من أن كافة ضوابط التحقق من الهوية فعالة من جهة الخادم.	9-1

It shall be verified that all authentication controls are enforced on the server side.	
التحقق من أن حقول كلمات المرور تسمح باستخدام عبارات مرور، ولا تمنع استخدام عبارات مرور طويلة أو معقدة للغاية، وتوفر حماية كافية من استخدام كلمات المرور الدراجة. It shall be verified that password entry fields allow or encourage the use of passphrases, and do not prevent the entry of long passphrases or highly complex passwords, and provide a sufficient minimum strength to protect against the use of commonly chosen passwords.	10-1
التحقق من أن كافة وظائف إدارة الحسابات، (مثل التسجيل، أو تحديث الملف التعريفي، أو "نسيت اسم المستخدم"، أو "نسيت كلمة المرور"، أو رمز التعريف غير المفعل/المفقود، أو مكتب المساعدة، أو الاستجابة الصوتية التفاعلية "IVR")، والتي يمكن أن تستعيد صلاحية الوصول إلى الحساب، قادرة على مقاومة الهجمات بنفس مستوى الآلية الأساسية للتحقق من الهوية. It shall be verified that all account management functions (such as registration, update profile, forgot username, forgot password, disabled/lost token, help desk or IVR) that might regain access to the account are at least as resistant to attacks as the primary authentication mechanism.	11-1
التحقق من أن المستخدمين يمكنهم تغيير بيانات اعتمادهم باستخدام آلية مقاومة للهجمات تتمتع بنفس قدرة الآلية الأساسية للتحقق من الهوية على مقاومة الهجمات. عند تغيير كلمات المرور، يجب إدخال كلمة المرور الحالية قبل إدخال كلمة المرور الجديدة وأن يتبع ذلك عملية إعادة تحقق من المستخدم. It shall be verified that users can safely change their credentials using a mechanism that is at least as resistant to attacks as the primary authentication mechanism. Password changes shall require the existing password to be entered prior to entering a new password, followed by re-authentication of the user.	12-1
التحقق من انتهاء صلاحية بيانات الاعتماد بعد مرور فترة زمنية يتم إعدادها إدارياً. ويجب أن تكون فترة انتهاء صلاحية كلمة المرور قصيرة بناءً على حساسية التطبيق، مما يفرض بالتالي تغيير كلمة المرور بشكل أسرع.	13-1

It shall be verified that authentication credentials expire after an administratively configurable period of time. The password expiry duration shall be shorter based on the criticality of the application, thus ensuring a quicker password change.	
التحقق من تسجيل كافة قرارات التحقق من الهوية بما في ذلك "المباعدات الخطية" و"الأقفال المؤقتة". It shall be verified that all authentication decisions are logged, including linear back offs and soft-locks.	14-1
التحقق من أن كلمات مرور الحسابات مجزئة عشوائياً باستخدام طريقة تجزئة عشوائية خاصة لكل حساب (مثل هوية مستخدم الإنترنت أو إنشاء الحساب) واختزالها قبل التخزين. It shall be verified that account passwords are salted using a salt that is unique to each account (e.g., internal user ID, account creation, etc.) and hashed before storing.	15-1
التحقق من أن كافة بيانات اعتماد التحقق من الهوية للوصول للخدمات الخارجية بالنسبة للتطبيق مشفرة ومخزنة في موقع محمي (وليس في شفرة مصدرية). It shall be verified that all authentication credentials for accessing external services for the application are encrypted and stored in a protected location (not in source code).	16-1
التحقق من أن نسيان كلمة المرور ومسارات الاستعادة ترسل رمز تفعيل أو تحقّق من الهوية متعدّد العناصر له وقت محدد (مثل الرسائل النصية، أو رموز تعريفية، أو تطبيقات الهواتف المحمولة، أو غيرها) بدلاً من إرسال كلمة المرور. It shall be verified that forgot password and other recovery paths send a time-limited activation token or use multi-factor authentication (e.g., SMS, tokens, mobile application, etc.) instead of a password.	17-1
التحقق من أن وظيفة "نسيت كلمة المرور" لا تغلق الحساب أو تلغي تفعيله إلا بعد أن ينجح المستخدم في تغيير كلمة المرور. It shall be verified that “forget password” functionality does not lock or otherwise disable the account until after the user has successfully changed their password.	18-1

19-1	التحقق من عدم وجود أسئلة وإجابات معرفية مشتركة (ما يسمى بالأسئلة والإجابات "السرية"). It shall be verified that there are no shared knowledge questions/answers (Also called "secret" questions and answers).
20-1	التحقق من إمكانية إعداد النظام وضبطه بحيث لا يسمح باستخدام أرقام قابلة للإعداد من كلمات مرور سابقة. It shall be verified that the system can be configured to disallow the use of a configurable number of previous passwords.
21-1	التحقق من تنفيذ كافة ضوابط التحقق من الهوية مركزياً (بما في ذلك المكتبات التي تستدعي خدمات تحقق خارجية). It shall be verified that all authentication controls (including libraries that call external authentication services) have a centralized implementation.
22-1	التحقق من طلب إعادة التحقق من الهوية أو تحقق الإعداد أو التحقق من الهوية المتغير، أو الرسالة النصية أو التطبيق ثنائي العوامل أو توقيع المعاملة قبل السماح بأي عمليات حساسة على التطبيق وفقاً للملف التعريفي للمخاطر الخاصة بالتطبيق. It shall be verified that re-authentication, step up or adaptive authentication, SMS or other two-factor application, or transaction signing is required before any application-specific sensitive operations are permitted as per the risk profile of the application.
23-1	التحقق من وجود وظيفة لإلغاء تفعيل بيانات اعتماد المستخدم أو إبطالها في حال وقوع انتهاك أمني. It shall be verified that a functionality to invalidate or disable user credentials in the event of a compromise is in place.
24-1	التحقق من تشفير كلمة المرور وفقاً للمعايير والإجراءات ذات العلاقة. It shall be verified that password encryption is implemented in accordance with relevant standards and procedures.
25-1	إذا كان التطبيق يدير مخزن بيانات اعتماد، فإنه يجب أن يضمن تخزين قيمة الاختزال باتجاه واحد وبطريقة مشفرة بدرجة تعقيد عالية لكلمات المرور، وأن الجدول والملف

	الذي يخزن كلمات المرور والمفاتيح يمكن الكتابة عليه فقط عن طريق التطبيق. (يجب عدم استخدام خوارزمية "MD5" قدر الإمكان). If Hail University's application manages a credential store, it shall ensure that only cryptographically strong one-way salted hashes of passwords are stored and that the table/file that stores the passwords and keys is write-able only by the application. (If possible, MD5 algorithm shall not be used).
26-1	فصل منطق التحقق من الهوية عن المصدر الذي يتم طلبه، واستخدام إعادة التوجيه من وإلى مراقبة التحقق من الهوية المركزي. Authentication logic shall be segregated from the resource being requested, and redirection to and from the centralized authentication control shall be used.
27-1	يجب ألا تشير رسائل فشل التحقق من الهوية إلى الجزء غير الصحيح من بيانات التحقق من الهوية. فعلى سبيل المثال، بدلاً من استخدام "اسم مستخدم غير صحيح" أو "كلمة مرور غير صحيحة"، يجب استخدام "اسم مستخدم غير صحيح أو كلمة مرور غير صحيحة" لكلا الحالتين. ويجب أن تكون رسائل الأخطاء متطابقة في الشفرة المصدرية وعند عرضها. Authentication failure responses shall not indicate which part of the authentication data is incorrect. For example, instead of "Invalid username" or "Invalid password," "Invalid username and/or password" shall be used for both. Error responses shall be truly identical in both display and source code.
28-1	يجب تطبيق متطلبات درجة تعقيد كلمة المرور الواردة في السياسة أو اللائحة، كما يجب أن تكون بيانات اعتماد التحقق من الهوية كافية لمواجهة الهجمات التي تعتبر شائعة بالنسبة للتهديدات الموجودة في بيئة التثبيت. ويجب التحقق من أن كلمة المرور تتضمن كحد أدنى ما يلي: • حرف كبير واحد على الأقل (A-Z). • حرف صغير واحد على الأقل (a-z). • رقم واحد على الأقل (0-9). • رمز خاص واحد على الأقل مثل: (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~"). كما يجب التحقق من أن كلمة المرور لا تتضمن على الأقل ما يلي:

	• أكثر من رقمين أو رمزين متطابقين متتاليين (مثل "111" و"aa"). • أرقام أو رموز متسلسلة (مثل "123"، أو "789"، أو"abc"). • نفس اسم المستخدم. • كلمات قاموسية ("password"، أو "p@ssw0rd"، أو "secret123"). Password complexity requirements established by a policy or regulation shall be enforced. Authentication credentials shall be sufficient to withstand attacks that are typical of the threats in the deployed environment. Additionally, it shall be verified that passwords contain: • At least 1 upper case character (A-Z) • At least 1 lower case character (a-z) • At least 1 digit (9-0) • At least 1 special character (e.g.,-,+*()'&%$#"! “ ”~{|}`_^[\]@?<=>;:/) It shall be verified that passwords do not contain: • More than 2 identical digits or characters in a row (e.g., 111, aa, etc.) • Sequential digits or characters (e.g., 123, 789, and abc) • The same username • Dictionary words (e.g., password, p@ssw0rd, secret123, etc.)
29-1	إنفاذ إلغاء تفعيل الحساب بعد عدد محدد من محاولات تسجيل الدخول غير الصحيحة (على سبيل المثال، خمس محاولات للتطبيقات غير الهامة وثلاث محاولات للتطبيقات الحساسة). ويجب إلغاء تفعيل الحساب لفترة زمنية معينة تكون كافية لإحباط محاولات الهجوم التخميني لبيانات الاعتماد شريطة ألا تكون هذه المدة طويلة بحيث تسمح بتنفيذ هجمات حجب الخدمة (مثلاً إلغاء التفعيل لمدة 30 دقيقة فقط). Accounts shall be disabled after an established number of invalid login attempts (e.g., five attempts for non-critical applications and three attempts for critical applications). Accounts shall be disabled for a period of time sufficient to discourage brute force guessing of credentials, but not so

long as to allow for a denial-of-service attack to be performed. (For example, disabled for 30 minutes).	
يجب إبلاغ المستخدم بآخر استخدام للحساب (سواءً كان ناجحاً أم لا) عند تسجيله الدخول بنجاح. The last use (successful or unsuccessful) of a user account shall be reported to the user at their next successful login.	30-1
إدارة الجلسات (OWASP:A2: 2017 - إجراءات التحقق من الهوية غير الآمنة) Session Management (OWASP:A2:2017 – Broken Authentication)	2
التحقق من استخدام التطبيق لتنفيذ التحكم بإدارة الجلسة التلقائية الخاصة بإطار العمل. It shall be verified that the framework's default session management control implementation is used by the application.	1-2
التحقق من إبطال الجلسات عند تسجيل خروج المستخدم. It shall be verified that sessions are invalidated when the user logs out.	2-2
التحقق من انتهاء وقت الجلسات بعد مرور فترة معينة من عدم النشاط. It shall be verified that sessions timeout after a specified period of inactivity.	3-2
التحقق من أن كافة الصفحات التي تقتضي التحقق من الهوية للوصول إليها تتضمن روابط لتسجيل الخروج. It shall be verified that all pages that require authentication to access them have logout links.	4-2
التحقق من أن هوية الجلسة غير مكشوفة أبداً إلا في عناوين ملفات الارتباط (Cookie Headers)، وتحديداً في شريط العنوان (URL) أو رسائل الخطأ أو السجلات. ويتضمن هذا التحقق من أن التطبيق لا يدعم قيام شريط العنوان (URL) بإعادة كتابة جلسات الملفات التعريفية. It shall be verified that the session ID is never disclosed other than in cookie headers, particularly in URLs, error messages,	5-2

or logs. This includes verifying that the application does not support URL rewriting of session cookies.	
التحقق من تغيير هوية الجلسة أو مسحها عند تسجيل الخروج. It shall be verified that the session ID is changed or cleared on logout.	6-2
التحقق من أن الرموز التعريفية للجلسات المصادق عليها باستخدام ملفات الارتباط محمية باستخدام آلية "HttpOnly" (عدم عرض ملفات الارتباط عند المستخدم). It shall be verified that authenticated session tokens using cookies are protected by the use of "HttpOnly".	7-2
التحقق من أن الرموز التعريفية للجلسات المصادق عليها باستخدام ملفات الارتباط محمية بخاصية "Secure" وأن عناوين أمن النقل المقيد موجودة (مثل: "Strict-Transport-Security: max-age=60000; includeSubDomains"). It shall be verified that authenticated session tokens using cookies are protected with the "Secure" attribute and strict transport security headers (such as Strict-Transport-Security: max-age=60000; includeSubDomains) is present.	8-2
التحقق من تغيير هوية الجلسة عند تسجيل الدخول لمنع سرقة بيانات الجلسة. It shall be verified that the session ID is changed on login to prevent session fixation.	9-2
التحقق من تغيير هوية الجلسة عند إعادة التحقق من الهوية. It shall be verified that the session ID is changed on re-authentication.	10-2
التحقق من أن التطبيق يتعرف على هويات الجلسات الصادرة عن طريق إطار عمل التطبيق نفسه ويعتبر هذه الهويات فقط صحيحة. It shall be verified that only session IDs generated by the application framework are recognized as valid by the application.	11-2
التحقق من أن الرموز التعريفية للجلسات المصادق عليها طويلة وعشوائية بالقدر الكافي لمواجهة الهجمات التي تعتبر تهديدات شائعة في بيئة التثبيت.	12-2

It shall be verified that authenticated session tokens are sufficiently long and random to withstand attacks that are typical threats in the deployment environment.	
التحقق من أن الرموز التعريفية للجلسات المصادق عليها والتي تستخدم ملفات الارتباط لها مسار محدد بقيمة حصرية ملائمة لذلك الموقع. ويجب عدم تحديد تقييد خاصية ملف ارتباط النطاق إلا إذا كانت الأعمال تقتضي ذلك، كعملية تسجيل دخول موحد. It shall be verified that authenticated session tokens using cookies have their path set to an appropriately restrictive value for that site. The domain cookie attribute restriction shall not be set except for a business requirement, such as a single sign on.	13-2
التحقق من أن التطبيق لا يسمح بجلسات مستخدم متزامنة مكررة صادرة من أجهزة مختلفة. It shall be verified that the application does not permit duplicate concurrent user sessions, originating from different machines.	14-2
التحقق من انتهاء وقت الجلسات بعد مرور الحد الأقصى لفترة زمنية تم إعدادها إدارياً بغض النظر عن النشاط (أي وقت انتهاء مطلق). It shall be verified that sessions timeout after an administratively configurable maximum time period regardless of the performed activity (i.e., an absolute timeout).	15-2
إصدار هوية جديدة للجلسة في حال تغيير أمن الاتصال من بروتوكول نقل النص التشعبي (HTTP) إلى بروتوكول نقل النص التشعبي الآمن (HTTPS)، والذي قد يحدث خلال عملية التحقق من الهوية. من المستحسن استخدام بروتوكول نقل النص التشعبي الآمن (HTTPS) باستمرار في التطبيق بدلاً من التنقل بين بروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل النص التشعبي الآمن (HTTPS). A new session identifier shall be generated if the connection security is changed from HTTP to HTTPS, as can occur during authentication. Within an application, it is recommended to consistently utilize HTTPS rather than switching between HTTP to HTTPS.	16-2
التحكم بالوصول (OWASP:A5:2017 - إجراءات التحكم بالوصول غير الآمنة)	3

Access Control (OWASP:A5:2017 – Broken Access Control)	
التحقق من أن المستخدمين يمكنهم الوصول فقط إلى الوظائف أو الخدمات الآمنة التي يملكون تصاريح وصلاحيات خاصة لها. It shall be verified that users can only access secured functions or services for which they possess specific authorization.	1-3
التحقق من أن المستخدمين يمكنهم الوصول فقط إلى العناوين الآمنة (Secured URLs) التي يملكون تصاريح وصلاحيات خاصة لها. It shall be verified that users can only access secured URLs for which they possess specific authorization.	2-3
التحقق من أن المستخدمين يمكنهم الوصول فقط إلى ملفات البيانات الآمنة التي يملكون تصاريح وصلاحيات خاصة لها. It shall be verified that users can only access secured data files for which they possess specific authorization.	3-3
التحقق من أن مرجعيات الكائنات المباشرة محمية بحيث يمكن الوصول فقط إلى الكائنات المصرح بها لكل مستخدم. It shall be verified that direct object references are protected in a way that ensures only authorized objects are accessible to each user.	4-3
التحقق من إلغاء تفعيل تصفح الدليل (Directory Browsing) إلا إذا كان ذلك مطلوباً. It shall be verified that directory browsing is disabled unless required.	5-3
التحقق من أن المستخدم يمكنه الوصول فقط إلى المعلومات المحمية التي يملك تصاريح وصلاحيات خاصة لها (على سبيل المثال، من خلال تطبيق ضوابط لحماية مرجعيات الكائنات من التلاعب المباشر والوصول غير المصرح به إلى البيانات). It shall be verified that users can only access protected data for which they possess specific authorization (for example, by implementing controls to protect against direct object reference tampering and prevent unauthorized access to data).	6-3

7-3	التحقق من إخفاق ضوابط الوصول بصورة آمنة. It shall be verified that access controls fail securely.
8-3	التحقق من أن نفس قواعد التحكم بالوصول المتضمنة في طبقة العرض مطبقة على الخادم بحسب دور المستخدم، بحيث لا يمكن إعادة تفعيل الضوابط والمعايير أو إعادة إضافتها من مستخدمين يمتلكون مزايا وصلاحيات أعلى. It shall be verified that the same access control rules implied by the presentation layer are enforced on the server side for that user role, and that controls and parameters cannot be re-enabled or re-added by users with higher privileges.
9-3	التحقق من أن كافة خصائص المستخدمين والبيانات ومعلومات السياسة المستخدمة من قبل ضوابط الوصول لا يمكن التلاعب بها من قبل المستخدمين إلا إذا كان مصرحاً لهم بذلك تحديداً. It shall be verified that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.
10-3	التحقق من أن كافة ضوابط الوصول فعالة من جهة الخادم. It shall be verified that all access controls are enforced on the server side.
11-3	التحقق من أن قرارات التحكم بالوصول يمكن تسجيلها وأن كافة القرارات غير الناجحة قد تم تسجيلها. It shall be verified that all access control decisions can be logged and all failed decisions are logged.
12-3	التحقق من أن التطبيق أو إطار العمل يصدر رموزاً تعريفية عشوائية معقدة مضادة لتزوير الطلب عبر المواقع (Cross-Site Request Forgery "CSRF")، وتكون هذه الرموز خاصة بالمستخدم باعتبارها جزءاً من كافة المعاملات عالية القيمة أو الوصول إلى المعلومات المحمية، وأن التطبيق يتحقق من وجود هذه الرموز التعريفية بالقيمة الملائمة للمستخدم الحالي عند معالجة هذه الطلبات. It shall be verified that the application or framework generates strong random anti-CSRF tokens unique to the user as part of all high value transactions or accessing protected data, and that the application verifies the presence of such tokens with

the proper value for the current user when processing these requests.	
الحماية التراكمية للتحكم بالوصول- التحقق من أن النظام يستطيع توفير الحماية من الوصول التراكمي أو المستمر للوظائف المحمية أو المصادر أو البيانات، وذلك من خلال استخدام ضابط مصادر (Resource Governor) على سبيل المثال، للحد من عدد حالات التسجيل لكل ساعة أو منع مستخدم فردي من سحب بيانات قاعدة البيانات بأكملها. Aggregate access control protection – It shall be verified that the system can protect against aggregate or continuous access of secured functions, resources, or data, possibly by the use of a resource governor, for example, to limit the number of registrations per hour or to prevent the entire database from being scraped by an individual user.	13-3
التحقق من وجود آلية مركزية (بما في ذلك المكتبات التي تستدعي خدمات تصاريح وصلاحيات خارجية) للتحكم بالوصول إلى كل نوع من المصادر المحمية. It shall be verified that a centralized mechanism (including libraries that call external authorization services) is in place to control access to each type of protected resource.	14-3
التحقق من الفصل بين المنطق الذي يتمتع بمزايا وصلاحيات عن شفرات التطبيق الأخرى. It shall be verified that there is segregation between privileged logic and other application code.	15-3
تطبيق ضوابط الوصول الملائمة إلى المعلومات المحمية المخزنة على الخادم. وتشمل هذه المعلومات البيانات المخزنة والملفات المؤقتة والبيانات التي يمكن الوصول إليها فقط من قبل مستخدمين نظام محددين. Appropriate access controls shall be implemented for protected data stored on the server. This includes cached data, temporary files and data accessible only by specific system users.	16-3
التحقق من أن حسابات الخدمة أو الحسابات التي تدعم الاتصالات من الأنظمة الخارجية أو إليها تمتلك الحد الأدنى من الصلاحيات والامتيازات.	17-3

It shall be verified that service accounts or accounts supporting connections to or from external systems have the least privilege possible.	
التحقق من تطبيق تدقيق الحسابات وإلغاء تفعيل الحسابات غير المستخدمة (على سبيل المثال، بعد مرور أكثر من 30 يوماً من تاريخ انتهاء صلاحية كلمة مرور الحساب). It shall be verified that account auditing is implemented and that unused accounts are disabled (for example, after more than 30 days from the expiration of an account's password).	18-3
في حال السماح بالجلسات الطويلة المصادق عليها، يجب إعادة التحقق دورياً من تصاريح وصلاحيات المستخدم لضمان عدم تغير مزاياه، وفي حال تغيرها، يجب تسجيل خروج المستخدم وإجباره على إجراء عملية إعادة التحقق من الهوية. If long authenticated sessions are allowed, a user's authorization shall be periodically re-validated to ensure that their privileges have not changed. In case their privileges have changed, the user shall be logged out and forced to re-authenticate.	19-3
التحقق من أن التطبيق يدعم إلغاء تفعيل الحسابات وإنهاء الجلسات عند توقف التصاريح والصلاحيات (على سبيل المثال، عند حدوث تغيير في الدور، أو في حالة التوظيف، أو إجراءات الأعمال، أو غيرها). It shall be verified that the application supports disabling of accounts and terminating sessions when authorization ceases (for example, upon changes to role, employment status, business process, etc.).	20-3
اعتماد المدخلات (OWASP:A1:2017 - الحقن والإدخال و OWASP:A7:2017 - البرمجة النصية عبر المواقع) Input validation (OWASP:A1:2017 – Injection & OWASP:A7:2017 – Cross-Site Scripting)	4
التحقق من أن بيئة التشغيل غير معرضة لتجاوز سعة المخزن المؤقت، وأن ضوابط الأمن تمنع تجاوز سعة المخزن المؤقت. It shall be verified that the runtime environment is not susceptible to buffer overflows, and that security controls prevent buffer overflows.	1-4

2-4	التحقق من أن بيئة التشغيل غير معرضة لحقن تعليمات الاستعلام البنيوية (SQL Injection)، وأن ضوابط الأمن تمنع حقن تعليمات الاستعلام البنيوية (SQL Injection). It shall be verified that the runtime environment is not susceptible to SQL Injection, and that security controls prevent SQL Injection.
3-4	التحقق من أن بيئة التشغيل غير معرضة لحقن النصوص البرمجية عبر المواقع (XSS)، وأن ضوابط الأمن تمنع حقن النصوص البرمجية عبر المواقع (XSS). It shall be verified that the runtime environment is not susceptible to Cross Site Scripting (XSS), and that security controls prevent XSS.
4-4	التحقق من أن بيئة التشغيل غير معرضة لحقن بروتوكول النفاذ إلى الدليل البسيط (LDAP Injection) وأن ضوابط الأمن تمنع حقن بروتوكول النفاذ إلى الدليل البسيط (LDAP Injection). It shall be verified that the runtime environment is not susceptible to LDAP Injection, and that security controls prevent LDAP Injection.
5-4	التحقق من أن بيئة التشغيل غير معرضة لحقن أوامر نظام التشغيل (OS Command Injection)، وأن ضوابط الأمن تمنع حقن أوامر نظام التشغيل (OS Command Injection). It shall be verified that the runtime environment is not susceptible to OS Command Injection, and that security controls prevent OS Command Injection.
6-4	التحقق من نوع البيانات ونطاقها وطولها (إذا أمكن). Data type, range and length shall be verified (if possible).
7-4	عند الحاجة إلى السماح برموز خطرة محتملة كمدخلات، يجب التأكد من تطبيق ضوابط إضافية مثل ترميز المدخلات، وحماية واجهات برمجة التطبيقات الخاصة بالمهام، ومعرفة الجهات التي تستخدم تلك البيانات طوال فترة استخدام التطبيق. وتشمل الأمثلة على الرموز الخطرة الشائعة الآتي: (< > " ' % ( ) & + \ \' \"\). If any potentially hazardous characters must be allowed as input, additional controls; such as output encoding, secure task specific APIs, and accounting for the utilization of that data throughout the application; shall be implemented.

Examples of common hazardous characters include: (" < > : "\ '\\ + & ( ) % ').	
التأكد من أن جميع عمليات التحقق من صحة المدخلات تتم بواسطة روتين مركزي للتحقق من صحة المدخلات للتطبيق. It shall be verified that all input validation is carried out by a centralized input validation routine for the application.	8-4
التحقق من أن كافة عمليات التحقق الفاشلة تؤدي إلى رفض المدخلات أو تدقيقها. It shall be verified that all input validation failures result in input rejection or input sanitization.	9-4
التحقق من تنفيذ كافة إجراءات التحقق أو إجراءات تطوير التطبيقات وإنفاذها على الخادم. It shall be verified that all input validation or encoding routines are performed and enforced on the server side.	10-4
التحقق من التخلص من كافة البيانات غير الموثوقة والتي تعتبر مخرجات بالنسبة للغة "HTML" (بما في ذلك عناصر لغة "HTML" وخصائصها، وقيم بيانات لغة "JavaScript"، وكتل الصفحات النمطية المتسلسلة "CSS Blocks"، وخصائص شريط العنوان "URL") بصورة ملائمة لمحتوي التطبيق. It shall be verified that all untrusted data that is output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URL attributes) is properly discarded for the applicable context.	11-4
التحقق من أن مجموعات الرموز، مثل "UTF-8"، محددة لكافة مصادر المدخلات. It shall be verified that a character set, such as UTF-8, is specified for all sources of input.	12-4
التحقق من أن كافة البيانات المدخلة موحدة لكافة برمجيات فك تشفير أو برمجيات تفسير البيانات المرسلة إلى العميل قبل مصادقتها. It shall be verified that all input data is canonicalized for all downstream decoders or interpreters prior to validation.	13-4
إذا كان إطار عمل التطبيق يسمح بالتخصيص التلقائي الضخم للمعايير (ويسمى أيضاً ربط المتغيرات التلقائي) من طلب وارد إلى نموذج، فيجب التحقق من أن الحقول	14-4

	الحساسة أمنياً مثل "رصيد الحساب" أو "الدور" أو "كلمة المرور" محمية من الربط التلقائي الخبيث. If the application framework allows automatic mass parameter assignment (also called automatic variable binding) from the inbound request to a model, it shall be verified that security sensitive fields such as “accountBalance”, “role” or “password” are protected from malicious automatic binding.
15-4	التحقق من أن التطبيق محمي من هجمات تلوث متغيرات بروتوكول نقل النص التشعبي (HTTP)، خصوصاً إذا كان إطار عمل التطبيق لا يميز بين مصادر متغيرات الطلب (مثل طلب "GET"، وطلب "POST"، وملفات الارتباط، والعناوين، والبيئة، وغيرها). It shall be verified that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.)
16-4	التحقق من أن التطبيق يستخدم ضابط تحقق من المدخلات واحد لكل نوع من البيانات التي يتم قبولها. It shall be verified that a single input validation control is used by the application for each type of data that is accepted.
17-4	التحقق من تسجيل كافة حالات الإخفاق في التحقق من المدخلات. It shall be verified that all input validation failures are logged.
18-4	التحقق من أن كل نوع من عمليات ترميز المخرجات أو التخلص منها التي يقوم بها التطبيق له ضابط أمني واحد للوجهة المقصودة. It shall be verified that for each type of output encoding/escaping performed by the application, there is a single security control for that type of output for the intended destination.
5	إلغاء التسلسل غير الآمن (OWASP:A8:2017- إلغاء التسلسل غير الآمن) Insecure Deserialization (OWASP:A8:2017 – Insecure Deserialization)

تطبيق عمليات التحقق من سلامة المعلومات، مثل التواقيع الرقمية، لأي كائنات متسلسلة لمنع إنشاء كائنات عدائية أو التلاعب بالبيانات. Integrity checks, such as digital signatures, shall be implemented on any serialized objects to prevent hostile object creation or data tampering.	1-5
إنفاذ قيود محددة خلال إلغاء التسلسل قبل إنشاء الكائن لأن الشفرة تتوقع عادة مجموعة فئات قابلة للتحديد. من غير المستحسن الاعتماد على هذا الأسلوب فقط نظراً إلى وجود طرق لتجاوزه. Strict type constraints during deserialization shall be enforced before object creation as the code typically expects a definable set of classes. Bypasses to this technique have been demonstrated; therefore, reliance solely on this technique is not advisable.	2-5
عزل الشفرة التي يتم إلغاء تسلسلها وتشغيلها في بيئات متدنية المزايا والصلاحيات حيثما أمكن. Code that deserializes shall be isolated and run in low privilege environments whenever possible.	3-5
تسجيل استثناءات إلغاء التسلسل وحالات الإخفاق، مثل الحالات التي لا يكون فيها النوع الوارد هو النوع المتوقع أو التي يحدد فيها إلغاء تسلسل الاستثناءات. Deserialization exceptions and failures; such as the cases in which the incoming type is not the expected type, or the deserialization throws exceptions; shall be logged.	4-5
تقييد أو مراقبة الربط البيني الوارد والصادر في الشبكة من الحاويات أو الخوادم التي تم إلغاء تسلسلها. Incoming and outgoing network connectivity from containers or servers that deserialize shall be restricted or monitored.	
مراقبة إلغاء التسلسل والتنبيه إذا كان المستخدم يلغي التسلسل باستمرار. Deserialization shall be monitored, and an alert shall be issued if a user deserializes constantly.	
التشفير (OWASP:A3:2017 - تعرض المعلومات المحمية للمخاطر) Cryptography (OWASP:A3:2017 – Protected Data Exposure)	6

1-6	التحقق من أن كافة دالات التشفير المستخدمة لحماية الأسرار من مستخدم التطبيق مطبقة على الخادم. It shall be verified that all cryptographic functions used to protect secrets from the application user are implemented on the server side.
2-6	التحقق من أن كافة وحدات التشفير تخفق بصورة آمنة. It shall be verified that all cryptographic modules fail securely.
3-6	التحقق من حماية أي أسرار رئيسية من الوصول غير المصرح به (السر الرئيسي هو بيانات اعتماد التطبيق المخزنة كنص غير مشفر على القرص والتي تستخدم لحماية الوصول إلى معلومات الإعدادات الأمنية). It shall be verified that any master secret(s) is protected from unauthorized access (A master secret is an application credential stored as plaintext on disk that is used to protect access to security configuration information).
4-6	التحقق من أن كافة الأرقام العشوائية، وأسماء الملفات العشوائية، والمعرفات الموحدة (GUIDs)، وسلاسل الحروف العشوائية (Strings) صادرة من مولد الأرقام العشوائية المعتمد لنموذج التشفير، وذلك عندما يكون الهدف من هذه القيم العشوائية هو جعل الجهة المهاجمة غير قادرة على تخمينها. It shall be verified that all random numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved random number generator when these random values are intended to be unguessable by an attacker.
5-6	التحقق من أن نماذج التشفير المستخدمة في التطبيق قد تم التحقق منها وفقاً للسياسات والإجراءات ذات العلاقة. It shall be verified that cryptographic modules used by the application have been validated as per relevant policies and procedures.
6-6	التحقق من أن نماذج التشفير تعمل بنظامها المعتمد وفقاً للسياسات والإجراءات ذات العلاقة.

It shall be verified that cryptographic modules operate in their approved mode in accordance with relevant policies and procedures.	
التحقق من وجود سياسة صريحة حول كيفية إدارة مفاتيح التشفير (مثل كيفية إصدارها وتوزيعها وإلغائها وانتهاء صلاحيتها) والتحقق من تطبيق هذه السياسة بصورة ملائمة. It shall be verified that there is an explicit policy for how cryptographic keys are managed (for example, generated, distributed, revoked, or expired), and that this policy is properly enforced.	7-6
التحقق من وجود عدم الإنكار(Non-Repudiation) من خلال التشفير (التوقيع الرقمي) للمعاملات المالية والتجارة الإلكترونية والسجلات. It shall be verified that non-repudiation through cryptography (digital signing) is present for financial or e-commerce transactions and records.	8-6
التحقق من حماية كافة مفاتيح التشفير بصورة ملائمة. في حال تعرض المفتاح لانتهاك أمني، فإنه لا يمكن الوثوق به ويجب استبداله أو إلغاؤه. It shall be verified that all cryptographic keys are adequately protected. If a key has been compromised, it shall no longer be trusted and shall be replaced or revoked.	9-6
التحقق من تشفير المعلومات القابلة لتحديد الهوية (PII) والمعلومات المحمية والبيانات المخزنة عندما لا تكون قيد الاستخدام. It shall be verified that Personally Identifiable Information (PII) and protected information and data are stored encrypted at rest.	10-6
التعامل مع الأخطاء وتسجيلها (OWASP:A10:2017 - عدم كفاية وفاعلية التسجيل والمراقبة) Error Handling and Logging (OWASP:A10:2017 – Insufficient Logging & Monitoring)	7
ضمان إجراء التحقق الصريح من الأخطاء للبرمجيات المطورة داخلياً، وتوثيقه لكافة المدخلات، بما في ذلك الحجم ونوع البيانات والنطاقات أو الصيغ المسموحة.	1-7

For in-house developed software, explicit error checking shall be performed and documented for all input, including size, data type, and acceptable ranges or formats.	
التحقق من أن التطبيق لا يظهر رسائل خطأ أو يكدس آثاراً تتضمن معلومات محمية، بما في ذلك هوية الجلسة والمعلومات الشخصية، والتي يمكن أن تساعد الجهة المهاجمة على تنفيذ أنشطتها. It shall be verified that the application does not output error messages or stack traces containing protected data that could assist an attacker, including a session ID and personal information.	2-7
التحقق من تنفيذ جميع عمليات التعامل مع الأخطاء على أجهزة موثوقة. It shall be verified that error handling is performed on trusted devices.	3-7
التحقق من تطبيق كافة ضوابط التسجيل على الخادم. It shall be verified that all logging controls are implemented on the server.	4-7
التحقق من أن منطق التعامل مع الأخطاء في الضوابط الأمنية يحجب الوصول تلقائياً. It shall be verified that error handling logic in security controls denies access by default.	5-7
التحقق من أن ضوابط التسجيل الأمنية تسمح بتسجيل أحداث النجاح والإخفاق التي تم تحديدها باعتبارها مهمة أمنياً. It shall be verified that security logging controls provide the ability to log both success and failure events that are identified as security-relevant.	6-7
التحقق من أن كل حدث في السجل يتضمن ختماً زمنياً من مصدر موثوق، ومستوى شدة الحدث، ومؤشراً على أن الحدث مهم أمنياً (إذا كان مختلطاً مع سجلات أخرى)، وهوية المستخدم الذي تسبب بالحدث (إذا كان هناك مستخدم مرتبط بالحدث)، ومصدر عنوان بروتوكول الإنترنت للطلب المصاحب للحدث سواءً كان الحدث ناجحاً أو فاشلاً، ووصفاً للحدث. It shall be verified that each log event includes a time stamp from a reliable source, severity level of the event, an indication that the event is a security relevant event (if mixed	7-7

with other logs), the identity of the user that caused the event (if there is a user associated with the event), the source IP address of the request associated with the event, whether the event succeeded or failed, and a description of the event.	
التحقق من أن كافة السجلات محمية من الوصول غير المصرح به والتعديل. It shall be verified that all logs are protected from unauthorized access and modification.	8-7
التحقق من أن التطبيق لا يسجل معلومات محمية خاصة بالتطبيق، بما في ذلك هوية الجلسة والمعلومات الشخصية أو المحمية، والتي يمكن أن تساعد الجهة المهاجمة على تنفيذ أنشطتها. It shall be verified that the application does not log application-specific protected data that could assist an attacker, including user's session IDs and personal or protected information.	9-7
التحقق من توفر أداة تحليل السجل مما يسمح للمحلل بالبحث عن أحداث السجل بناءً على تركيبة من معايير البحث في كافة الحقول في صيغة السجل المدعومة من النظام. It shall be verified that a log analysis tool is available which allows an analyst to search for log events based on a combination of search criteria across all fields in the log record format supported by this system.	10-7
التحقق من عدم تنفيذ كافة الأحداث التي تتضمن بيانات غير موثوقة باعتبارها شفرة في برمجيات استعراض السجلات المعنية. It shall be verified that all events that include untrusted data will not execute as code in the intended log viewing software.	11-7
التحقق من وجود تنفيذ تسجيل موحد مستخدم في التطبيق. It shall be verified that there is a single logging implementation that is used by the application.	12-7
التحقق من أن السجلات لها إجراء منتظم موحد للنسخ الاحتياطية أو الأرشفة. It shall be verified that logs have a standard regular procedure for backing up or archiving.	13-7
تطبيق "التعامل مع الاستثناءات في الشفرات" حيثما أمكن.	14-7

“Try catch” shall be implemented where applicable.	
التحقق من أن السجلات أدناه مفعلة: • سجل يشمل كل حالات الإخفاق في التحقق من المدخلات. • سجل يشمل كل محاولات التحقق من الهوية، وخصوصاً حالات الإخفاق. • سجل يشمل كل حالات الإخفاق في التحكم بالوصول. • سجل يشمل كل أحداث التلاعب الظاهرة، بما في ذلك التغييرات غير المتوقعة على حالة البيانات. • سجل يشمل كل محاولات الاتصال بالرموز التعريفية لجلسة منتهية الصلاحية أو غير صحيحة. • سجل يشمل كل استثناءات النظام. • سجل يشمل كل الوظائف الإدارية، بما في ذلك التغييرات على إعدادات الضبط والتهيئة الأمنية. • سجل يشمل كل حالات إخفاق اتصال أمن طبقة النقل بأجهزة النقطة النهائية. • سجل يشمل كل حالات إخفاق نموذج التشفير. It shall be verified that all the below logs are enabled: • Log of all input validation failures • Log of all authentication attempts, especially failures • Log of all access control failures • Log of all apparent tampering events, including unexpected changes to data status. • Log of attempts to connect with invalid or expired session tokens • Log of all system exceptions • Log of all administrative functions, including changes to the security configuration settings • Log of all backend TLS connection failures • Log of cryptographic module failures	15-7
حماية المعلومات (OWASP:A3:2017 - تعرض المعلومات المحمية للمخاطر) Data Protection (OWASP:A3:2017 – Protected Data Exposure)	8
التحقق من إلغاء تفعيل تخزين النماذج التي تتضمن معلومات محمية لدى العميل، بما في ذلك خصائص الإكمال التلقائي.	1-8

It shall be verified that all forms containing protected information have disabled client side caching, including autocomplete features.	
التحقق من إرسال كافة المعلومات المحمية إلى الخادم في متن رسالة بروتوكول نقل النص التشعبي (HTTP)، (أي منع استخدام معايير شريط العنوان "URL" لإرسال البيانات المحمية). It shall be verified that all protected data is sent to the server in the HTTP message body (i.e., URL parameters shall never be used to send protected data).	2-8
التحقق من أن كافة النسخ المخزنة أو المؤقتة للمعلومات المحمية المخزنة على الخادم محمية من الوصول غير المصرح به، والتأكد من حذف الملفات العاملة المؤقتة بمجرد انقضاء الحاجة لها. It shall be verified that all cached or temporary copies of protected data stored on the server are protected from unauthorized access, and that those temporary working files are purged a soon as they are no longer required.	3-8
إلغاء تفعيل التخزين أو حفظ النسخ المؤقتة للصفحات التي تتضمن معلومات محمية لدى العميل، والتحقق من أن هذه النسخ محمية من الوصول غير المصرح به أو مسحها أو إلغاء صلاحيتها بعد وصول المستخدم المصرح له إليها. (يمكن استخدام "Cache-Control: no-store" مع ضابط عنوان بروتوكول نقل النص التشعبي "HTTP". "Pragma: no-cache"، وهو أقل فاعلية، ولكنه متوافق مع النسخ الأقدم "1.0" من بروتوكول نقل النص التشعبي "HTTP"). Client-side caching or temporary copies of pages containing protected data shall be disabled. Additionally, it shall be verified that such copies are protected from unauthorized access or purged/invalidated after an authorized user accesses the protected data). (Cache-Control: no-store, may be used in conjunction with HTTP header control "Pragma: no-cache," which is less effective, but is HTTP/1.0 backward compatible).	4-8
التحقق من تحديد قائمة بالمعلومات المحمية التي يعالجها التطبيق، والتأكد من وجود سياسة صريحة حول كيفية التحكم بالوصول إلى هذه المعلومات، ومتى يجب تشفيرها (أثناء عدم الاستخدام وأثناء النقل والاستخدام)، والتحقق من تطبيق هذه السياسة بصورة ملائمة.	5-8

It shall be verified that the list of protected data processed by the application is identified, and that there is an explicit policy for how access to this data must be controlled, and when this data must be encrypted (both at rest and in transit). Additionally, it shall be verified that such policy is properly enforced.	
التحقق من وجود طريقة لحذف كل أنواع المعلومات المحمية الموجودة في التطبيق عند نهاية فترة الاحتفاظ المطلوبة. It shall be verified that there is a method to remove each type of protected data from the application at the end of its required retention period.	6-8
التحقق من أن التطبيق يقلل عدد المعايير المرسلة إلى الأنظمة غير الموثوقة مثل الحقول المخفية ومتغيرات "Ajax" وملفات الارتباط وقيم العناوين. It shall be verified that the application minimizes the number of parameters sent to untrusted systems, such as hidden fields, Ajax variables, cookies and header values.	7-8
التحقق من قدرة التطبيق على كشف الأرقام غير الطبيعية لطلبات المعلومات والتنبيه بشأنها، أو معالجة المعاملات عالية القيمة لدور المستخدم مثل سحب الشاشة، أو الاستخدام التلقائي لاستخلاص خدمات الويب، أو منع فقدان البيانات. على سبيل المثال، يجب أن لا يكون المستخدم العادي قادراً على الوصول إلى أكثر من 5 سجلات في الساعة أو أكثر من 30 سجلاً في اليوم. It shall be verified that the application has the ability to detect and alert on abnormal numbers of requests for information, or on the processing of high value transactions for a user's role, such as screen scraping, automated use of web service extraction, or data loss prevention. For example, the average user shall not be able to access more than 5 records per hour or 30 records per day.	8-8
التحقق من أن بيانات الاعتماد التي يستخدمها التطبيق على الخادم، مثل اتصال قاعدة البيانات، وكلمة المرور، والمفاتيح السرية للتشفير، ليست مثبتة في الشفرة. ويجب تخزين أي بيانات اعتماد في ملف إعدادات منفصل على نظام موثوق وتشفيرها. It shall be verified that credentials used by the application on the server side; such as database connection, password and encryption secret keys; are not hard coded. Any credentials	9-8

shall be stored in a separate configuration file on a trusted system and shall be encrypted.	
التحقق من أن خصائص الإكمال التلقائي غير مفعلة على النماذج باستثناء النماذج التي تتضمن معلومات محمية، بما في ذلك التحقق من الهوية. It shall be verified that autocomplete features are disabled on forms expected to contain protected information, including authentication.	10-8
أمن الاتصالات (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة) Communication Security (OWASP:A6:2017 – Security Misconfiguration)	9
التحقق من أنه يمكن بناء مسار من جهة إصدار شهادات موثوقة لكل شهادة تشفير خادم أمن طبقة النقل (TLS)، وأنه قد تم التحقق من صلاحية شهادة كل خادم. It shall be verified that a path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and that each server certificate is valid.	1-9
التحقق من استخدام أحدث إصدار من أمن طبقة النقل (TLS) في كافة الاتصالات (بما في ذلك الاتصالات الخارجية واتصالات أجهزة النقطة النهائية) التي تم مصادقتها أو التي تتضمن معلومات أو وظائف محمية. It shall be verified that the latest version of TLS is used for all connections (including both external and backend connections) that are authenticated or involve protected data or functions.	2-9
التحقق من تسجيل حالات إخفاق اتصالات أمن طبقة النقل (TLS) بأجهزة النقطة النهائية. It shall be verified that backend TLS connection failures are logged.	3-9
التحقق من المصادقة على كافة الاتصالات مع الأنظمة الخارجية التي تتضمن معلومات أو وظائف محمية. It shall be verified that all connections to external systems that involve protected information or functions are authenticated.	4-9

5-9	التحقق من أن كافة الاتصالات مع الأنظمة الخارجية التي تتضمن معلومات أو وظائف محمية تستخدم حساباً تم إعداده ومنحه الحد الأدنى من المزايا والصلاحيات اللازمة ليعمل التطبيق بالشكل الصحيح. It shall be verified that all connections to external systems that involve protected information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.
6-9	التحقق من أن اتصالات أمن طبقة النقل (TLS) الفاشلة لا ينتج عنها اتصال غير آمن (غير مشفر). It shall be verified that failed TLS connections do not fall back to an insecure connection.
7-9	التحقق من أن مسارات شهادات التشفير قد تم بناؤها والتحقق منها لكافة شهادات التشفير الخاصة بالعميل باستخدام جهات الصلاحيات الموثوقة ومعلومات الإلغاء. It shall be verified that certificate paths are built and verified for all client certificates using configured trust anchors and revocation information.
8-9	التحقق من وجود تنفيذ أمن طبقة النقل (TLS) موحد يتم استخدامه في التطبيق وتم إعداده ليعمل في نظام عمل معتمد. It shall be verified that there is a single standard TLS implementation that is used by the application and configured to operate in an approved mode of operation.
9-9	التحقق من أن ترميز الرموز المحددة معرف لكافة الاتصالات (مثل "UTF-8"). It shall be verified that specific character encodings are defined for all connections (e.g., UTF-8).
10	أمن البروتوكول (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة و OWASP:A4:2017 لغة الترميز القابلة للامتداد لجهات خارجية) Protocol Security (OWASP:A6:2017 – Security Misconfiguration & OWASP:A4:2017 XML External Entities)
1-10	التحقق من أن التطبيق يقبل مجموعة محددة فقط من طرق طلب بروتوكول نقل النص التشعبي (HTTP) مثل طلب "GET" وطلب "POST" وأن الطرق غير المستخدمة محظورة.

It shall be verified that the application accepts only a defined set of HTTP request methods, such as GET and POST, and that unused methods are explicitly blocked.	
التحقق من أن كل استجابة لبروتوكول نقل النص التشعبي (HTTP) تتضمن عنوان نوع محتوى يحدد مجموعة رموز آمنة (مثل "UTF-8"). It shall be verified that every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8).	2-10
التحقق من أن عناوين بروتوكول نقل النص التشعبي (HTTP) و/أو الآليات الأخرى للمتصفحات الأقدم متضمنة من أجل الحماية من هجمات الخطف بالنقر (Click Jacking). It shall be verified that HTTP headers and/or other mechanisms for older browsers have been included to protect against click jacking attacks.	3-10
التحقق من أن عناوين بروتوكول نقل النص التشعبي (HTTP) في الطلبات والاستجابات تتضمن فقط رموز المدونة الموحدة الأمريكية لتبادل المعلومات القابلة للطباعة (ASCII). It shall be verified that HTTP headers in both requests and responses contain only printable ASCII characters.	4-10
التحقق من استخدام صيغ بيانات أقل تعقيداً مثل جافا سكريبت (JSON)، وتجنب جعل المعلومات المحمية متسلسلة. The use of less complex data formats, such as JSON, shall be verified, and serialization of protected data shall be avoided.	5-10
تحديث وإصلاح أو ترقية معالجات لغة الترميز القابلة للامتداد (XML) والمكتبات قيد الاستخدام في التطبيق أو نظام التشغيل الأساسي، واستخدام عمليات التحقق من الاعتماديات، وتحديث البروتوكول البسيط للوصول إلى الكائنات (SOAP) إلى إصدار 1.2 أو إصدار أحدث. All XML processors and libraries in use by the application or on the underlying operating system shall be patched or upgraded. Additionally, dependency checkers shall be used, and SOAP shall be updated to SOAP 1.2 or higher.	6-10

إلغاء تفعيل لغة الترميز القابلة للامتداد لجهات خارجية ومعالجة "DTD" في كافة محللات لغة الترميز القابلة للامتداد (XML) في التطبيق وفقاً لتوجيهات المشروع المفتوح لأمن تطبيقات الويب "XXE Prevention". XML external entity and DTD processing shall be disabled in all XML parsers in the application, as per OWASP Cheat Sheet "XXE Prevention".	7-10
تطبيق التحقق الإيجابي من المدخلات على الخادم (السماح بقائمة محددة) أو التصفية أو التدقيق لمنع البيانات العدائية ضمن وثائق أو عناوين أو عُقد لغة الترميز القابلة للامتداد (XML). Positive server-side input validation (whitelisting), filtering, or sanitization shall be implemented to prevent hostile data within XML documents, headers, or nodes.	8-10
التحقق من أن وظيفة رفع الملف بلغة الترميز القابلة للامتداد (XML) أو بلغة الأسلوب الموسع (XSL) تتحقق من لغة الترميز القابلة للامتداد (XML) باستخدام تحقق لغة كتابة الملفات المرافقة للغة (XSD) أو طريقة تحقق مشابهة. It shall be verified that XML or XSL file upload functionality validates incoming XML using XSD validation or similar.	9-10
استخدام أدوات اختبار أمن التطبيقات الثابت (SAST) واختبار أمن التطبيقات الديناميكي (DAST) للمساعدة في كشف لغة الترميز القابلة للامتداد لجهات خارجية (XXE) في الشفرة المصدرية، مع الأخذ بعين الاعتبار أن مراجعة الشفرة يدوياً هي الطريقة التي يفضل اتباعها في التطبيقات الكبيرة والمعقدة ذات العديد من التداخلات. SAST and DAST tools shall be used to help detect XXE in source code, although manual code review is the best alternative in large and complex applications with many integrations.	10-10
إذا كان من غير الممكن تطبيق هذه الضوابط، يجب دراسة استخدام حزم التحديثات الافتراضية، أو البوابات الأمنية لواجهات برمجة التطبيقات، أو جدار الحماية لتطبيقات الويب لكشف هجمات لغة الترميز القابلة للامتداد لجهات خارجية (XXE) ومراقبتها وحجبها. If the implementation of these controls is not possible, the use of virtual patching, API security gateways, or Web Application Firewalls (WAFs) shall be considered to detect, monitor, and block XXE attacks.	11-10

الشفرة الخبيثة والثغرات (OWASP:A9:2017 - استخدام المكونات مع الثغرات المعروفة) Malicious Code and Vulnerabilities (OWASP:A9:2017 – Using Components with Known Vulnerabilities)	11
التحقق من عدم وجود شفرات خبيثة في أي شفرة تم تطويرها أو تعديلها بهدف إنشاء التطبيق. It shall be verified that no malicious code is in any code that was either developed or modified in order to create the application.	1-11
التأكد من أن سلامة الشفرة المفسرة والمكتبات والأوامر التنفيذية وملفات الإعدادات قد تم التحقق منها باستخدام المجموعات الاختبارية أو عمليات حساب ملخص النص المميز. It shall be ensured that the integrity of interpreted code, libraries, executables, and configuration files is verified using checksums or hashes.	2-11
التحقق من أن كافة الشفرات التي تطبق ضوابط التحقق من الهوية أو تستخدمها لم تتأثر بأي شفرات خبيثة. It shall be verified that all code implementing or using authentication controls is not affected by any malicious code.	3-11
التحقق من أن كافة الشفرات التي تطبق إدارة الجلسات أو تستخدمها لم تتأثر بأي شفرات خبيثة. It shall be verified that all code implementing or using session management controls is not affected by any malicious code.	4-11
التحقق من أن كافة الشفرات التي تطبق ضوابط الوصول أو تستخدمها لم تتأثر بأي شفرات خبيثة. It shall be verified that all code implementing or using access controls is not affected by any malicious code.	5-11
التحقق من أن كافة ضوابط التحقق من المدخلات لم تتأثر بأي شفرات خبيثة. It shall be verified that all input validation controls are not affected by any malicious code.	6-11

7-11	التحقق من أن كافة الشفرات التي تطبق ضوابط التحقق من المخرجات أو تستخدمها لم تتأثر بأي شفرات خبيثة. It shall be verified that all code implementing or using output validation controls is not affected by any malicious code.
8-11	التحقق من أن كافة الشفرات التي تطبق نموذج التشفير أو تستخدمه لم تتأثر بأي شفرات خبيثة. It shall be verified that all code supporting or using a cryptographic module is not affected by any malicious code.
9-11	التحقق من أن كافة الشفرات التي تطبق ضوابط التعامل مع الأخطاء وتسجيلها أو تستخدمها لم تتأثر بأي شفرات خبيثة. It shall be verified that all code implementing or using error handling and logging controls is not affected by any malicious code.
10-11	التحقق من أن كافة الأنشطة الخبيثة قد خضعت لتقنية الحماية المعزولة (Sandboxing). It shall be verified all malicious activity is adequately sandboxed.
11-11	التحقق من التخلص من المعلومات المحمية المخزنة في الذاكرة بسرعة عند عدم الحاجة لها. It shall be verified that protected data is rapidly sanitized from memory as soon as it is no longer needed.
12-11	تحديث المكونات بأحدث التحديثات والإصلاحات عند معرفة المستخدم بالثغرات المنشورة. Components shall be updated with the latest patches as soon as a user knows about published vulnerabilities.
13-11	إلغاء الاعتماديات غير المستخدمة والخصائص غير اللازمة والمكونات والملفات والوثائق. Unused dependencies, unnecessary features, components, files, and documentation shall be removed.
14-11	عمل قائمة جرد مستمرة لإصدارات المكونات من طرف العميل والخادم (مثل أطر العمل والمكتبات) واعتمادياتها باستخدام أدوات مثل الإصدارات،

	و"DependencyCheck"، و"retire.js"، وغيرها، والمراقبة المستمرة للمصادر مثل تعداد الثغرات الشائعة (CVE) وقاعدة بيانات الثغرات الوطنية (NVD) بحثاً عن الثغرات في المكونات، إلى جانب استخدام أدوات تحليل تكوين البرمجيات من أجل أتمتة العملية، والاشتراك في تنبيهات البريد الإلكتروني من أجل الثغرات الأمنية ذات العلاقة بالمكونات قيد الاستخدام. Versions of both client-side and server-side components, (e.g., frameworks and libraries), and their dependencies shall be continuously inventoried using tools such as versions, DependencyCheck, retire.js, etc. Additionally, sources such as CVE and NVD, shall be continuously monitored for vulnerabilities in the components, and software composition analysis tools shall be used to automate the process. Subscription to email alerts for security vulnerabilities related to the used components shall be ensured as well.
15-11	الحصول على المكونات من مصادر رسمية وعبر روابط محمية فقط، وتفضيل الحزم الموقعة لتقليل فرص وجود مكون خبيث معدل. Components shall be obtained from official sources and over secure links only. Signed packages shall be preferred to reduce the chance of including a modified, malicious component.
16-11	مراقبة المكتبات والمكونات التي لا تتوافر لها صيانة أو ليس للإصدارات القديمة منها تحديثات وإصلاحات أمنية. إذا كان تثبيت حزم التحديثات غير ممكناً، يجب دراسة تثبيت التحديثات والإصلاحات الافتراضية لمراقبة المشكلات المكتشفة أو كشفها أو الحماية منها. Libraries and components that are unmaintained or do not create security patches for older versions shall be monitored. If patching is not possible, deploying a virtual patch to monitor, detect, or protect against the discovered issue shall be considered.
12	قواعد العمل (Business Logic)
1-12	التحقق من عمليات التطبيق ومن كافة تدفقات قواعد العمل عالية القيمة في بيئة موثوقة مثل الخادم المحمي والمراقب.

Application processes and all high value business logic flows shall be verified in a trusted environment, such as on a protected and monitored server.	
التحقق من أن التطبيق لا يسمح بمعاملات عالية القيمة منتحلة، مثل السماح للمستخدم المهاجم (أ) بمعالجة معاملة باعتباره المستخدم الضحية (ب) من خلال التلاعب أو إعادة إعداد الجلسة أو حالة المعاملة أو هوية المستخدم أو المعاملة. It shall be verified that the application does not allow spoofed high value transactions, such as allowing Attacker User A to process a transaction as Victim User B, by tampering with or replaying session, transaction state, transaction or user IDs.	2-12
التحقق من أن التطبيق لا يسمح بالتلاعب بمعايير قواعد العمل عالية القيمة والتي تشمل، على سبيل المثال لا الحصر، السعر، والفائدة، والخصومات، والمعلومات القابلة لتحديد الهوية (PII)، والأرصدة، وهويات الأسهم، وغيرها. It shall be verified that the application does not allow high value business logic parameters to be tampered with, which include, but are not limited to, price, interest, discounts, PII, balances, stock IDs, etc.	3-12
التحقق من وجود إجراءات دفاعية في التطبيق للحماية من هجمات الإنكار، حيث تشمل هذه الإجراءات سجلات المعاملات المحمية والقابلة للتحقق، وسجلات التدقيق أو سجلات النظام، وفي الأنظمة ذات القيمة الأعلى، المراقبة المباشرة لأنشطة المستخدم والمعاملات بحثاً عن أي أنشطة غير طبيعية. It shall be verified that the application has defensive measures; such as verifiable and protected transaction logs, audit trails or system logs, and, in the highest value systems, real time monitoring of user activities and transactions for anomalies; to protect against repudiation attacks.	4-12
التحقق من أن التطبيق يوفر الحماية من هجمات الإفصاح عن المعلومات مثل مرجعيات الكائنات المباشرة، والتلاعب، واستخدام الهجمات التخمينية لاختراق الجلسة، وأنواع الهجمات الأخرى. It shall be verified that the application protects against information disclosure attacks, such as direct object reference, tampering, session brute force or other attacks.	5-12

6-12	التحقق من وجود ضوابط كشف وضبط كافية في التطبيق للحماية من الهجمات التخمينية (مثل الاستخدام المستمر لدالة معينة) أو هجمات حجب الخدمة. It shall be verified that the application has sufficient detection and governor controls to protect against brute force (such as the continuous use of a particular function) or denial of service attacks.
7-12	التحقق من وجود ضوابط وصول كافية في التطبيق لمنع هجمات رفع مستوى المزايا والصلاحيات، وتشمل هذه الضوابط منع المستخدمين المجهولين من الوصول إلى البيانات المحمية أو الدالات المحمية، أو منع المستخدمين من الوصول إلى معلومات المستخدمين الآخرين، أو استخدام وظائف ذات مزايا وصلاحيات هامة وحساسة. It shall be verified that the application has sufficient access controls to prevent elevation of privilege attacks. Such controls shall include preventing anonymous users from accessing secured data or secured functions, and preventing users from accessing each other's details or using privileged functions.
8-12	التحقق من أن التطبيق يعالج دفعات قواعد العمل في خطوات متتالية فقط، بحيث تتم معالجة كافة الخطوات مباشرة، وتجنب المعالجة بطريقة غير منتظمة أو التجاوز عن أي خطوات، أو معالجة خطوات مستخدم آخر أو المعاملات المقدمة بسرعة. It shall be verified that the application processes business logic flows in sequential steps only, with all steps being processed directly. Additionally, the application shall be verified not to process out of order, skip steps, process steps from another user, or process transactions submitted quickly.
9-12	التحقق من أن التطبيق يتضمن تصاريح وصلاحيات إضافية (مثل تحقق الإعداد أو التحقق من الهوية المتغير) لأنظمة القيم المتدنية و/أو فصل المهام للتطبيقات ذات القيم المرتفعة لإنفاذ ضوابط مكافحة الاحتيال وفقاً لمخاطر التطبيق وعمليات الاحتيال السابقة. It shall be verified that the application has additional authorization (such as step up or adaptive authentication) for lower value systems, and/or segregation of duties for high value applications, to enforce anti-fraud controls as per the risk of application and past fraud.

التحقق من أن للتطبيق حدود عمل يطبقها في موقع موثوق (كتطبيقها على خادم محمي) على كل مستخدم أو بشكل يومي، والتي تتضمن تنبيهات قابلة للإعداد واستجابات تلقائية للهجمات التلقائية أو غير الاعتيادية. It shall be verified that the application has business limits and enforces them in a trusted location (e.g., on a protected server) on a per user or per day basis, with configurable alerting and automated reactions to automated or unusual attack.	10-12
الملفات والمصادر (OWASP:A9:2017 - استخدام المكونات تحتوي ثغرات معروفة) Files and Resources (OWASP:A9:2017 – Using Components with Known Vulnerabilities)	13
التحقق من أن إعادة التوجيه والإرسال في شريط العنوان (URL) لا تتضمن بيانات غير مصرحة. It shall be verified that URL redirects and forwards do not include unvalidated data.	1-13
التحقق من توحيد أسماء الملفات وبيانات المسارات التي يتم الحصول عليها من مصادر غير موثوقة لإلغاء هجمات تجاوز المسار. It shall be verified that filenames and path data obtained from untrusted sources are canonicalized to eliminate path traversal attacks.	2-13
التحقق من فحص الملفات التي يتم الحصول عليها من مصادر غير موثوقة من خلال برامج مكافحة الفيروسات لمنع تحميل برمجيات خبيثة معروفة. It shall be verified that files obtained from untrusted sources are scanned by antivirus scanners to prevent the upload of known malicious content.	3-13
التحقق من عدم استخدام المعايير التي تم الحصول عليها من مصادر غير موثوقة للتلاعب في أسماء الملفات أو أسماء المسارات أو ملفات وكائنات النظام دون توحيدها أولاً والتحقق من مدخلاتها لمنع هجمات إدراج الملفات المحلية. It shall be verified that parameters obtained from untrusted sources are not used in manipulating filenames, pathnames	4-13

or any file system object without first being canonicalized and input validated to prevent local file inclusion attacks.	
التحقق من توحيد المعايير التي تم الحصول عليها من مصادر غير موثوقة والتحقق من مدخلاتها وترميز مخرجاتها لمنع هجمات إدراج الملفات عن بعد، خصوصاً عندما يكون من الممكن تنفيذ المدخلات مثل العناوين أو المصادر أو إدراج القوالب. It shall be verified that parameters obtained from untrusted sources are canonicalized, input validated, and output encoded to prevent remote file inclusion attacks, particularly where input could be executed, such as header, source, or template inclusion.	5-13
التحقق من عدم السماح بإدراج محتوى عشوائي عن بعد عند مشاركة موارد "IFRAMEs" و"HTML 5" عبر النطاقات. It shall be verified that sharing remote IFRAMEs and HTML 5 resources across domains does not allow the inclusion of arbitrary remote content.	6-13
التحقق من تخزين الملفات التي تم الحصول عليها من مصادر غير موثوقة خارج "Webroot". It shall be verified that files obtained from untrusted sources are stored outside the webroot.	7-13
التحقق من إعداد وضبط خادم الويب أو التطبيق تلقائياً لحجب الوصول إلى المصادر البعيدة أو الأنظمة خارج خادم الويب أو التطبيق. It shall be verified that web or application server is configured by default to deny access to remote resources or systems outside the web or application server.	8-13
التحقق من أن شفرة التطبيق لا تنفذ بيانات مرفوعة تم الحصول عليها من مصادر غير موثوقة. It shall be verified the application code does not execute uploaded data obtained from untrusted sources.	9-13

10-13	التحقق من ضبط إعدادات مشاركة مصادر تطبيقات "Flash" أو "Silverlight" أو غيرها من تطبيقات الإنترنت الغنية (RIA) عبر النطاقات بحيث تمنع الوصول غير المصرح به أو الوصول عن بعد غير المعتمد. It shall be verified that Flash, Silverlight or other Rich Internet Application (RIA) cross-domain resource sharing configuration is set to prevent unauthenticated or unauthorized remote access.
11-13	التحقق من أن كافة أنواع الملفات المسموح برفعها مقتصرة على غايات العمل وحسب الحاجة (مثل ملفات "PDF" ومستندات برامج "Office"). It shall be verified that file types allowed for upload are limited to business purpose and needs only (e.g., PDF and office documents).
12-13	التأكد من أن التحقق من نوع الملف يتم من خلال التحقق من عناوين الملفات وليس من خلال اسم امتداد الملفات فقط. It shall be verified that file type validation is performed not only by checking file headers but also by checking file extension names.
13-13	التحقق من عدم تفعيل امتيازات وصلاحيات التنفيذ في أدلة تحميل الملفات. It shall be verified that execution privileges are turned off on file upload directories.
14-13	التحقق من ضبط إعدادات ملفات ومصادر التطبيق تلقائياً على وضعية القراءة فقط. It shall be verified that application files and resources are read-only by default.
15-13	التحقق من إلغاء كافة أنواع المشاركات والمشاركات الإدارية غير اللازمة، وتقييد الوصول إلى المشاركات أو جعله يتطلب التحقق من الهوية. It shall be verified that all unnecessary shares and administrative shares are removed, and that access to required shares is either restricted or requires authentication.
16-13	طلب التحقق من الهوية قبل السماح برفع الملفات.

Authentication shall be required before allowing a file to be uploaded.	
وضع حد على حجم الملفات التي يمكن رفعها والذي يجب ألا يتجاوز الحجم المطلوب لغايات العمل (على سبيل المثال، 1 ميغابايت كحد أعلى)، وإضافة ملاحظة على صفحة الويب تخص أحجام الملفات المقبولة. Size of files that can be uploaded shall be limited to the size that is needed for business purposes only (for example, maximum 1 MB), and a note shall be added on the web page for the accepted file sizes.	17-13
التحقّق من الهاتف المحمول (Mobile Verification)	14
التأكد من تحقق العميل من شهادات تشفير طبقة المنافذ الآمنة (SSL). It shall be verified that the client validates SSL certificates.	1-14
التحقق من عدم استخدام قيم رقم تعريف الجهاز المميز (UDID) كضوابط أمنية. It shall be verified that Unique Device ID (UDID) values are not used as security controls.	2-14
التحقق من أن تطبيق الهاتف المحمول لا يخزن المعلومات المحمية على المصادر المشتركة على الجهاز (مثل بطاقة "SD" أو المجلدات المشتركة). It shall be verified that the mobile application does not store protected data on shared resources on a device (for example, on SD card or shared folders).	3-14
التحقق من أن المعلومات المحمية ليست مخزنة في قاعدة بيانات "SQLite" على الجهاز. It shall be verified that protected data is not stored on SQLite database on the device.	4-14
التحقق من أن المفاتيح السرية وكلمات المرور ليست مثبتة في الشفرة في البرامج التنفيذية. It shall be verified that secret keys or passwords are not hard coded in the executable.	5-14

6-14	التحقق من أن تطبيق الهاتف المحمول يمنع تسرب المعلومات المحمية عن طريق خاصية التصوير التلقائي في نظام تشغيل "iOS". It shall be verified that the mobile application prevents the leakage of protected data via iOS autosnapshot feature.
7-14	التحقق من أن التطبيق لا يمكن تشغيله على جهاز تم إلغاء القيود الموجودة عليه (Jailbroken) أو جهاز يتمتع بصلاحيات ومزايا هامة وحساسة (Rooted). It shall be verified that the application cannot be run on a jailbroken or rooted device.
8-14	التحقق من أن وقت انتهاء الجلسة له قيمة منطقية. It shall be verified that the session timeout is of a reasonable value.
9-14	التحقق من التصاريح التي يتم طلبها ومن المصادر التي يتم منح تصاريح الوصول إليها (AndroidManifest.xml، وiOS Entitlements). Requested permissions, as well as the resources authorized to be accessed (i.e., AndroidManifest.xml, iOS Entitlements), shall be verified.
10-14	التحقق من أن سجلات انهيار النظام لا تتضمن معلومات محمية. It shall be verified that crash logs do not contain protected data.
11-14	التحقق من عدم وضوح النظام الثنائي في التطبيق. It shall be verified that the application binary has been obfuscated.
12-14	التحقق من أن كافة بيانات الاختبار قد تم إزالتها من حاوية التطبيق (.apk .bar .ipa). It shall be verified that all test data has been removed from the application container (.ipa .apk .bar).
13-14	التحقق من أن التطبيق لا يقوم بتسجيل المعلومات المحمية على سجل النظام أو ملفات النظام. It shall be verified that the application does not log protected data to the system log or filesystem.

14-14	التحقق من أن التطبيق لا يتيح الإكمال التلقائي للنصوص الحساسة في حقول المدخلات مثل حقول كلمات المرور أو المعلومات الشخصية أو بطاقات الائتمان. It shall be verified that the application does not enable autocomplete for sensitive text input fields, such as password, personal information or credit card fields.
15-14	التحقق من أن تطبيق الهاتف المحمول يطبق عملية تثبيت الشهادات (Certificate Pinning) لمنع إدارة حركة البيانات في التطبيق بالوكالة. It shall be verified that the mobile application implements certificate pinning to prevent the proxying of application traffic.
16-14	التحقق من عدم وجود إعدادات خاطئة في ملفات الإعدادات (مجموعة العلامات التصحيحية، وتصاريح قابلة للقراءة وللكتابة العالمية). It shall be verified that no misconfigurations are present in the configuration files (Debugging flags set, world readable/writable permissions).
17-14	التحقق من تحديث مكتبات الأطراف الخارجية قيد الاستخدام وعدم احتوائها على أي ثغرات معروفة. It shall be verified that all third party libraries in use are up to date, and contain no known vulnerabilities.
18-14	التحقق من عدم تخزين بيانات الويب مثل حركة بيانات بروتوكول نقل النص التشعبي الآمن (HTTPS). It shall be verified that web data, such as HTTPS traffic, is not cached.
19-14	التحقق من عدم استخدام سلسلة الأحرف للاستفسار (Query String) مع المعلومات المحمية. بدلاً من ذلك، يجب استخدام طلب "POST" عبر طبقة المنافذ الآمنة (SSL) مع رمز تعريفي للحماية من تزوير الطلب عبر المواقع (CSRF). It shall be verified that the query string is not used for protected data. Instead, a POST request via SSL shall be used with a CSRF token.
20-14	التحقق، إن أمكن، من أن أرقام الحسابات الشخصية متقطعة قبل تخزينها على الجهاز.

It shall be verified that, if applicable, any personal account numbers are truncated prior to storing them on a device.	
التحقق من أن التطبيق يستفيد من خاصية التوزيع العشوائي لمخطط مساحات العناوين (ASLR). It shall be verified that the application makes use of Address Space Layout Randomization (ASLR).	21-14
التحقق من أن البيانات المسجلة عن طريق لوحة المفاتيح (iOS) لا تتضمن بيانات اعتماد أو معلومات مالية أو معلومات محمية أخرى. It shall be verified that data logged via the keyboard (iOS) does not contain credentials, financial information or other protected data.	22-14
في تطبيقات الأندرويد، التحقق من أن التطبيق لا ينشئ ملفات بتصاريح " MODE_WORLD_READABLE " أو " MODE_WORLD_WRITABLE ". For Android applications, it shall be verified that the application does not create files with permissions of MODE_WORLD_READABLE or MODE_WORLD_WRITABLE.	23-14
التحقق من تخزين المعلومات المحمية بطريقة مشفرة وآمنة (حتى عند تخزينها في سلسلة مفاتيح "iOS"). It shall be verified that protected data is stored in a cryptographically secure manner (even when stored on iOS keychain).	24-14
التحقق من تطبيق آليات مكافحة التصحيح والهندسة العكسية في التطبيق. It shall be verified that anti-debugging and reverse engineering mechanisms are implemented in the application.	25-14
التحقق من أن التطبيق لا يستورد أنشطة حساسة أو مزودي محتوى أو غيرهم على الأندرويد. It shall be verified that the application does not export sensitive activities, intents, content providers, etc. on Android.	26-14

التحقق من استخدام هيكليات متغيرة لسلاسل الحروف العشوائية (Strings) الحساسة مثل أرقام الحسابات، والكتابة فوقها عند عدم استخدامها (لتقليل الأضرار الناجمة عن هجمات تحليل الذاكرة). It shall be verified that mutable structures have been used for sensitive strings such as account numbers and are overwritten when not used, (to mitigate damage from memory analysis attacks).	27-14
التأكد من تنفيذ التحقق الكامل من البيانات على المدخلات لأي رسائل أنشطة ومزودي محتوى ومتلقي بث معرضين للمخاطر (الأندرويد). It shall be verified that any exposed intents, content providers and broadcast receivers perform full data validation on input (Android).	28-14
أمن قواعد البيانات (OWASP:A6:2017 - الإعدادات الأمنية الخاطئة) Database Security (OWASP:A6:2017 – Security Misconfiguration)	15
التحقق من استخدام الاستفسارات المضبوطة بمعايير لمنع حقن تعليمات الاستعلام البنيوية (SQL Injection). It shall be verified that parameterized queries are used to prevent SQL Injection.	1-15
التحقق من استخدام بيانات اعتماد معقدة وآمنة للوصول إلى قواعد البيانات. It shall be verified that strong and secure credentials are used for database access.	2-15
التحقق من أن التطبيق الذي يصل إلى قواعد البيانات يمتلك أدنى مستوى ممكن من الامتيازات والصلاحيات المطلوبة. It shall be verified that the application accessing the database uses the lowest possible level of privileges required.	3-15
التحقق من أن سلاسل الحروف العشوائية (Strings) للاتصال ليست مثبتة في الشفرة ضمن التطبيق، خصوصاً بيانات اعتماد التحقق من الهوية من قاعدة البيانات. It shall be verified that connection strings are not hard coded within the application, especially database authentication credentials.	4-15

5-15	التحقق من إغلاق الاتصال بقاعدة البيانات بأسرع ما يمكن. It shall be verified that the connection to the database is closed as soon as possible.
6-15	التحقق من حذف كافة وظائف قاعدة البيانات غير اللازمة أو غير المستخدمة أو إلغاء تفعيلها، بما في ذلك محتوى المورد التلقائي، وتثبيت الحد الأدنى من الخصائص والخيارات اللازمة لعمل التطبيق. على سبيل المثال، إلغاء تفعيل الإجراءات أو الخدمات المخزنة وحزم الخصائص المفيدة غير اللازمة. It shall be verified that all unnecessary and unused database functionalities, including default vendor content, have been turned off or disabled. Only the minimum set of features and options required for the application to function shall be installed. For example, unnecessary stored procedures or services and utility packages, shall be disabled.
7-15	التحقق من إلغاء تفعيل أي حسابات تلقائية أو غير ضرورية والتي يمكن من خلالها الوصول إلى قواعد البيانات غير اللازمة لدعم متطلبات الأعمال. It shall be verified that any default or unnecessary accounts with access to databases that are not required to support business requirements are disabled.
8-15	التحقق من أن التطبيق يستخدم بيانات اعتماد مختلفة لكل ميزة وصلاحية (مثل مستخدم، ومستخدم للقراءة فقط، وضيف، ومشرفين) عند اتصاله بقاعدة البيانات. It shall be verified that the application connects to the database with different credentials for every trust distinction and accountability (for example, user, read-only user, guest, administrators).
9-15	التحقق من إلغاء تفعيل تسجيل الدخول عن بعد والجلسات المجهولة إذا لم يكن هناك حاجة إليها. It shall be verified that remote logons and null sessions are disabled if not needed.
10-15	بالنسبة للتطبيقات التي تعتمد على قاعدة بيانات، يجب استخدام قوالب الإعداد والتحصين الموحدة، واختبار جميع الأنظمة التي تعتبر جزءاً من إجراءات العمل الحساسة.

For applications that rely on a database, standard hardening configuration templates shall be used, and all systems that are part of critical business processes shall be tested.	

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني بجامعه حائل

2- **مراجعة وتحديث المعيار:** إدارة الأمن السيبراني

3- **تنفيذ وتطبيق المعيار:** عمادة تقنية المعلومات والتعليم الإلكتروني

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني بجامعه حائل ضمان التزام جامعه حائل بهذا المعيار باستمرار.

2- يجب على عمادة تقنية المعلومات والتعليم الإلكتروني و إدارة الأمن السيبراني في جامعه حائل الالتزام بهذا المعيار.

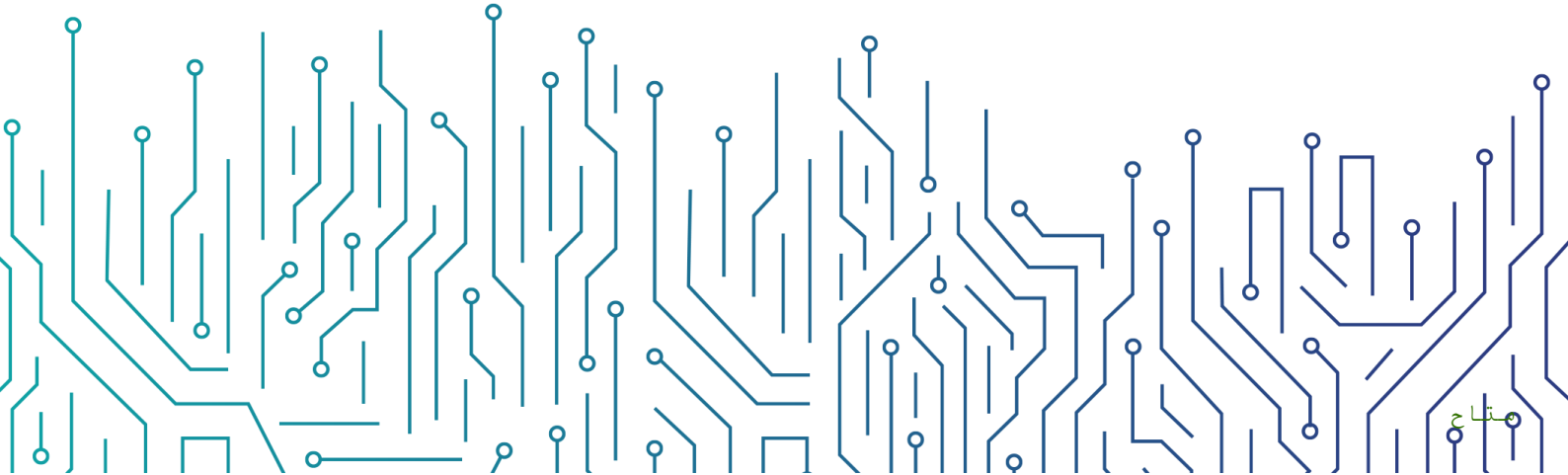
3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعه حائل

جامعة حائل
University of Ha'il

نموذج معيار حماية تطبيقات الويب

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني



متاح

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية تطبيقات الويب الخارجية الخاصة بـجامعه حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ١-١٥-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع تطبيقات الويب الخارجية الخاصة جامعه حائل وينطبق على جميع العاملين في جامعه حائل.

المعايير

1	إدارة هويات الدخول (Access Management)
الهدف	ضمان حماية تطبيقات الويب من الوصول غير المصرح به.
المخاطر المحتملة	يترتب على الوصول غير المصرّح به لتطبيقات الويب مخاطر كبيرة قد تؤدي إلى تسرب أو سرقة المعلومات، وقد تساعد هذه المعلومات في تنفيذ المزيد من الهجمات السيبرانية ضد البنية التحتية لـجامعه حائل
الإجراءات المطلوبة	
1-1	استخدام مبدأ الحد الأدنى من الصلاحيات والامتيازات "Principle of Least Privilege" الذي يمنح المستخدمين الحد الأدنى من صلاحيات الوصول إلى تطبيقات الويب الخارجية. Security Principle of Least Privilege shall be applied to provide users with least privileged access permissions to external web applications.
2-1	حصر الوصول إلى المكونات التقنية الخاصة بالويب وتطبيقات الويب حسب الأدوار الوظيفية (مثل: مشرفو النظام، ومسؤولو دعم التطبيقات، وغيرها) وذلك باستخدام الحسابات الفردية لتلك الأدوار فقط. بالإضافة إلى ذلك، استخدام قوائم التحكم بالوصول

	إلى الشبكة (ACL) التي تعتمد على عناوين بروتوكولات الإنترنت (IP Address) الخاصة بأجهزة المستخدمين. Access to web applications and technical equipment shall be restricted to the required job roles (e.g., system administrator, deployment engineer, developer, etc.) by using the individual accounts for these roles only. In addition, network Access-Control Lists (ACLs) which use the IPs of users' workstations shall be used only.
3-1	إيقاف أو حذف الحسابات الافتراضية غير المستخدمة. Non-interactive or unused default and virtual accounts shall be removed or disabled.
4-1	إلى جانب ضرورة إدخال اسم المستخدم وكلمة المرور، إلزام المستخدم باستعمال التحقّق من الهوية متعدّد العناصر باستخدام آليات أخرى للتحقّق من الهوية مثل الخصائص الحيوية والمفاتيح المادية وكلمات المرور المؤقتة والبطاقات الذكية وشهادات التشفير، وغيرها. Besides a user/password combination, users shall be required to implement multi-factor authentication using a different authentication mechanism such as biometrics, hardware keys, one-time passwords, smart cards, certificates, etc.
5-1	استخدام كلمة مرور معقدة للدخول إلى تطبيقات الويب وفقاً لسياسة إدارة هويات الدخول والصلاحيات في جامعه حائل Complex passwords shall be used for web applications, in accordance with Hail University's Identity and Access Management Policy.
6-1	ضبط إعدادات تطبيقات الويب الخاصة بالأنظمة الحساسة من خلال تحديد وقت انتهاء مهلة الجلسة وإقفالها عند عدم الاستخدام (على سبيل المثال، لمدة 5 دقائق). Session timeout and session idle lockout on web applications shall be configured for critical systems (e.g., 5 minutes).
2	هندسة تطبيقات الويب (Web Application Architecture)

الهدف	تحديد متطلبات الأمن السيبراني في بناء تطبيقات الويب وتصميمها وتطبيقها بشكل آمن وفعال.
المخاطر المحتملة	قد يسبب البناء العشوائي لتطبيقات الويب مخاطر أمنية حساسة يمكن استغلالها في الهجمات السيبرانية التي قد تؤثر على أعمال جامعه حائل
الإجراءات المطلوبة	
1-2	تنفيذ البنية التحتية لتطبيقات الويب للأنظمة الحساسة باستخدام مبدأ البنية متعددة الطبقات (3 مستويات على الأقل)، أو معمارية الخدمات الصغيرة المحمية بجدار حماية ثنائي الطبقة. وتحديداً، إدراج **خادم الويب** في منطقة الإنترنت المحايدة، و**خوادم تطبيقات الويب** في منطقة الإنتاج، و**خوادم قواعد البيانات** في المنطقة الموثوقة أو منطقة قاعدة البيانات. Web applications for critical systems infrastructure following at least 3-tier security architecture or micro-services architecture protected by a dual layer of firewalls shall be implemented. More specifically, **webservers** shall be placed in the Internet DMZ, **web application servers** shall be placed in the Production Zone, and **database servers** shall be placed in the Trusted/Database zone.
2-2	تطبيق العزل المادي أو المنطقي لتطبيقات الويب الحساسة عن التطبيقات أو الأنظمة الأخرى. فعلى سبيل المثال، يمكن تحقيق العزل المادي من خلال استضافة تطبيقات الويب في بيئة مادية منفصلة ومختلفة تماماً، في حين يمكن تحقيق العزل المنطقي من خلال إدراج تطبيقات الويب في مناطق منفصلة داخل الشبكة دون السماح بالوصول إليها من أي منطقة أخرى. Logical or physical isolation of critical web applications from other web applications or systems shall be implemented. For example, physical isolation can be achieved by hosting web applications in a completely different separate physical environment, while logical isolation can be achieved by implementing web applications in a separate zone inside the network without allowing access from any other zone.
3-2	عزل تطبيقات الويب الخاصة بالإنتاج منطقياً عن بيئة الاختبار وبيئة التطوير باستخدام محددات الشبكة عن طريق ضبط إعدادات قوائم التحكّم بالوصول (ACL) والسياسات الأمنية على جدران الحماية. Production web applications shall be logically isolated from test and development environments using network

	restrictions by configuring Access-Control Lists (ACLs) and security policies on firewalls.
4-2	تقييد الوصول عبر الشبكة لتطبيقات الويب وحصره بمنطقة خوادم الويب، ومنطقة خوادم تطبيقات الويب، ومنطقة الإدارة. Network access to web applications shall be restricted to web servers zones, web applications server zones and management server zone.
5-2	تثبيت جدار الحماية لتطبيقات الويب (WAF) على خوادم تطبيقات الويب للتحقق من حركة البيانات الواردة والمصادقة عليها، وتسجيل أي حركة بيانات غير مصرح بها وحجبها، حيث تعمل أجهزة جدار الحماية لتطبيقات الويب (WAF)على كشف هجمات الويب أو هجمات التطبيقات على الخدمات الخارجية وتطبيقات الويب أو حجبها. (بالإضافة إلى ذلك، إعداد جدار الحماية لتطبيقات الويب (WAF) لتمكين خاصية التحكم ببروتوكول الإنترنت وخصائص الموقع الجغرافي لبروتوكول الإنترنت من أجل حجب بروتوكولات الإنترنت المحظورة ودول معينة). A Web Application Firewall (WAF) shall be deployed in front of all web application servers to verify and validate the traffic going to the server. Since WAF devices detect or block web-based and application-based attacks on external-facing services and web applications, any unauthorized traffic shall be blocked and logged. (Additionally, WAF shall be configured to enable IP the intelligence feature and IP geo-location features in order to block blacklisted IPs and specific countries).
6-2	إعداد جدار الحماية لتطبيقات الويب (WAF) للحد من أعلى المخاطر الشائعة التي تستهدف تطبيقات الويب الصادرة عن المشروع المفتوح لأمن تطبيقات الويب (OWASP Top Ten) على تطبيقات الويب الحساسة وفقاً للمعايير والإجراءات ذات العلاقة في جامعه حائل Configure WAF to mitigate the Open Web Application Security Project (OWASP Top Ten) web applications security risks for critical web applications as per Hail University's relevant standards.
7-2	ضبط إعدادات نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات (IPS) وجدار الحماية لتطبيقات الويب (WAF) لإتاحة التواقيع التي تطابق سلوك وبروتوكولات

	تطبيقات الويب (مثل Oracle OHS، وIIS، وApache، وSQL، وXML، وغيرها). IPS and WAF shall be configured to enable signatures that match the web application behavior and protocols (e.g., Oracle OHS, IIS, Apache, SQL, XML, etc.).
8-2	ضبط إعدادات تقنيات الحماية من البرمجيات الضارة وأنظمة الحماية من التهديدات المتقدمة المستمرة للتحقق من كافة عمليات نقل الملفات المرتبطة بتطبيقات الويب بحثاً عن أي ملفات خبيثة وفقاً لسياسة ومعيار الحماية من البرمجيات الضارة المعتمدين في جامعه حائل Malware protection solution and APT systems shall be configured to check all file transfer operations related to web applications for malicious files as per Hail University's Malware Protection Policy and Standard.
9-2	ضبط إعدادات تقنيات وأنظمة حماية تطبيقات الويب لتتبع نموذجاً أمنياً إيجابياً أو نموذج السماح بقائمة محددة من التطبيقات، وذلك من خلال السماح بأنواع محددة من عمليات نقل الملفات، وبروتوكولات ومنافذ محددة، وتطبيقات ويب محددة من المستوى 7، ومتغيرات تطبيقات ويب محددة، وحجب جميع التطبيقات والملفات التي لم يتم ضبط إعداداتها. Web application security solutions and systems shall be configured to follow a positive security model or whitelisting model by allowing only specific file types for transfer, specific protocols and ports, specific layer 7 web applications and specific web application parameters, and denying all files and applications that are not configured.
10-2	استخدام تطبيقات ويب وبروتوكولات اتصالات آمنة مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وبروتوكول أمن طبقة النقل (TLS) وغيرها. Secure web applications and communication protocols, such HTTPS, SFTP and TLS, shall be used.
3	مراجعة الإعدادات والتحصين (Secure Configuration and Hardening)
الهدف	تحديد الإعدادات والتحصين ومراجعتها للتأكد من ضبط إعدادات تطبيقات الويب وتشغيلها بشكل آمن وفعال.

المخاطر المحتملة	قد يؤدي عدم الدقة في ضبط إعدادات تطبيقات الويب ومكوناتها التقنية إلى ظهور ثغرات أمنية يمكن استغلالها لشن هجمات سيبرانية أو التأثير على سير الأعمال في جامعه حائل
الإجراءات المطلوبة	
1-3	يجب إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسات إدارة الثغرات الأمنية واختبار الاختراق المعتمدة في جامعه حائل Regular security testing (such as vulnerability assessments and penetration testing) shall be performed in accordance with Hail University's Vulnerability Management and Penetration Testing Policies.
2-3	إجراء اختبارات دورية لتقييم حماية تطبيقات الويب مثل اختبار أمن التطبيقات الثابت (SAST) واختبار أمن التطبيقات الديناميكي (DAST). Web application security assessments, including Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST), shall be performed regularly.
3-3	تنصيب حزم التحديثات والإصلاحات على تطبيقات الويب ومكوناتها التقنية بانتظام وفقاً لسياسة إدارة التحديثات والإصلاحات المعتمدة في جامعه حائل Web applications shall be regularly patched and updated in accordance with Hail University's Patch Management Policy.
4-3	إيقاف الوظائف والخدمات وملفات الإعدادات غير الضرورية أو غير المستخدمة أو تعطيلها. Unnecessary/unrequired services, functionalities and configuration files shall be removed or disabled.
5-3	حجب إمكانية الوصول إلى الملفات والمجلدات المشاركة عبر الشبكة غير الضرورية أو غير اللازمة. Access to unnecessary/unrequired network shared files and directories shall be blocked.
6-3	حماية الشفرة المصدرية وتحصينها. Application source code shall be secured and hardened.

7-3	إنشاء نسخ أو قوالب آمنة لكافة تطبيقات الويب بناءً على المعايير الأمنية المعتمدة. وإعادة نسخ تطبيقات الويب باستخدام أحد قوالب النسخ في حال تعرضها لانتهاك أمني. Secure web application images or templates shall be created for all web applications based on the approved configuration standards. Any web application server that becomes compromised shall be reimaged using one of these image templates.
8-3	تخزين النسخ في بيئة آمنة على خوادم مؤمنة والتحقق منها باستخدام أدوات مراقبة سلامة المعلومات دورياً. Images shall be stored in a secure environment on securely configured servers, and shall be regularly validated using integrity monitoring tools.
9-3	يجب مزامنة توقيت تطبيقات الويب من مصادر الوقت المعتمدة من قبل جامعه حائل Web applications shall be configured to synchronize time to Hail University's approved time sources.
4	توافر المعلومات (Availability)
الهدف	الحفاظ على توافر تطبيقات الويب الخارجية وحمايتها من هجمات حجب الخدمة (DoS Attacks) وتعطل الخدمة العرضي.
المخاطر المحتملة	إذا لم يتم توفير أنظمة الحماية من هجمات حجب الخدمة وتعطل البنية التحتية، قد تكون تطبيقات الويب هدفاً لهجمات حجب الخدمة، مما قد يسبب انقطاعاً دائماً في الخدمات أو يؤثر على كفاءة تطبيق الويب.
الإجراءات المطلوبة	
1-4	استخدام مبدأ معمارية تطبيقات الويب التوزيعية الذي يعمل على توزيع نقاط التعطل الحاسمة. A web application architecture that eliminates the existence of single points of failure shall be deploy and implemented.
2-4	توفير تقنيات توزيع الجهد (Load Balancer) مثل تقنيات توزيع حركة البيانات والاتصالات. Load balancing mechanisms, such as those offered by an application load balancer device, shall be deployed.

3-4	تطبيق آليات تكرار البيانات (Data Replication) على تطبيقات الويب في مواقع التعافي من الكوارث أو المواقع البديلة (Secondary Data Center). Web application data replication mechanisms shall be implemented on Disaster Recovery (DR) or secondary sites.
4-4	توفير نسخة مطابقة لبيئة إنتاج تطبيقات الويب للأنظمة الحساسة في موقع التعافي من الكوارث. An exact replica of critical web application production environment shall be deployed on the Disaster Recovery (DR) site.
5-4	فيما يتعلق بتطبيقات الويب التي تستضيفها أطراف خارجية، يجب أن تتضمن بنود اتفاقية مستوى الخدمة مستوى مقبول من توافر تطبيقات الويب والخدمات المقدمة من خلالها، وفقاً لسياسة الأمن السيبراني المتعلق بالأطراف الخارجية المعتمدة في جامعه حائلFor web applications hosted by third parties, the Service Level Agreement (SLA) shall maintain an acceptable level of web application and services availability in accordance with Hail University's Third Party Cybersecurity Policy.
6-4	ضبط إعدادات إعادة توجيه حركة بيانات تطبيقات الويب تلقائياً أو يدوياً لموقع النسخ الاحتياطية أو التعافي من الكوارث في حال تعطل بيئة الإنتاج. Automated or manual web application traffic redirection to the backup or Disaster Recovery (DR) site shall be configured in case of production environment failure.
5	التشفير (Cryptography)
الهدف	ضمان سرية بيانات تطبيقات الويب والتأكد من سلامتها.
المخاطر المحتملة	في حال عدم استخدام تقنيات التشفير والتحقق من سلامة المعلومات، يمكن أن تتعرض المعلومات المحمية وبيانات تطبيقات الويب إلى الكشف أو التلاعب بها أو الوصول غير المصرح به.
الإجراءات المطلوبة	

1-5	تطبيق تقنيات التشفير مثل أمن طبقة النقل (Transport Layer Security) والشبكات الخاصة الافتراضية (Virtual Private Networks) لحماية تقنيات التحقّق من الهوية (Authentication)، إلى جانب استخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) وفقاً لمعيار التشفير المعتمد في جامعه حائل Encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), shall be implemented to protect authentication mechanisms during transmission. In addition, recommended next generation encryption protocols and cipher suites shall be used as per Hail University's Cryptography Standard.
2-5	ضبط إعدادات تطبيقات الويب وتمكينها من استخدام بروتوكولات آمنة للتشفير حيثما أمكن، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول النقل الآمن (FTP) عبر أمن طبقة النقل (TLS) وغيرها. Web application protocols shall be configured to use encryption wherever applicable (e.g., HTTPS, FTP over TLS, etc.).
3-5	توفير تقنيات التشفير للاتصالات بين الخوادم وأجهزة المستخدمين في تطبيقات الويب (End-to-End Encryption). End-to-end encryption for web applications client/server communications shall be implemented.
4-5	تقييد استخدام بروتوكولات النقل الآمن (SSHv2) وبروتوكول التحكم بسطح المكتب عن بعد (RDP) عن طريق تقنيات التشفير مثل أمن طبقة النقل (TLS). The use of secure encrypted management protocols such as Secure Shell (SSH) v2 and Remote Desktop Protocol (RDP) over TLS shall be restricted.
5-5	استخدام تقنيات التشفير غير التماثلي القائم على شهادات التشفير (الخاص/العام) لكافة تطبيقات الويب العامة والخارجية وفقاً لمعيار التشفير المعتمد في جامعه حائل Certificate based asymmetric (private/public) cryptography shall be used for all public external web applications as per Hail University's Cryptography Standard.
6-5	شراء شهادات تشفير تطبيقات الويب من جهة إصدار شهادات موثوقة ومعتمدة وفقاً للمتطلبات التنظيمية والتشريعية ذات العلاقة والتأكّد من تجديدها بشكل دوري.

	Web application certificates shall be purchased from a trusted CA compliance source and periodically renewed in accordance with the related laws and regulations.
7-5	تثبيت وظائف التشفير وإدارة شهادات التشفير على جدار الحماية لتطبيقات الويب للسيطرة بشكل أكبر على الهجمات والتهديدات. Encryption functionalities and certificate management shall be offloaded on the web application firewall to provide more visibility into threats and attacks.
8-5	تخزين مفاتيح تشفير تطبيقات الويب في مكان ملائم وآمن وفقاً للسياسات والإجراءات ذات العلاقة في جامعه حائل Web applications cryptographic keys shall be stored in a secure vault and physically secure locations as per Hail University's relevant policies and procedures.
6	تسجيل الأحداث وسجل التدقيق (Event and Audit Logging)
الهدف	ضمان حفظ سجلات الأحداث لتطبيقات الويب في جامعه حائل ومراقبتها.
المخاطر المحتملة	يؤدي عدم حفظ ومراقبة سجلات الأحداث لتطبيقات الويب في جامعه حائل إلى صعوبة الكشف عن حوادث وتهديدات الأمن السيبراني وغيرها، وقد يتسبب بمضاعفة الأضرار التي قد تلحق بالتطبيقات.
الإجراءات المطلوبة	
1-6	تفعيل جميع سجلات الأحداث (سجلات التدقيق والسجلات المتعلقة بالأمن السيبراني) لجميع تطبيقات الويب ومكوناتها التقنية. All levels of logging as well as audit trail and security logs shall be enabled on all web application and technical components.
2-6	جمع سجلات الأحداث الخاصة بالأمن السيبراني في نظام تسجيل مركزي (SIEM) وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدين في جامعه حائل Server logging and audit trail shall be configured to be forwarded to a centralized logging system as per Hail

	University's Cybersecurity Event Logs and Monitoring Management Policy and Standard.
7	النسخ الاحتياطي والأرشفة (Backup and Archival)
الهدف	ضمان سلامة بيانات تطبيقات الويب من العبث بها أو فقدانها بالخطأ أو تخريبها، والتأكد من توافرها وقابلية استعادتها.
المخاطر المحتملة	في حال حذف بيانات تطبيقات الويب أو العبث بها أو فقدانها بالخطأ أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن جامعه حائل من استرداد البيانات مما سيؤثّر على أنشطة أعمالها الاعتيادية.
الإجراءات المطلوبة	
1-7	عمل نسخ احتياطية كاملة لتطبيقات الويب وترقيمها تسلسلياً وتحديد تاريخها ووقتها وفهرستها وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعه حائل وينبغي أن تشمل النسخ الاحتياطية على الأقل النسخ الاحتياطية لإعدادات تطبيقات الويب وبيانات ومعلومات تطبيقات الويب المخزنة. Full backups for web applications shall be performed, serialized, time-dated and indexed in accordance with Hail University's Backup and Recovery Management Policy. The backups must include at minimum web applications' configuration backups, and the stored data and information of web applications.
2-7	تشفير النسخ الاحتياطية لتطبيقات الويب الخاصة بـ جامعه حائل Hail University's web applications backups shall be encrypted.
3-7	تخزين النسخ الاحتياطية من تطبيقات الويب للأنظمة الحساسة الخاصة جامعه حائل على الأقل في موقعين ماديين ومعزولين مادياً عن بعضهما البعض. Backups of Hail University's web applications for critical systems shall be stored in at least two geographically distinct protected off-sites.
4-7	اختبار إمكانية استرجاع النسخة الاحتياطية كل ثلاثة أشهر أو وفقاً للسياسات والإجراءات ذات العلاقة في جامعه حائل

	Backup recovery test shall be conducted every quarter or in accordance with Hail University's relevant policies and procedures.
5-7	استخدام تقنيات توثيق وسلامة النسخ الاحتياطي لضمان نسخ بيانات تطبيقات الويب وأرشفتها بطريقة صحيحة. Backup verification and integrity mechanisms shall be employed to ensure that web application data is correctly backed up and archived.
6-7	أرشفة النسخ الاحتياطية لتطبيقات الويب الخاصة بـجامعه حائل في موقع تخزين معزول مادياً ومنطقياً ووفقاً للسياسات والإجراءات ذات العلاقة في جامعه حائل Hail University's web applications backups shall be archived in an offsite storage for a retention period as per Hail University's relevant policies and procedures.
8	تطبيقات الويب الحديثة والسحابية الأصلية (Modernized and Cloud Native Web Applications)
الهدف	تحديد متطلبات الأمن السيبراني لتطبيقات الويب المستضافة بالحوسبة السحابية لضمان إعدادها وتثبيتها وتشغيلها بطريقة آمنة.
المخاطر المحتملة	قد يؤدي استخدام خدمة الحوسبة السحابية لتشغيل تطبيقات الويب بدون وضع معايير أمنية وتطبيق متطلبات الأمن السيبراني إلى ظهور ثغرات أمنية شائعة يمكن استغلالها لشن هجمات سيبرانية أو التأثير على كفاءة أعمال جامعه حائل
الإجراءات المطلوبة	
1-8	تطوير منهجية التطوير الآمن وفقاً لآلية "DevSecOps". A DevSecOps methodology and process shall be developed and adopted.
2-8	تطوير نظام التكامل المستمر/التثبيت المستمر (CI/CD) الآمن وتطبيقه باتباع أفضل الممارسات. A secure Continuous Integration/Continuous Deployment (CI/CD) pipeline shall be developed and implemented following best practices.

3-8	تنصيب منصة أمن الحاويات من مورد موثوق لإدارة أمن الحاويات وضمان حماية نظام الحاويات. A container security platform shall be deployed from a trusted vendor to manage container security and ensure that the container system is safe.
4-8	تنصيب حزم التحديثات والإصلاحات دورياً. Security patches shall be regularly deployed.
5-8	توفير حلول إدارة المعلومات الحساسة وذلك من أجل إدارة المعلومات الحساسة والمفاتيح والشهادات ومنع تخزين المعلومات الحساسة في الحاويات. Critical information management mechanisms shall be implemented to manage Confidential information, keys and certifications, and prevent storing confidential information in containers.
6-8	استخدام نسخ الحاويات من مصادر موثوقة أو معتمدة. Container images from trusted or approved sources shall be used.
7-8	عزل البنية التحتية الخاصة بالحاويات. Containers' infrastructure shall be isolated.
8-8	استخدام كشف الثغرات التلقائي لفحص الحاويات قبل وبعد تثبيتها في بيئة الإنتاج. Automated vulnerability detection shall be used to scan containers before and after their deployment into the production environment.
9-8	توفير تقنيات وأدوات المراقبة للتأكد من سلامة تطبيقات الويب وتوافرها وكفاءتها باستمرار. Monitoring tools shall be deployed to regularly monitor applications' health, availability and efficiency.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني
2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني بجامعه حائل
3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الإلكتروني

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعه حائل بهذا المعيار باستمرار.
2- يجب على كافة العاملين في جامعه حائل الالتزام بهذا المعيار.
3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعه حائل

جامعة حائل
University of Ha'il

نموذج سياسة إدارة مخاطر الأمن السيبراني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لإدارة مخاطر الأمن السيبراني في جامعه حائل، وذلك وفقاً لاعتبارات سرية الأصول المعلوماتية والتقنية وتوافرها وسلامتها.

تتبع هذه السياسة المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهي متطلب تشريعي كما هو مذكور في الضابط رقم ١-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية وأنظمة وأجهزة التحكم الصناعي الخاصة بـجامعه حائل وإجراءات عمل جامعه حائل، وتنطبق على جميع العاملين في جامعه حائل.

بنود السياسة

1- البنود العامة

1-1 يجب تطوير وتوثيق واعتماد منهجية إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management Methodology) وإجراءات إدارة مخاطر الأمن السيبراني في جامعه حائل، ويجب مواءمتها مع الإطار الوطني لمخاطر الأمن السيبراني (National Cybersecurity Risk Management Framework) ويمكن استخدام المعايير والأطر التوجيهية المعتمدة دولياً (مثل: ISO27005، وISO31000، وNIST) في تطوير منهجية إدارة مخاطر الأمن السيبراني.

2-1 يجب أن تغطي منهجية إدارة مخاطر الأمن السيبراني بحد أدنى ما يلي:

1-2-1 تحديد الأصول ومعرفة أهميتها.

2-2-1 تحديد وتقييم المخاطر التي تمس أعمال أو أصول أو العاملين في جامعه حائل (مثل: الآثار المترتبة على جامعه حائل الناتجة عن المخاطر السيبرانية).

3-2-1 تحديد التهديدات والثغرات المتعلقة بالأمن السيبراني التي قد تؤثر على الأصول المعلوماتية والتقنية وتقييمها.

4-2-1 تحديد أساليب التعامل مع المخاطر السيبرانية.

5-2-1 ترتيب تدابير الحدّ من المخاطر السيبرانية حسب الأولية ووفق إجراءات محدّدة.

6-2-1 تصنيف مستويات المخاطر السيبرانية وتعريفها بناءً على مستوى التأثير واحتمالية حدوث التهديد لـجامعه حائل.

7-2-1 إنشاء سجل مخاطر الأمن السيبراني لتوثيق المخاطر ومتابعتها.

8-2-1 تحديد الأدوار والمسؤوليات لإدارة مخاطر الأمن السيبراني والتعامل معها.

3-1 يجب تنفيذ تقييم المخاطر دورياً لضمان حماية الأصول المعلوماتية والتقنية والتعامل مع المخاطر حسب الأولوية.

4-1 يجب أن تكون إدارة مخاطر الأمن السيبراني متوافقة مع إدارة المخاطر المؤسسية (Enterprise Risk Management "ERM") في جامعه حائل.

2- المراحل الرئيسية لإدارة المخاطر السيبرانية

1-2 تحديد المخاطر (Risk Identification): يجب أن تُحدّد إدارة الأمن السيبراني الأحداث أو الظروف التي من الممكن أن تنتهك سريّة الأصول المعلوماتية والتقنية وسلامتها وتوافرها، ويشمل ذلك على وجه الخصوص تحديد الأصول المعلوماتية والتقنية، والتهديدات التي من المحتمل أن تتعرّض لها والثغرات ذات الصلة، والضوابط المعتمدة، ومن ثمّ تحديد الآثار الناتجة عن فقدان سريّة هذه الأصول وسلامتها وتوافرها.

2-2 تقييم المخاطر (Risk Assessment):

1-2-2 يجب على إدارة الأمن السيبراني تنفيذ إجراءات تقييم مخاطر الأمن السيبراني بحد أدنى في الحالات التالية:

1-1-2-2 في المراحل الأولى من المشاريع التقنية.

2-1-2-2 قبل إجراء تغيير جوهري في البنية التقنية.

3-1-2-2 عند التخطيط للحصول على خدمات طرف خارجي.

4-1-2-2 عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة.

2-2-2 يجب إعادة تقييم المخاطر وتحديثها على النحو التالي:

1-2-2-2 دورياً لجميع الأصول المعلوماتية والتقنية، وسنوياً على الأقل للأنظمة الحسّاسة. (CSCC-1-2-1-1)

2-2-2-2 بعد وقوع حادث متعلّق بالأمن السيبراني ينتهك سلامة الأصول المعلوماتية والتقنية وتوافرها وسريّتها.

3-2-2-2 بعد الحصول على نتائج تدقيق مهمّة أو معلومات استباقية.

4-2-2-2 في حال التغيير على الأصول المعلوماتية والتقنية.

3-2-2 يجب أن تغطي عملية تقييم المخاطر ما يلي:

1-3-2-2 تحليل المخاطر (Risk Analysis): يجب أن تُقيّم إدارة الأمن السيبراني احتمالية وقوع التهديدات والآثار الناتجة عنها، وأن تستخدم نتائج هذا التقييم لتحديد المستوى العام لهذه المخاطر. ويجب أن تعتمد إدارة الأمن السيبراني منهجية كميّة (Quantitative) أو نوعيّة (Qualitative) لإجراء تحليل المخاطر.

2-3-2-2 تقدير المخاطر (Risk Evaluation): يجب أن تُقدِّر إدارة الأمن السيبراني حجم المخاطر السيبرانية بالتوافق مع معايير تقدير المخاطر المؤسسية المعتمدة في جامعه حائل، وتحديد أساليب التعامل معها حسب الأولوية.

3-2 معالجة المخاطر (Risk Treatment):

2-3-1 يجب أن تحدد إدارة الأمن السيبراني خيارات معالجة المخاطر حسب القائمة التالية:

2-1-3-1 معالجة المخاطر أو تقليلها (Risk Mitigation): معالجة أو تقليل درجة الخطر من خلال تطبيق الضوابط الأمنية اللازمة لتقليل احتمال الحدوث أو التأثير أو كليهما، والتي تساعد في احتواء المخاطر والمحافظة عليها ضمن مستويات مقبولة.

2-1-3-2 تجنّب المخاطر (Risk Avoidance): التخلص من الخطر بتجنب الاستمرار بمصدر الخطر.

2-1-2-1-3 مشاركة المخاطر أو تحويلها (Risk Transfer): مشاركة المخاطر مع طرف ثالث لديه الإمكانيات في التعامل مع المخاطر بشكل أكثر فعالية، أو التأمين على الأصول المعلوماتية والتقنية في حال تعرضها لمخاطر سيبرانية.

2-2-1-3-2 تقبّل المخاطر وتحمّلها (Risk Acceptance): مستوى الخطر مقبول ولكن يجب المراقبة باستمرار في حال حدوث تغيير.

2-3-2 يجب تحديد خيارات معالجة المخاطر وتوثيقها بناءً على نتائج تقييم المخاطر وتكلفة التنفيذ والمنافع المتوقّعة.

2-4 متابعة المخاطر (Risk Oversight):

2-4-1 لمتابعة المخاطر يجب أن تُعِدّ إدارة الأمن السيبراني سجلاً للمخاطر وأن تحافظ عليه لتوثيق مخرجات عملية إدارة المخاطر. على أن يشمل بحد أدنى على المعلومات التالية:

2-4-1-1 عملية تحديد المخاطر.

2-4-1-2 نطاق المخاطر.

2-4-1-3 المسؤول أو صاحب المخاطر.

2-4-1-4 وصف للمخاطر بما في ذلك أسبابها وآثارها.

2-4-1-5 تحليل للمخاطر يُوضّح التأثيرات الناتجة عن المخاطر ونطاقها الزمني.

2-4-1-6 تقييم وتصنيف للمخاطر يشتمل على احتمالية المخاطر وحجمها وتصنيفها الإجمالي في حال حدوثها.

2-4-1-7 خطّة التعامل مع المخاطر تتضمّن إجراء التعامل معها والشخص المسؤول عنها وجدولها الزمني.

2-4-1-8 وصف الخطر المتبقي.

2-4-2 يجب استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان فعالية إدارة مخاطر الأمن السيبراني.

2-4-3 يجب على إدارة الأمن السيبراني جمع الأدلة المتعلقة بحالة المخاطر السيبرانية ومراجعتها بشكل دوري.

3- مستوى المخاطر المقبول (Risk Appetite)

3-1 يجب تحديد معايير تقبّل المخاطر وتوثيقها، وفقاً لمستوى المخاطر وتكلفة معالجة الخطر مقابل تأثيره.

2-3 يجب تطبيق ضوابط إضافية من أجل تقليل المخاطر إلى مستوى مقبول في حال عدم استيفاء الخطر المتبقي لمعايير تقبّل المخاطر.

3-3 في حال تجاوز معايير تقبّل المخاطر، يتم التصعيد لصاحب الصلاحية لاتخاذ الإجراءات أو القرارات اللازمة.

4- متطلبات أخرى

1-4 يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حال حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.

2-4 يجب مراجعة سياسة إدارة مخاطر الأمن السيبراني سنوياً، وتوثيق التغييرات واعتمادها.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني بجامعه حائل

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني بجامعه حائل

3- **تنفيذ السياسة وتطبيقها:** إدارة الأمن السيبراني بجامعه حائل

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني بجامعه حائل ضمان التزام جامعه حائل بهذه السياسة دورياً.

2- يجب على جميع العاملين في جامعه حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعه حائل.

جامعة حائل
University of Ha'il

نموذج معيار أمن الشبكات

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية أمن الشبكات الخاصة بـ لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية، وهي: سرية المعلومات، وسلامتها، وتوافرها.

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أنظمة الشبكات التقنية الخاصة بـجامعة حائل، وينطبق على جميع العاملين في جامعة حائل.

المعايير

1	الوصول الآمن (Secure Access)
الهدف	ضمان تطبيق الإعدادات الصحيحة للوصول إلى واجهات إدارة أمن الشبكات من أجل حمايتها بشكل فعال من الهجمات السيبرانية.
المخاطر المحتملة	تؤدي الإعدادات غير الكافية لحلول واجهات إدارة أمن الشبكات إلى تعرض أجهزة الشبكات داخل بيئة جامعة حائل إلى هجمات أو انتهاكات أمنية.
الإجراءات المطلوبة	
1-1	إعداد قوائم الوصول بصورة تسمح بالتحكم بالوصول إلى أجهزة اتصالات الشبكة بحيث يمكن للأشخاص المصرح لهم فقط الوصول إلى هذه الأجهزة. Access lists shall be configured to control access to network communication devices and ensure that these devices are accessible to authorized users only.
2-1	إعداد قائمة وصول لحماية جميع أجزاء الشبكة من انتحال عنوان بروتوكول الإنترنت (IP Address Spoofing). An access list shall be configured to protect all network segments from Layer-3 IP address spoofing.

3-1	استخدام آلية تحقق مركزية للتحقق من جميع المستخدمين التفاعليين الذين يقومون بعمل تغييرات على كافة أجهزة الشبكة. كما يجب أن تكون أنظمة التحقق بأقل عدد ممكن. Centralized user-level authentication shall be deployed to authenticate all interactive users making changes to all network devices. Additionally, authentication systems shall be as few as possible.
4-1	أن يقتصر وصول مشرفي إدارة مكونات الشبكة اللاسلكية عبر استخدام أجهزة حاسب مخصصة ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs) أو خوادم الوصول إلى المناطق الآمنة (Jump Servers) الموجودة على واجهات إدارة مستقلة على شبكة مفصولة عن شبكة جامعة حائل ومعزولة عن الإنترنت، ومنع وصولهم لاسلكياً. Restrict wireless network administrators' access to use dedicated Privileged Access Workstations (PAWs) or jump servers placed in an out-of-band management network, segmented from Hail university's network and isolated from the internet, and not wirelessly.
5-1	تطبيق التحقّق من الهوية متعدّد العناصر واستخدام الجلسات المشفرة لإدارة كافة أجهزة الشبكات. Multi-Factor Authentication shall be implemented and encrypted sessions shall be used to manage all network devices.
6-1	تقييد استخدام كلمة المرور المحددة بتعليمات ثابتة وحصره على مشرفين محددين فقط بحسب ما هو ضروري لغايات غير تفاعلية ولاستعادة أجهزة الشبكة التي تم فصلها عن الشبكة. The use of hard-coded passwords shall be limited to relevant administrators only as necessary for non-interactive purposes, as well as to recover network devices that have become disconnected from the network.
7-1	إعداد أجهزة الشبكة لعرض رسالة نصية تنبيهية عند تسجيل الدخول. ويجب ألا تُظهر هذه الرسالة النصية الخصائص الأساسية للشبكة. Network devices shall be configured to display an awareness banner at login. This banner text shall not provide the underlying characteristics of the network.

2	فصل الشبكة (Network Segregation)
الهدف	ضمان حماية تصميم وبنية الشبكة وحماية الأجزاء الشبكية وفقاً لمستوى الأمن الخاص بها.
المخاطر المحتملة	تتشارك الشبكات غير المفصولة في نفس نطاق البث وتكون الأجهزة قادرة على التواصل دون مراقبة أو ضبط حركة البيانات، وبالتالي يمكن أن يؤدي أي هجوم على النظام إلى تهديدات داخلية خطيرة وهجمات على معظم أنظمة الشبكة، مما يسهل حركة البيانات الجانبية ضمن الشبكة.
الإجراءات المطلوبة	
1-2	تصميم وتطبيق شبكة معزولة منطقياً و/أو مادياً مع الأخذ بعين الاعتبار احتياجات الأعمال والمعمارية المؤسسية وذلك بالاستناد إلى الدفاع الأمني متعدد المراحل والمعمارية متعددة المستويات. A logically and/or physically segmented network shall be designed and implemented, taking into consideration business needs and enterprise architecture, and based on the principles of defense-in-depth and multi-tier architecture.
2-2	تطبيق المستوى الملائم من ضوابط الأمن السيبراني على الأجزاء الشبكية المختلفة بناءً على قيمة وتصنيف المعلومات المخزنة أو المعالجة في الشبكة ومستويات الموثوقية والتأثير على الأعمال والمخاطر المرافقة. Appropriate level of security controls shall be applied to different network segments based on the value and classification of information stored or processed in the network, levels of trust, business impact and associated risks.
3-2	تطبيق المعمارية متعددة المستويات المحمية بجدار حماية ثنائي الطبقة. وعلى وجه الخصوص، تقسيم الشبكة إلى ثلاثة مستويات أو أكثر (مستوى الحدود/المحيط، والمستوى الرئيسي، والمستوى الموثوق)، وتقسيم الأجزاء الشبكية إلى مناطق (المنطقة المحايدة "DMZ"، ومنطقة الإدارة، ومنطقة الإنتاج، ومنطقة التطوير/الاختبار، وغيرها) وفقاً للبنية المؤسسية والبنية الأمنية في جامعة حائل.

Multi-tier architecture protected by dual layer of firewalls shall be implemented. Specifically, the network shall be segmented into three or more layers (boundary/perimeter, core and trusted) and the network segments shall be divided into zones (demilitarized zone “DMZ”, management zone, production zone, database zone, development/testing zone, etc.) as per Hail university’s enterprise architecture and security architecture.	
تصميم وإعداد الشبكات لتصفية مرور البيانات بين مختلف الأجزاء وحجب الوصول غير المصرح به. Networks shall be designed and configured to filter traffic between different segments and block any unauthorized access.	4-2
وضع الخوادم أو مخازن البيانات التي تتضمن معلومات محمية في أجزاء شبكية منفصلة ومخصصة. Servers or data stores with sensitive information shall be placed in dedicated separate network segments.	5-2
إعداد جدران الحماية والموجّهات (Routers) لمنع أي اتصالات غير مصرح بها بين الشبكات غير الموثوقة وأي مكونات نظام تقوم بتخزين معلومات حساسة أو حساسة جداً. Firewalls and routers shall be configured to prevent any unauthorized connections between untrusted networks and any system components storing highly confidential or confidential information.	6-2
تحديد وتطبيق المستويات والحدود لكل منطقة أمنية. Levels and boundaries shall be defined and implemented for each security zone.	7-2
تحديد وتطبيق منطقة أو جزء شبكي لواجهات الإدارة المستقلة، بما في ذلك كافة خوادم الإدارة، والمعدات ذات صلاحية الوصول الإدارية، وخوادم بروتوكول النقل الآمن (SSH)، وخوادم الوصول إلى المناطق الآمنة (Jump Servers)، وأجهزة الحاسب ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs). An out-of-band management network zone or segment, including all administration servers, machines with	8-2

administrative access, Secure Shell (SSH) servers, jump servers and Privileged Access Workstations (PAWs), shall be defined and implemented.	
فصل الشبكات اللاسلكية عن الشبكة الداخلية والشبكات المعزولة والشبكات الخاصة. Wireless networks shall be segregated from the internal network, isolated networks and private networks.	9-2
تحديد الخوادم والشبكات وبيئات الإنتاج والاختبار والبيئات الموثوقة المستخدمة في تطوير واختبار وفحص وتخزين البيانات والنشاطات ذات الصلة بوضوح وفصلها عن الشبكات الأخرى. Servers, networks and production, test, and trusted environments used for developing, testing, scanning and storing data and any other related activities, shall be clearly identified and segregated from other networks.	10-2
فصل أجزاء الأنظمة الحساسة منطقياً عن البيئات الأخرى. Segments of critical systems shall be logically isolated from other environments.	11-2
منع الأنظمة الحساسة من الاتصال بالشبكة اللاسلكية. Critical systems shall be prevented from connecting to the wireless network.	12-2
منع الأنظمة الحساسة من الاتصال بالإنترنت في حال كانت هذه الأنظمة تقدم خدمات داخلية لا تحتاج إلى صلاحية الوصول عن بعد أو الوصول عبر الإنترنت. Critical systems that offer internal services which do not require remote or Internet access shall be prevented from connecting to the Internet	13-2
مراجعة الإعدادات والقواعد والسياسات والملفات التعريفية الأمنية لجدران الحماية والموجهات (Routers) التي تدعم الشبكات الحساسة مرة كل ستة أشهر على الأقل. Security configurations, rules, policies and profiles for firewalls and routers that support critical networks shall be reviewed at least every six months.	14-2
تأمين الحدود (Boundary Defense)	3

الهدف	حماية حدود الشبكة من التهديدات.
المخاطر المحتملة	في حال تم ترك حدود الشبكة من دون الحماية التي توفرها الضوابط الأمنية المناسبة، سيتمكن المهاجمون من اختراق الشبكة بسهولة وفرض المزيد من التهديدات الخطيرة.
الإجراءات المطلوبة	
1-3	الاحتفاظ بقائمة جرد محدثة لكافة حدود الشبكة في جامعة حائل. An up-to-date inventory of all of Hail university's network boundaries shall be maintained.
2-3	القيام بعمليات مسح وفحص منتظمة من الخارج لكل حد شبكة موثوق لاكتشاف أي اتصالات غير مصرح بها يمكن الوصول إليها عبر الحدود. Regular scans from outside each trusted network boundary shall be performed to detect any unauthorized connections that can be accessed across the boundary.
3-3	حظر الاتصالات مع عناوين بروتوكولات الإنترنت الخبيثة أو غير المستخدمة وحصر الوصول بمجالات عنوان بروتوكولات الإنترنت الموثوقة والضرورية عند كل حد من حدود شبكة جامعة حائل. Communications with known malicious or unused Internet IP addresses shall be denied, and access shall be limited to trusted and necessary IP address ranges at each of Hail university's network boundaries.
4-3	حظر الاتصالات عبر منافذ بروتوكول التحكم بالنقل (TCP) أو بروتوكول حزم بيانات المستخدم (UDP) أو حركة التطبيقات لضمان السماح فقط للبروتوكولات المصرح لها بالدخول أو الخروج من الشبكة عبر حدود الشبكة عند كل حد من حدود شبكة جامعة حائل. Communication over unauthorized TCP or UDP ports or application traffic shall be denied to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of Hail university's network boundaries.
5-3	إعداد أنظمة المراقبة لتسجيل حزم بيانات الشبكة التي تمر عبر الحدود عند كل حد من حدود شبكة جامعة حائل.

Monitoring systems shall be configured to record network packets passing through the boundary at each of Hail university's network boundaries.	
تثبيت حساسات أنظمة كشف التسلل (IDS) على الشبكة لكشف أي آليات هجوم غير اعتيادية وكشف أي انتهاكات أمنية لهذه الأنظمة عند كل حد من حدود شبكة جامعة حائل. Network-based Intrusion Detection Systems (IDS) sensors shall be deployed to detect any unusual attack mechanisms and detect any compromise of these systems at each of Hail university's network boundaries.	6-3
تثبيت أنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات على الشبكة لكشف أي حركة بيانات خبيثة على الشبكة عند كل حد من حدود شبكة جامعة حائل. Network-based Intrusion Prevention Systems (IPS) shall be deployed to block malicious network traffic at each of Hail university's network boundaries.	7-3
تثبيت تقنيات كشف/منع التهديدات المتقدمة المستمرة (APT) على الشبكة لكشف أو حجب الهجمات على الشبكة والهجمات غير المعروفة مسبقاً عند كل حد من حدود شبكة جامعة حائل. Network-based Advanced Persistent Threat (APT) detection/prevention systems shall be deployed to detect or block malicious network attacks and zero-day attacks at each of Hail university's network boundaries.	8-3
تثبيت جدار حماية التحقق من التطبيقات لحجب أي تطبيقات غير مدرجة في قائمة التطبيقات المسموحة أو غير معروفة أو لا تمتثل للضوابط الأمنية (مثل التطبيقات التي تتواصل عبر منفذ بروتوكول حزم بيانات المستخدم الخاص بنظام أسماء النطاقات "UDP/53" وهي غير ممتثلة لبروتوكول نظام أسماء النطاقات) عند كل حد من حدود شبكة جامعة حائل. Application inspection firewall shall be deployed to block applications that are not whitelisted, unknown or non-compliant with security controls (for example, applications communicating over UDP/53 while not being compliant with DNS protocol) at each of Hail university's network boundaries.	9-3
تثبيت جدار الحماية لتطبيقات الويب (WAF) لتحليل وتصفية ومراقبة حركة البيانات، ومنع حركة بيانات غير المصرح لها من وإلى تطبيقات الويب.	10-3

Web Application Firewall (WAF) shall be placed to analyzes, filters, monitors, and blocks Internet traffic to and from a web application.	
ضبط إعدادات بروتوكولات التشفير المقبولة والموافق عليها مثل بعض أنواع أمن طبقة النقل (TLS) للعمل على أي جهاز من أجهزة جدران الحماية لتطبيقات الويب (WAF) للتحقق من البيانات غير المشفرة. وفي حال عدم دعم الجهاز عملية تفريغ البيانات عبر أمن طبقة النقل، فلا بد من وضع جدار الحماية لتطبيقات الويب في جهاز فك تشفير للتحقق من البيانات غير المشفرة، أو تثبيت جدار الحماية لتطبيقات الويب على المستضيف. Acceptable and approved encryption protocols such as some types of Transport Layer Security (TLS) shall be configured to terminate on any WAF device to inspect decrypted traffic. If the device does not support TLS offloading, WAF shall sit behind a decryption device to inspect decrypted traffic. Otherwise, a host-based web application firewall shall be deployed.	11-3
تمكين جمع معلومات حركة البيانات عبر الشبكة (NetFlow) وتسجيل البيانات على كافة أجهزة حدود الشبكة. The collection of NetFlow and logging data shall be enabled on all network boundary devices.	12-3
ضمان أن كافة أشكال حركة البيانات عبر الشبكة من أو إلى الإنترنت تمر عبر خادم وكيل طبقة التطبيقات المعتمدة والمجهز لتصفية الاتصالات غير المصرح بها. All network traffic to/from the Internet shall pass through an authenticated application layer proxy that is configured to filter unauthorized connections.	13-3
السماح للمستخدمين بالوصول إلى فئات عناوين (URL) محددة ومصرح بها، وحجب إمكانية الوصول إلى فئات العناوين (URL) الضارة أو المخصصة للاختراق، أو التي تعمل عبر خوادم مفوضة أو خوادم غير معروفة الهوية، أو المخصصة للتصيد أو المشبوهة أو غير المعروفة أو غير المصنفة. Only specific and whitelisted URL categories shall be allowed to users. Access to hacking, malware, proxy, anonymizers, phishing, suspicious, unknown and uncategorized URLs shall be disabled.	14-3

15-3	فك تشفير كافة حركة بيانات تصفح الإنترنت المشفرة عند الخادم المفوض على الحدود قبل تحليل المحتوى. يمكن لـجامعة حائل استخدام قائمة محددة من التطبيقات لمواقع مسموحة يمكن الوصول إليها عبر خادم وكيل دون فك تشفير حركة البيانات. All encrypted Internet browsing traffic at the boundary proxy shall be decrypted prior to analyzing the content. However, Hail university may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
16-3	ضبط إعدادات الوصول وتسجيل الدخول عن بعد إلى شبكة جامعة حائل للقيام بتشفير البيانات قيد الاستخدام والنقل، واستخدام التحقّق من الهوية متعدّد العناصر. All remote login access to Hail university's network shall be configured to encrypt data in transit. Additionally, Multi-Factor Authentication shall be used.
17-3	تثبيت جهاز وصول عن بعد يستخدم تقنيات مثل الشبكات الخاصة الافتراضية أو حلول طبقة المنافذ الآمنة-الشبكات الخاصة الافتراضية (SSL-VPN) لحجب وحماية كافة أشكال الوصول إلى شبكة جامعة حائل. A remote access device that uses technologies such as Virtual Private Network (VPN), or SSL-VPN solutions shall be deployed to terminate and protect all remote access to Hail university's network.
18-3	مسح جميع أجهزة المشاريع التي تقوم بالدخول عن بعد إلى شبكة جامعة حائل قبل وصولها إلى الشبكة لضمان تطبيق جميع سياسات الأمن المعتمدة في جامعة حائل بنفس الطريقة التي تم تطبيقها على أجهزة الشبكة المحلية. All enterprise devices remotely logging into Hail university's network shall be scanned prior to accessing the network to ensure that all of Hail university's security policies have been enforced in the same manner used on local network devices.
19-3	تثبيت تقنيات كشف/منع هجمات حجب الخدمة (DoS) وهجمات تعطيل الخدمات الموزعة (DDoS) على أجهزة جامعة حائل أو من قبل أطراف خارجية لكشف وحجب هجمات حجب الخدمة (DoS) عند كل حد من حدود شبكة جامعة حائل. Denial of Service (DoS) and Distributed DoS (DDoS) detection/prevention technologies shall be deployed (on prim or by a third party) to detect or block DoS attacks at each of Hail university's network boundaries.

20-3	تثبيت تقنيات أمن نظام أسماء النطاقات لكشف أو حجب الهجمات على نظام أسماء النطاقات عند كل حد من حدود شبكة جامعة حائل. Domain Name System (DNS) security technologies shall be deployed to detect or block DNS attacks at each of Hail university's network boundaries.
21-3	تمكين تسجيل الاستفسارات على نظام أسماء النطاقات لكشف وتحديد اسم المستضيف للنطاقات الخبيثة المعروفة. Domain Name System (DNS) query logging shall be enabled to detect hostname lookups for known malicious domains.
22-3	تثبيت بوابة أمن البريد الإلكتروني لكشف أو حجب الهجمات عبر البريد الإلكتروني على حدود شبكة جامعة حائل. Email security gateway shall be deployed to detect or block email-based attacks at each of Hail university's network boundaries.
23-3	ضمان التحديث المنتظم لكافة خدمات الاشتراك وفئات العناوين (URL) ومصادر المعلومات الاستباقية والقوائم المحددة من التطبيقات الممنوعة (Blacklists) والإشارات المعرفة المسبقة. All subscription services, URL categories, threat feeds, blacklists, and signatures shall be up-to-date and updated regularly.
4	القيود والضوابط (Limitations and Controls)
الهدف	الحد من مصادر الهجمات وحماية الشبكة الداخلية من التهديدات.
المخاطر المحتملة	تؤدي حماية الشبكة الداخلية إلى تقليل مخاطر التهديدات الداخلية والحركة الجانبية (Network Lateral Movement).
الإجراءات المطلوبة	
1-4	ربط المنافذ والخدمات والأجهزة النشطة بأصول المعدات في قائمة جرد الأصول. Active ports, services and protocols shall be associated with the hardware assets in the asset inventory.
2-4	تقييد منافذ الشبكة وبروتوكولاتها والخدمات المتاحة على النظام وحصرها على متطلبات الأعمال لكل نظام.

Only network ports, protocols, and services listening on a system with validated business needs shall be running on each system.	
القيام بعمليات مسح آلية للمنافذ بشكل منتظم على كافة الأنظمة، والتنبيه عند اكتشاف منافذ غير مصرح بها على النظام. Automated port scans shall be performed on a regular basis against all systems, and alerts shall be raised upon the detection of unauthorized ports on a system.	3-4
تطبيق جدار حماية المستضيف أو أدوات تصفية المنافذ لكل نظام مع تطبيق قاعدة المنع التلقائي التي تحجب جميع أشكال حركة البيانات باستثناء الخدمات والمنافذ المصرح لها فقط. Host-based firewalls or port filtering tools shall be applied on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	4-4
تثبيت جدار حماية لمركز البيانات لفحص ومراقبة الاتصالات عبر الشبكة المحلية الافتراضية (VLAN)، والمنافذ الموثوقة وغير الموثوقة، وما بين المناطق والأجزاء والخوادم لحماية الشبكات الداخلية وحجب الهجمات الداخلية. A datacenter firewall shall be deployed to inspect and monitor inter-VLAN, trust-to-untrust, zone-to-zone, segment-to-segment, and east-west communications to protect the internal network and block internal attacks.	5-4
إعداد سياسات جدار الحماية ونموذج القواعد لاتباع نموذج الأمن الإيجابي (نموذج السماح بقائمة محددة من التطبيقات) من خلال حجب كافة أنواع حركة البيانات تلقائياً والسماح فقط بحركة بيانات محددة إلى خدمات معينة. ويمكن تحقيق هذا الأمر من خلال ضبط إعدادات آخر قاعدة في قائمة التحكم بالوصول بحيث تحجب كافة أنواع حركة البيانات. ويمكن القيام بهذا الأمر بشكل صريح أو ضمني حسب المنصة. Firewall policies and rules model shall be configured to follow positive security model (whitelisting model) by blocking all traffic by default and only allowing specific traffic to identified services. This can be achieved by configuring the last rule in an access control list to deny all traffic. In addition, this can be performed explicitly or implicitly, depending on the platform.	6-4

7-4	إعداد جدار حماية لمركز البيانات مجهز بآلية التعرف على التطبيقات (المستوى 4-المستوى 7) وآلية السماح بقائمة محددة من التطبيقات (Whitelisting) ومنع قائمة محددة أخرى من التطبيقات (Blacklisting). Datacenter firewall shall be configured with application identification (Layer4-Layer7), and application whitelisting and blacklisting.
8-4	ضبط إعدادات قوائم جدار الحماية بآلية التعرف على المستخدم لوضع السياسات بناءً على هوية المستخدم (UID). Firewall rules shall be configured with user identification to build policies based on User Identity (UID).
9-4	تطبيق الضوابط 3-6 إلى 3-10 المذكورة أعلاه في هذا المعيار على الشبكة الداخلية. Controls 3-6 to 3-10 from this standard shall be implemented on the internal network.
10-4	في حال كانت شبكة جامعة حائل تعمل على الإصدار الرابع من بروتوكول الإنترنت (IPv4)، يجب تثبيت ضوابط الأمن من المستوى 2 لحماية الشبكة الداخلية. In case <entity name> network is IPv4 based, Layer 2 security controls shall be deployed to protect the internal network
11-4	إعداد شبكات محلية افتراضية خاصة/معزولة لأجزاء الشبكة الحساسة أو الأجزاء المعزولة. Private/Isolated VLANs shall be configured for critical network segments or isolated segments.
12-4	منع إمكانية وصول الشبكات أو أجزاء الأنظمة الحساسة إلى أي نظام في البيئة ما لم يتم مسحها مع تطبيق الضوابط الأمنية المطلوبة والتحقق من الوضع الأمني للنظام. Networks or segments of critical systems shall not be allowed to access any system in the environment unless they are scanned, and if required security controls are applied and security posture of the system is verified.
13-4	عزل شبكة الاتصالات من خلال وضعها في شبكات محلية افتراضية منفصلة وملائمة بناءً على وظيفتها مع استغلال الشبكات المحلية الافتراضية الخاصة أو التجزئة الدقيقة للشبكة.

	Communications network shall be isolated by placing it in appropriate separate VLANs based on function and leveraging private VLANs or micro segmentation.
5	الوصول اللاسلكي (Wireless Access)
الهدف	ضبط استخدام الشبكات اللاسلكية وحمايتها.
المخاطر المحتملة	في حال تم ترك الشبكات اللاسلكية من دون حماية، ستتعرض جامعة حائل لمخاطر الاتصال غير المصرح به بالشبكة أو كشف البيانات.
الإجراءات المطلوبة	
1-5	إجراء تقييم مخاطر شامل لتقييم مخاطر اتصال الشبكات اللاسلكية بالشبكة الداخلية. A comprehensive risk assessment exercise shall be conducted to evaluate the risks of connecting wireless networks to the internal network.
2-5	الاحتفاظ بقائمة جرد بنقاط الوصول اللاسلكية المصرح بها والمتصلة بالشبكة السلكية. An inventory of authorized wireless access points connected to the wired network shall be maintained.
3-5	إعداد أدوات مسح الثغرات الأمنية في الشبكة لكشف أو منع أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده. Network vulnerability scanning tools shall be configured to detect and alert on unauthorized wireless access points connected to the wired network.
4-5	استخدام نظام كشف التسلل اللاسلكي (WIDS) لكشف أي وصول لاسلكي غير مصرح به متصل بالشبكة السلكية والتنبيه بوجوده. Wireless Intrusion Detection System (WIDS) shall be used to detect/prevent and alert on unauthorized wireless access points connected to the wired network.
5-5	إلغاء تفعيل الوصول اللاسلكي على الأجهزة التي لا تقتضي طبيعة عملها ذلك. Wireless access on devices that do not have a business purpose for wireless access shall be disabled.

6-5	إعداد الوصول اللاسلكي على أجهزة المتصلين التي لا تحتاج لذلك لغايات العمل بحيث يتم السماح بالوصول إلى الشبكات اللاسلكية المصرح بها فقط وتقييد الوصول إلى الشبكات اللاسلكية الأخرى. Wireless access on client machines that do not have a business need for wireless access shall be configured to allow access to authorized wireless networks only, and to restrict access to other wireless networks.
7-5	إلغاء تفعيل قدرات الشبكة اللاسلكية (المخصصة) لمشاركة الملفات بين الأجهزة مباشرة على الشبكات اللاسلكية لدى المتصلين. Peer-to-peer (ad hoc) wireless network capabilities shall be disabled on wireless clients.
8-5	إعداد نقاط الوصول اللاسلكية والأجهزة اللاسلكية للاتصال بالشبكة اللاسلكية باستخدام بروتوكولات آمنه مثل (WPA2) أو (WPA3). Wireless access points and wireless devices shall be configured to connect to the wireless network using secure protocol such as WPA2 or WPA3.
9-5	ضمان استخدام الشبكات اللاسلكية لبروتوكولات التحقق مثل بروتوكول المصادقة القابل للامتداد-أمن طبقة النقل (EAP/TLS) الذي يقتضي استخدام التحقّق من الهوية متعدّد العناصر بشكل متبادل. Wireless networks shall use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual Multi-Factor Authentication.
10-5	إلغاء تفعيل الوصول اللاسلكي للأجهزة الطرفية الموجودة على الأجهزة (مثل تقنية بلوتوث "Bluetooth" والاتصال قريب المدى "NFC") ما لم تقتضي طبيعة العمل ذلك. Wireless access of peripheral devices (such as Bluetooth and NFC) shall be disabled unless such access is required for a business purpose.
11-5	إيجاد شبكات لاسلكية منفصلة للأجهزة الشخصية أو غير الموثوقة، والتعامل مع هذه الشبكات بحذر واعتبارها مصادراً غير موثوقة مما يستدعي مراقبتها وتصفيتها بشكل مستمر.

	A separate wireless network shall be created for personal or untrusted devices. Enterprise access from this network shall be treated as untrusted and shall be filtered and audited accordingly.
6	التشفير (Cryptography)
الهدف	ضمان الحفاظ على سريّة حركة بيانات الشبكة والتأكّد من سريتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات المحمية.
المخاطر المحتملة	قد يؤدي عدم وجود التقنيات الأمنية المناسبة لضمان تشفير بيانات الشبكة إلى تعرض بيانات جامعة حائل لمخاطر سيبرانية عالية نتيجة الوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-6	وضع ضوابط على استخدام بروتوكولات الإدارة المشفرة الآمنة، مثل بروتوكول النقل الآمن (SSHv2) وبروتوكول التحكم بسطح المكتب عن بعد (RDP) عبر أمن طبقة النقل (TLS). The use of secure encrypted management protocols, such as Secure Shell (SSH) v2 and Remote Desktop Protocol (RDP) over TLS, shall be restricted.
2-6	تشفير حركة بيانات الشبكة السرية والمحمية باستخدام الجيل التالي من خوارزميات التشفير المدعومة (مثل التشفير بمجموعة "Suite B"). يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة حائل. Sensitive and confidential network traffic shall be encrypted by using next generation encryption cipher suites (such as Suite B cryptography). Refer to Hail university's Cryptography Standard.
3-6	تشفير حركة بيانات الوصول عن بعد عبر أمن بروتوكول الإنترنت (IPSec) أو أمن طبقة النقل (TLS) باستخدام الجيل التالي من خوارزميات التشفير المدعومة (مثل التشفير بمجموعة "Suite B"). يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة حائل. Remote access traffic over IPSec or TLS shall be encrypted with next generation encryption cipher suites (such as Suite B cryptography). Refer to Hail university's Cryptography Standard.

4-6	إعداد بروتوكولات التطبيقات لتستخدم التشفير حيثما أمكن (مثل: بروتوكول نقل النص التشعبي الآمن "HTTPS" وبروتوكول النقل الآمن "FTPS" عبر طبقة المنافذ الآمنة "SSL"، وبروتوكول النفاذ إلى الدليل البسيط "LDAP" عبر طبقة المنافذ الآمنة "SSL"). Application protocols shall be configured to use encryption wherever applicable (HTTPS, FTP over SSL, LDAP over SSL, etc.)
7	الأمن المادي (Physical Security)
الهدف	ضمان حماية جميع أجهزة الشبكة المطلوبة لاتصالات الشبكة من العبث أو التعديل أو أي هجمات مادية أخرى.
المخاطر المحتملة	يمكن أن يؤدي الهجوم المادي على أجهزة الشبكة التي تحفظ عمليات الاتصالات إلى الإضرار بالأصول المعلوماتية والتقنية الخاصة بـجامعة حائل، وبالتالي التأثير على سير أعمالها المعتاد. في حال تلف الجهاز أو العبث به أو تعديله مادياً، لا يمكن لـجامعة حائل الوثوق بالمعلومات المرسلة عبره وسيرتفع مستوى المخاطر التي قد تهدد أمن الشبكة.
الإجراءات المطلوبة	
1-7	وضع كافة أجهزة الشبكة المطلوبة لاتصالات الشبكة في منطقة آمنة مع تطبيق ضوابط الوصول المادي عليها. All network devices that are required for network communications shall be placed in a secured area with physical access controls implemented.
2-7	وضع معدات الشبكة الرئيسية في منطقة محمية بنظام إنذار. Core network equipment shall be placed in an alarmed area.
3-7	ربط معدات الشبكة الرئيسية بمولد طاقة غير منقطعة (UPS) أو نظام توليد للطاقة. Core network equipment shall be attached to a UPS or a generator system.
4-7	إعداد آليات الدفاع المادية في أجهزة الشبكة، بما في ذلك آليات مثل: • الحماية عبر إعدادات نظام الإدخال/الإخراج الأساسي (BIOS).

	• نظام الإنذار بوجود محاولة لفتح هياكل الأجهزة. تمكين تلك الآليات في حال توفرها للتقنيات الموجودة. Physical defensive mechanisms shall be configured in network devices, including: • BIOS protection • Chassis intrusion alarm These mechanisms shall be enabled if available for the technologies in place.
8	التسجيل والمراقبة (Logging and Monitoring)
الهدف	ضمان مراقبة وتخزين كافة الأحداث الحساسة المتعلقة بأمن الشبكة من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال جامعة حائل.
المخاطر المحتملة	لضمان سلامة الشبكة، يجب مراقبة كافة أجهزة الشبكة بشكل منتظم وضمان إمكانية الوصول إليها من قبل فرق الأمن السيبراني في جامعة حائل. دون القدرة على مراقبة وتسجيل الأحداث في الشبكة، لن تتمكن جامعة حائل من التحقيق في الهجمات التي يتعرض لها أمن الشبكة مما يؤدي إلى زيادة تكرار تلك الهجمات.
الإجراءات المطلوبة	
1-8	إعداد كافة أجهزة الأمن والشبكة لتسجيل سجلات الأحداث والتدقيق في نظام إدارة الأحداث والسجلات المركزي لأغراض التحليل والربط والتنبيه وفقاً لمعيار إدارة ومراقبة سجل الأحداث المعتمد في جامعة حائل. All network and security devices shall be configured to log events and audit logs to the central event and log management system for analysis, correlation and alerting as per Hail university's Event Log Management and Monitoring Standard.
2-8	ضمان اتساق كافة سجلات الأجهزة مع متطلبات معيار إدارة ومراقبة سجل الأحداث المعتمد في جامعة حائل. All device logs shall be consistent with the requirements of Hail university's Event Log Management and Monitoring Standard.

3-8	إعداد جميع أجهزة أمن الشبكة لتسجيل كافة طلبات شريط العنوان (URL) وكافة الجلسات المحجوبة وأحداث التهديدات. All network security devices shall be configured to log all URL requests, denied sessions and threat events.
4-8	إعداد أجهزة الشبكة لإرسال الأحداث المتعلقة بمحاولات الدخول الناجحة وغير الناجحة إلى واجهات الإدارة إلى نظام إدارة الأحداث والسجلات المركزي لأغراض التحليل والربط والتنبيه. Network devices shall be configured to send events related to failed and successful login to administration interfaces to the central event and log management system for analysis, correlation and alerting.
5-8	تخزين كافة السجلات في بيئة آمنة مع تفعيل خاصية التحكم بالوصول إليها. All logs shall be stored in a secured environment with access control enabled.
9	الإعدادات والتحصين والنسخ الاحتياطية (Secure Configuration and Backup)
الهدف	ضمان أن أي تغييرات تنطوي على مخاطر كبيرة على شبكة جامعة حائل ستسير وفقاً لعملية الرقابة على التغيير.
المخاطر المحتملة	لضمان سلامة الشبكة، يجب عمل نسخ احتياطية من الإعدادات قبل تنفيذ أي تغييرات قد تعرض شبكة جامعة حائل إلى مخاطر كبيرة، كما يجب وضع سجل بالتغييرات لتتبعها وتحديد الجهات المسؤولة عنها.
الإجراءات المطلوبة	
1-9	صياغة الحد الأدنى من المعايير الأمنية الأساسية (MBSS) لكافة أجهزة الشبكة. Minimum baseline security standards shall be developed for all network devices.
2-9	مراجعة الحد الأدنى من المعايير الأمنية الأساسية (MBSS) بشكل منتظم لكافة الأجهزة مرة واحدة كل 6 أشهر على الأقل. Minimum baseline security standards shall be regularly reviewed for all devices at least every six months.

3-9	ضمان امتثال جميع الأجهزة بالحد الأدنى من المعايير الأمنية الأساسية (MBSS) والإبلاغ عن أي انحرافات يتم اكتشافها. All devices shall be compliant with the minimum baseline security standards, and any deviations discovered shall be reported.
4-9	تطبيق واتباع عملية الرقابة على التغيير لأي تغييرات تنطوي على مخاطر كبيرة على شبكة جامعة حائل، بما في ذلك القواعد التي تسمح بتدفق حركة البيانات عبر أجهزة الشبكة وسياسات أمن جدران الحماية وترجمة عنوان الشبكة (NAT)، وغيرها. ويجب توثيق هذه العملية بما في ذلك العناصر التالية: • الغاية من القاعدة • الخدمات أو التطبيقات المتأثرة • المستخدمون والأجهزة المتأثرة • تاريخ إضافة القاعدة • تاريخ انتهاء صلاحية القاعدة، إذا كان ينطبق ذلك • اسم الشخص الذي أضاف القاعدة • بيان المشكلة • البيانات الداعمة • موافقة الإدارة على التغييرات A change control process shall be implemented and followed for any changes bearing a significant risk to Hail university's network, including rules that allow traffic to flow through network devices, firewall security policies, Network Address Translation (NAT), etc. The process shall be documented and shall include the following: • The rule's purpose • The affected service(s) or application(s) • The affected users and devices • The date when the rule was added • The rule's expiration date, if applicable • The name of the person who added the rule • The problem statement • Supporting data • Management's approval of changes

5-9	عمل نسخ احتياطية من الإعدادات لكافة معدات الشبكة المتضررة من التغيير قبل تطبيق التغيير على أرض الواقع. A backup of the configuration of all network equipment affected by a change shall be performed prior to the change implementation.
6-9	إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في جامعة حائل. Regular security testing, such as vulnerability assessments and penetration testing, shall be performed as per Hail university's Vulnerability Management Policy.
7-9	إجراء التحديثات والإصلاحات على أجهزة الشبكات بشكل منتظم وفقاً لسياسة إدارة التحديثات والإصلاحات في جامعة حائل لضمان تحديث جميع البرامج الثابتة على الأجهزة وتطبيق التحديثات والإصلاحات. Network devices shall be regularly patched and updated as per Hail university's Patch Management Policy to ensure all devices firmware is up-to-date and all patches are applied.
8-9	إزالة/إلغاء تفعيل الخدمات غير الضرورية أو غير اللازمة على أجهزة الشبكة مثل: بروتوكول النقل الآمن (FTP) أو بروتوكول تل نت (Telnet) أو غيرها. Unnecessary/unrequired services on network devices, such as FTP, Telnet, etc., shall be removed/disabled.
9-9	إعداد وضبط كافة أجهزة الشبكة ليتزامن وقتها مع ثلاث خوادم زمنية إضافية على الأقل. All network devices shall be configured to synchronize clock with at least three centralized time sources.
10	التحقق من سلامة البرمجيات والمعدات (Hardware and Software Integrity Validation)
الهدف	ضمان أن جميع برامج ومعدات الشبكة تأتي من مصادر شرعية وأنه لم يتم العبث بها والتحقق من ذلك.
المخاطر المحتملة	تعتبر الاختراقات في سلسلة الإمداد فرصة لتركيب وتثبيت البرامج والمعدات الخبيثة ضمن شبكة جامعة حائل، وقد تؤثر البرامج والمعدات التي تتعرض لانتهاك أمني على أداء الشبكة وتهدد سرية وسلامة وتوافر المعلومات الخاصة بـجامعة حائل. ونتيجة لذلك،

	سيصبح من الممكن تحميل البرمجيات غير المصرح بها أو الخبيثة على الجهاز بعد تشغيلها.
الإجراءات المطلوبة	
1-10	فحص كافة أجهزة الشبكة المادية بحثاً عن أي علامات لوجود عبث عند التركيب. All physical network devices shall be scanned for signs of tampering upon installation.
2-10	الحصول على البرمجيات وتحديثات النظام وحزم التحديثات والإصلاحات والترقيات الخاصة بمكونات الشبكة من مصادر موثوقة. Software, updates, patches, and upgrades to network components shall be obtained from validated sources.
3-10	أثناء تنزيل البرمجيات من الإنترنت، يجب التحقق من التجزئة مع قاعدة بيانات المورد لكشف أي تعديل غير مصرح به على البرامج الثابتة أو البرمجيات. When downloading software from the Internet, hash verification shall be compared against the vendor's database to detect unauthorized modification to firmware or software.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني.

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الالكتروني.

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذا المعيار دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة اختبار الاختراق

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير في تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في جامعة حائل وذلك من خلال محاكاة تقنيات وأساليب الهجوم السيبراني الفعلية، ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني لـجامعة حائل من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأنظمة الحساسة ومكوناتها التقنية، وجميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف الذكية واللوحية، والبريد الإلكتروني والدخول عن بعد في جامعة حائل، وتنطبق هذه السياسة على جميع العاملين في جامعة حائل.

بنود السياسة

1- المتطلبات العامة

1-1 يجب على جامعة حائل إجراء اختبار الاختراق (Penetration Testing) دورياً، لتقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني.

2-1 تحدد إدراة الأمن السيبراني الأنظمة والخدمات والمكونات التقنية التي يجب إجراء اختبار الاختراق عليها وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب على جامعة حائل إجراء اختبار الاختراق على جميع الخدمات المقدمة خارجياً ومكوناتها التقنية دورياً. (ECC-2-11-3-1)

4-1 يجب التأكد من أن اختبار الاختراق لا يؤثر على الأنظمة والخدمات المقدمة في جامعة حائل.

5-1 يجب على جامعة حائل إجراء اختبار الاختراق على الأنظمة الحساسة ومكوناتها التقنية كل ستة أشهر؛ على الأقل. (CSCC-2-10-2)

6-1 يجب إجراء اختبار الاختراق لاكتشاف نقاط الضعف الأمنية بكافة صورها والتي تشمل نقاط الضعف التي تنتج عادةً عن أخطاء في تطوير التطبيقات (Application Development Error) وضبط إعدادات النظام بشكل غير آمن (Configurations Faults) وإمكانية استغلال ثغرة محددة (Exploitability of Identified Vulnerability).

7-1 يجب تطوير إجراءات خاصة باختبار الاختراق واعتمادها ونشرها، مع الأخذ بالاعتبار عدم تأثيرها على سير الأعمال الخاصة بـجامعة حائل.

8-1 يجب على إدارة الأمن السيبراني تحديد أو الموافقة على أساليب اختبار الاختراق والأدوات والتقنيات التي يستخدمها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.

9-1 في حال تفويض طرف خارجي للقيام باختبار الاختراق نيابة عن جامعة حائل، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية ووفقاً لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة في جامعة حائل.

10-1 يجب تصنيف نتائج اختبار الاختراق بناءً على خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها ووفقاً لمنهجية إدارة المخاطر المعتمدة لدى جامعة حائل.

11-1 يجب وضع خطة عمل لمعالجة نتائج اختبار الاختراق يوضح فيها تأثير المخاطر وآلية معالجتها والمسؤول عن تطبيقها والفترة الزمنية اللازمة لتنفيذها.

2- متطلبات أخرى

1-2 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لعمليات اختبار الاختراق.

2-2 يجب مراجعة تطبيق متطلبات الأمن السيبراني لعمليات اختبار الاختراق في جامعة حائل دورياً. (ECC-2-11-4)

3-2 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الإلكتروني و إدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة إدارة الثغرات

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال؛ وذلك لمنع احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية أو تقليلها، وكذلك التقليل من الآثار المترتبة على أعمال جامعة حائل وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٠-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية والتقنية في جامعة حائل، وتنطبق هذه السياسة على جميع العاملين في جامعة حائل.

بنود السياسة

1- المتطلبات العامة

1-1 يجب على جامعة حائل إجراء فحص الثغرات (Vulnerabilities Assessment) دورياً، لاكتشاف وتقييم الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال.

2-1 تحدد إدارة الأمن السيبراني الأنظمة والخدمات والمكونات التقنية التي يجب إجراء فحص الثغرات عليها وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب على إدارة الأمن السيبراني التأكد من استخدام أساليب وأدوات موثوقة لاكتشاف الثغرات.

4-1 يجب تطوير واعتماد إجراءات خاصة بتنفيذ فحص واكتشاف الثغرات وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.

5-1 في حال تفويض طرف خارجي للقيام بفحص واكتشاف الثغرات نيابة عن جامعة حائل، يجب التحقق من تطبيق جميع متطلبات الأمن السيبراني المتعلقة بالأطراف الخارجية وفقاً لسياسة الأمن السيبراني المتعلّق بالأطراف الخارجية المعتمدة في جامعة حائل.

2- متطلبات تقييم الثغرات

1-2 يجب فحص واكتشاف الثغرات قبل نشر الخدمات أو الأنظمة على الإنترنت أو عند القيام بأي تغيير على الأنظمة الحساسة وفقاً لسياسة الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية.

2-2 يجب تصنيف الثغرات حسب خطورتها، ومعالجتها حسب المخاطر السيبرانية المترتبة عليها وفقاً لمنهجية إدارة المخاطر المعتمدة لدى جامعة حائل.

2-3 يجب على جامعة حائل إجراء تقييم الثغرات لجميع الأصول التقنية ومعالجتها دورياً. (ECC-2-10-3-1)

2-4 يجب على جامعة حائل إجراء تقييم الثغرات للمكونات التقنية للأنظمة الحساسة الداخلية ومعالجتها كل ثلاثة أشهر؛ على الأقل. (CSCC-2-9-1-3)

2-5 يجب على جامعة حائل إجراء تقييم الثغرات للمكونات التقنية للأنظمة الحساسة الخارجية والمتصلة بالإنترنت مرة واحدة شهرياً. (CSCC-2-9-1-2)

3- متطلبات معالجة الثغرات

3-1 بعد الانتهاء من تقييم الثغرات، يجب إعداد تقرير يوضح الثغرات المكتشفة وتصنيفها والتوصيات المقترحة لمعالجتها.

3-2 بعد إرسال تقرير تقييم الثغرات ومعالجتها من قبل الأطراف المعنية، يجب إجراء فحص واكتشاف الثغرات المكتشفة مرة أخرى للتأكد من معالجتها.

3-3 يجب استخدام حزم التحديثات والإصلاحات من مصادر موثوقة وآمنة ووفقاً لسياسة حزم التحديثات والإصلاحات.

3-4 يجب إصلاح وإغلاق الثغرات الحرجة (Critical Vulnerabilities) المكتشفة حديثاً، مع اتباع آليات إدارة التغيير المتبعة لدى جامعة حائل. (CSCC-2-9-1-3)

3-5 في حال تعذر إصلاح وإغلاق الثغرة الأمنية لأي سببٍ كان، يجب تطبيق ضوابط أخرى مثل إيقاف تشغيل الخدمة المتعلقة بالثغرة الأمنية، أو توفير ضابط حماية بديل (Compensating Control) مثل التحكم بالوصول عن طريق جدران الحماية وغيرها من الحلول، ومراقبة الثغرة الأمنية للهجمات الفعلية، وإبلاغ فريق الاستجابة للحوادث بهذه الثغرة واحتمالية استغلالها.

4- متطلبات أخرى

4-1 يجب على جامعة حائل التواصل والاشتراك مع مصادر أمن سيبراني موثوقة توفر المعلومات الاستباقية (Threat Intelligence)، ومجموعات خاصة ذات اهتمامات مشتركة وخبراء خارجيين في المواضيع المعنية من أجل جمع المعلومات حول التهديدات الجديدة وكيفية الحد من الثغرات الموجودة. (ECC-2-10-3-5)

4-2 يجب مراجعة تطبيق متطلبات الأمن السيبراني لإدارة الثغرات التقنية لـجامعة حائل دورياً.

4-3 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لإدارة الثغرات.

4-4 يجب مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني .

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الإلكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل دوري.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة أمن قواعد البيانات

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

متاح

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية قواعد البيانات (Database) الخاصة بـجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط ١-٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أنظمة قواعد البيانات الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل.

بنود السياسة

1- البنود العامة

1-1 يجب تحديد وتوثيق جميع أنظمة قواعد البيانات المستخدمة داخل جامعة حائل والعمل على توفير البيئة المناسبة لحمايتها من المخاطر البيئية والتشغيلية.

2-1 يجب تطوير واعتماد معايير التقنية الأمنية لأنظمة قواعد البيانات داخل جامعة حائل وتطبيقها من قبل مشرفي قواعد البيانات.

3-1 فيما عدا مشرفي قواعد البيانات، يمنع الوصول أو التعامل المباشر مع قواعد البيانات الخاصة بالأنظمة الحساسة، ويتم ذلك من خلال التطبيقات فقط. (CSCC-2-2-1-8)

4-1 يتم منح حق الوصول إلى قواعد البيانات وفقاً لسياسة إدارة هويات الدخول والصلاحيات.

5-1 يمنع نسخ أو نقل قواعد البيانات الخاصة بالأنظمة الحساسة من بيئة الإنتاج إلى أي بيئة اخرى. (CSCC-2-6-1-5)

2- الإجراءات الأمنية المطلوبة لاستضافة قواعد البيانات

1-2 التحديد الواضح لمتطلبات استمرارية الأعمال والتعافي من الكوارث الخاصة بقواعد البيانات المستضافة في العقود المعنية مع مزوّد الخدمة السحابية، والتي تتضمّن الأدوار والمسؤوليات المتبادلة من حيث النسخ الاحتياطية والاستجابة للحوادث وخطة التعافي من الكوارث وغيرها.

2-2 توفير العزل المنطقي بين قواعد البيانات الخاصة بـجامعة حائل وقواعد البيانات المستضافة الأخرى.

3-2 يجب أن يكون موقع الاستضافة الخاص بالخدمات السحابية موجوداً ضمن النطاق الجغرافي للمملكة العربية السعودية. (ECC-3-3-2-4)

4-2 تقييد صلاحية الوصول الإداري إلى قواعد البيانات باستخدام وسيلة تشفير مُحكَمة مثل بروتوكول النقل الأمن (SSH)، أو الشبكات الخاصة الافتراضية (VPN)، أو طبقة المنافذ الآمنة (SSL)/أمن طبقة النقل (TLS)، وذلك وفقاً لسياسة التشفير المعتمدة في جامعة حائل.

3- المتطلبات المتعلّقة بإدارة التغييرات على أنظمة قواعد البيانات

1-3 يجب أن تتم التغييرات على قواعد البيانات (مثل ترحيل قواعد البيانات، والنقل إلى بيئة الإنتاج) وفقاً لعملية إدارة التغيير المعتمدة في جامعة حائل.

2-3 يتم تثبيت التحديثات والإصلاحات على نظام قواعد البيانات وفقاً لسياسة إدارة حزم التحديثات والإصلاحات المعتمدة في جامعة حائل.

3-3 التأكد من استخدام أنظمة قواعد بيانات موثوقة ومعتمدة ومرخصة.

4-3 التأكد من وجود خطة واضحة للتعافي من الكوارث خاصة بأنظمة قواعد البيانات.

5-3 يجب على جامعة حائل توقيع اتفاقية مستوى الخدمة للدعم مع المورّدين فيما يتعلّق بنظام إدارة قواعد البيانات في بيئة الإنتاج.

6-3 تطبيق التجزئة والتشفير على قواعد البيانات المخزنة وفقاً لسياسة التصنيف وسياسة التشفير المعتمدة في جامعة حائل.

4- مراقبة سجلات الأحداث المتعلقة بنظام قواعد البيانات

1-4 تفعيل وحفظ سجلات الأحداث الخاصة بنظام قواعد البيانات وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة في جامعة حائل.

2-4 يجب على إدارة الأمن السيبراني مراقبة سجلات الأحداث المتعلقة بقواعد البيانات الخاصة بالأنظمة الحساسة، ومراقبة سلوك المستخدمين.

3-4 يجب على أدارة الامن السيبراني مراقبة سجلات الأحداث الخاصة بمشرفي قواعد البيانات ومراقبة سلوكهم ومراجعتها دورياً.

5- المتطلبات التشغيلية

1-5 توفير المتطلبات اللازمة لتشغيل قواعد البيانات بشكل آمن وملائم، مثل توفير بيئة مناسبة وآمنة، وتقييد الوصول المادي إلى الأنظمة والسماح بذلك للعاملين المصرح لهم فقط.

2-5 يجب على عمادة تقنية المعلومات والتعليم الإلكتروني مراقبة أنظمة قواعد البيانات التشغيلية والتأكد من جودة أدائها، وتوافرها، وتوفير سعة تخزينية مناسبة، ونحوه.

3-5 مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أنظمة قواعد البيانات. (ECC-2-3-3-4)

6- متطلبات أخرى

1-6 استخدام مؤشر قياس الأداء (Key Performance Indicator "KPI") لضمان التطوير المستمر لنظام إدارة قواعد البيانات.

2-6 مراجعة متطلبات الأمن السيبراني الخاصة بإدارة قواعد البيانات سنوياً على الأقل، أو في حال حدوث تغييرات في المتطلبات التشريعية أو التنظيمية أو المعايير ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** مدير إدارة لأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الإلكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة حماية تطبيقات الويب

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية تطبيقات الويب الخارجية الخاصة بـجامعة حائل، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١٥-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع تطبيقات الويب الخارجية الخاصة بـجامعة حائل، وتنطبق هذه السياسة على جميع العاملين في جامعة حائل.

بنود السياسة

1 المتطلبات العامة

1-1 يجب أن تتبع تطبيقات الويب الخارجية التي يتم شراؤها أو تطويرها داخلياً مبدأ المعمارية متعددة المستويات (Multi-tier Architecture). (ECC-2-15-3-2)

2-1 يجب استخدام مبدأ المعمارية متعددة المستويات لتطبيقات الويب الخارجية للأنظمة الحساسة على ألا يقل عدد المستويات عن 3 مستويات (3-tier Architecture). (CSCC-2-12-2)

3-1 يجب التأكد من استخدام بروتوكولات الاتصالات الآمنة فقط، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS) وبروتوكول نقل الملفات الآمن (SFTP) وأمن طبقة النقل (TLS) وغيرها. (ECC-2-15-3-3)

4-1 يجب استخدام نظام جدار الحماية لتطبيقات الويب (Web Application Firewall "WAF") لحماية تطبيقات الويب الخارجية من الهجمات الخارجية. (ECC-2-15-3-1)

5-1 يجب تطبيق العزل المنطقي لبيئة التطوير (Development Environment) وبيئة الاختبار (Testing Environment) عن بيئة الإنتاج (Production Environment).

6-1 يجب استخدام تقنيات حماية البيانات والمعلومات في تطبيقات الويب الخارجية ووفقاً لسياسة حماية البيانات والمعلومات وسياسة التصنيف.

7-1 في حال شراء تطبيقات ويب من طرف خارجي، يجب التأكد من التزام المورد بسياسات ومعايير الأمن السيبراني في جامعة حائل.

8-1 يجب تطبيق الحد الأدنى على الأقل لمعايير أمن التطبيقات وحمايتها (Ten OWASP Top) لتطبيقات الويب الخارجية للأنظمة الحساسة. (CSCC-2-12-1-2)

2 متطلبات حق الوصول (Access Right)

2-1 يجب استخدام التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication) لعمليات دخول المستخدمين على تطبيقات الويب الخارجية. (ECC-2-15-3-5)

2-2 يجب توثيق واعتماد معايير أمنية لتطوير تطبيقات الويب، وتشمل كحد أدنى إدارة الجلسات بشكل آمن (Secure Session Management) وموثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout). (CSCC-2-12-1-1)

2-3 ينبغي أن يقتصر حق الوصول إلى منظومات الإنتاج، وأن يتم التحكم به وفقاً للمسؤوليات الوظيفية.

2-4 يجب نشر سياسة الاستخدام الآمن لجميع مستخدمي تطبيقات الويب الخارجية. (ECC-2-15-3-4)

3 متطلبات تطوير أو شراء تطبيقات الويب

3-1 يجب إجراء تقييم لمخاطر الأمن السيبراني عند التخطيط لتطوير أو شراء تطبيقات الويب وقبل إطلاقها في بيئة الإنتاج ووفقاً لسياسة إدارة مخاطر الأمن السيبراني المعتمدة في جامعة حائل.

3-2 قبل استخدام المعلومات المحمية في بيئة الاختبار، يجب الحصول على إذن مسبق من إدارة الأمن السيبراني واستخدام ضوابط مشددة لحماية تلك البيانات، مثل: تقنيات مزج البيانات (Data Scrambling) وتقنيات تعتيم البيانات (Data Masking)، وحذفها مباشرة بعد الانتهاء من استخدامها.

3-3 يجب حفظ شفرة المصدر (Source Code) بشكل آمن وتقييد الوصول إليها للمصرح لهم فقط.

3-4 يجب إجراء اختبار الاختراق لتطبيق الويب الخارجي في بيئة الاختبار وتوثيق النتائج والتأكد من معالجة جميع الثغرات قبل إطلاق التطبيق على بيئة الإنتاج.

3-5 يجب إجراء فحص الثغرات للمكونات التقنية لتطبيقات الويب والتأكد من معالجتها بتثبيت حزم التحديثات والإصلاحات المعتمدة لدى جامعة حائل.

3-6 يجب اعتماد تطبيقات الويب من قبل اللجنة التقنية الاستشارية للتغيير (CAB) قبل إطلاقها في بيئة الإنتاج.

4 متطلبات أخرى

4-1 يجب مراجعة متطلبات الأمن السيبراني الخاصة بحماية تطبيقات الويب الخارجية دورياً. (ECC-2-15-4)

4-2 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية تطبيقات الويب الخارجية.

4-3 تتم مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الإلكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة بشكل مستمر.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

معيار الحماية من البرمجيات الضارة

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو تطبيق متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بالحماية من البرمجيات الضارة في جامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية، وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل وينطبق هذا المعيار على جميع العاملين في جامعة حائل.

المعايير

1	تطبيق تقنيات وآليات الحماية من البرمجيات الضارة (Malware Protection (Solution Implementation
الهدف	ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية لـجامعة حائل، وذلك بتطبيق تقنيات وآليات للحماية من البرمجيات الضارة.
المخاطر المحتملة	يُعد غياب تقنيات وآليات الحماية من البرمجيات الضارة سبباً أساسياً في انتهاك سرية أو سلامة أو توافر البيانات أو التطبيقات أو نظم التشغيل نتيجة تسرب البرمجيات الضارة بمختلف أنواعها إلى أجهزة معالجة المعلومات الخاصة بـجامعة حائل.
الإجراءات المطلوبة	
1-1	يجب أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بالقدرات التالية: • منع البرمجيات الضارة • اكتشاف البرمجيات الضارة Malware protection solutions shall have the following capabilities: • Malware Prevention • Malware Detection

2-1	يجب أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بالقدرات اللازمة للحماية من مختلف أنواع البرمجيات الضارة ومنها: • الفيروسات • الديدان الحاسوبية • فيروسات حصان طروادة • برامج التجسس • البرمجيات الضارة غير المعروفة مسبقًا Malware protection solutions shall have the capabilities to protect against different varieties of malware including but not limited to: • Viruses • Worms • Trojan Horses • Spyware • Zero-day malware
3-1	يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة لحماية النهايات الطرفية في الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل بما في ذلك: • جدار الحماية • خوادم البريد الإلكتروني • خوادم شبكة الويب • الخوادم الوكيلة • خوادم الوصول عن بُعد • أجهزة المستخدمين • الأجهزة المحمولة Malware protection solutions shall be configured to protect the endpoints of Hail University's information and technology assets, including: • Firewalls • Email servers • Web servers • Proxy servers • Remote-access servers • Workstations

• Mobile devices	
يجب أن تتمتع تقنيات وآليات الحماية من البرمجيات الضارة بلوحة تحكم مركزية، مما يضمن التطبيق المتسق لسياسة الحماية من البرمجيات الضارة على جميع الأجهزة ومراقبة تهديدات هذه البرمجيات الضارة. Malware protection solutions shall have a central console. This will ensure a consistent implementation of Malware Protection Policy across all endpoints, and continuous monitoring of malware threat.	4-1
يجب أن تتكون تقنيات وآليات الحماية من البرمجيات الضارة من واحدة أو أكثر من الأدوات التي تؤدي وظائف كل من: • برامج مكافحة الفيروسات • نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات • جدار الحماية • تصفية/فحص المحتوى • السماح بقائمة محددة من التطبيقات يجب أن تُحدد وظائف تقنيات وآليات الحماية من البرمجيات الضارة بناءً على مخرجات عملية تقييم المخاطر. Malware protection solution shall be comprised of one or multiple tools that provide the functions of: • Antivirus Software • Intrusion Prevention System • Firewall • Content Filtering/Scanning • Application Whitelisting The functions of malware protection solutions shall be determined based on the outcomes of the risk assessment process.	5-1
يجب إرسال سجلات الأحداث المتعلقة باكتشاف ومنع البرمجيات الضارة إلى تقنية الحماية من البرمجيات الضارة وإلى نظام سجلات الأحداث ومراقبة الأمن السيبراني لمراقبة الأحداث وتحليلها، وتحديد أوجه الارتباط، واتخاذ القرار. Malware detection and prevention events shall be sent to the central malware protection solution and to the central event	6-1

	and log management solution for analysis, correlation and decision-making.
7-1	يجب الاستمرار على تطبيق آليات الحماية من البرمجيات الضارة للحد من أثر تهديدات البرمجيات الضارة في حال حدوثها. وتشمل هذه الآليات ما يلي: • الحماية عبر إعدادات نظام الإدخال/الإخراج الأساسي (BIOS). • آلية فصل التطبيقات غير الموثوقة. • الفصل بين استخدامات المتصفح للتطبيقات المؤسسية وغير المؤسسية. • الفصل من خلال الأنظمة الافتراضية. • تقييد التفعيل التلقائي للملفات التي يتم تنزيلها أو البرامج المشتركة أو البرامج المجانية. • اقتصار صلاحيات المستخدم النهائي على الجهاز الذي يستخدمه (دون منحه حقوق إدارية). • تقييد التفعيل التلقائي أو استخدام الملفات المحتوية على حزم (Macros). • حجب أنظمة التحميل والتشغيل (Booting Systems) الموجودة على الأقراص المرنة أو الأقراص المدمجة، إلا في الحالات الطارئة أو عند استخدام وسائط موثوقة. • إعداد كافة البرمجيات لتنبيه المستخدم في حال فتح ملفات تحتوي على حزم (Macros). Malware defensive mechanisms shall be also implemented to reduce the impact of malware threats if they occur. Those mechanisms include: • BIOS protection. • Application sandboxing. • Browser segregation for corporate and non-corporate applications. • Segregation through virtualization. • Restriction of the automatic activation of a downloaded file, shareware or freeware. • Restriction of end user's privileges on the device they use (without administrative rights). • Restriction of the automatic activation or use of macro files. • Denial of booting systems from diskettes or CDs except in case of an emergency and when using verified media.

	• Configuration of all software to warn the user in case documents with macros are opened.
8-1	يجب أن يكون إجراء إزالة تثبيت برنامج تقنيات وآليات الحماية من البرمجيات الضارة محمياً بكلمة مرور وتتم إدارته عن بعد لضمان عدم قدرة المستخدم على إزالة تثبيت البرنامج أو تغيير إعداداته أو إلغاء تفعيله. Uninstallation of a malware protection solution's agent shall be password protected and remotely managed to ensure that end users are unable to uninstall the agent, change its settings, or deactivate it.
2	إعدادات تقنيات وآليات الحماية من البرمجيات الضارة (Malware Protection (Solution Configuration
الهدف	التأكد من تطبيق الإعدادات الصحيحة لتقنيات وآليات الحماية من البرمجيات الضارة وذلك لتوفير الحماية الفعالة من تهديدات البرمجيات الضارة.
المخاطر المحتملة	تؤدي الإعدادات غير المكتملة لتقنيات وآليات الحماية من البرمجيات الضارة إلى انتشار البرمجيات الضارة غير المكتشفة في بيئة جامعة حائل وبالتالي تقليل فعالية الحل بشكل عام.
الإجراءات المطلوبة	
1-2	يجب ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة لإجراء فحص مباشر لجميع الملفات عند الوصول إليها أو نسخها أو نقلها لضمان اكتشاف جميع البرمجيات الضارة قبل تنشيطها. The malware protection solution's agent shall be configured to perform a real time scan on all files when they are accessed, copied or transferred. This will ensure the detection of all malware before activation.
2-2	يجب إعداد برنامج تقنيات وآليات الحماية من البرمجيات الضارة لإجراء فحص كامل للنظام أسبوعياً على الأقل، ويمكن أن يكون وقت الفحص عند تشغيل النظام أو خلال ساعات الاستخدام المنخفض. The malware protection solution's agent shall be configured to perform full system scan at least once a week. The time of scanning can be either when the system boots up or during non-peak usage hours.

3-2	تمكين خاصية فحص مكافحة البرمجيات الضارة للوسائط القابلة للإزالة عند إدخالها أو توصيلها. Anti-malware scanning shall be enabled for removable media when they are inserted or connected.
4-2	ضبط وإعداد الأجهزة بصورة تمنع التشغيل التلقائي للمحتوى. Devices shall be configured to not auto-run content.
5-2	تفعيل خاصية تسجيل استعلامات نظام أسماء النطاقات (DNS) للكشف عن الاستعلامات الخاصة بنطاقات نظام أسماء النطاقات (DNS) الضارة المعروفة. DNS query logging shall be enabled to detect queries for known malicious DNS domains.
6-2	تفعيل ميزات مكافحة الاستغلال على نظام التشغيل لاكتشاف و/أو منع الأنشطة المشبوهة والضارة. Operating system anti-exploitation features shall be enabled to detect and/or prevent suspicious and malicious activities.
7-2	يجب ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة لاكتشاف البرمجيات الضارة أولاً ثم الاستجابة لها على النحو التالي: تطهير البرمجيات الضارة، أو حذفها، أو عزلها أو تشفيرها. يجب أن يكون التشفير قابلاً للفك في حالة الاكتشاف الخاطئ لإحدى البرمجيات الضارة. The malware protection solution shall be configured to firstly detect then respond to the malware as follows: disinfect, delete, quarantine or encrypt malware upon detection. Encryption of the malware shall be reversible in the case of false positive detection.
8-2	ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة بحيث يقوم بعزل الملفات التي أصابها الفيروس في حال عدم القدرة على حذفها. The malware protection solution's agent shall be configured to quarantine virus-infected files if they cannot be cleaned.
9-2	ضبط إعدادات تقنيات وآليات الحماية من البرمجيات الضارة بحيث يقوم بتنبيه المستخدم بعدم قدرته على تنظيف أو عزل الشفرة الخبيثة.

The malware protection solution's agent shall be configured to notify the user if it is unable to clean or quarantine the malicious code detected on the machine.	
تنصيب تقنيات وآليات الحماية من البرمجيات الضارة على خوادم البريد الإلكتروني، بما في ذلك بوابة بروتوكول إرسال البريد البسيط (SMTP). يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة بحيث تقوم بمسح محتوى الرسائل والمرفقات في كافة رسائل البريد الإلكتروني. وفي حال العثور على برمجيات ضارة في بروتوكول إرسال البريد البسيط (SMTP) الوارد، يجب اتباع الإجراءات التالية: • حذف الفيروسات بالمرفقات المصابة. • عزل المرفقات المصابة في حال عدم القدرة على مسحها. Malware protection solutions shall be installed on email servers including SMTP gateway. Malware protection solutions shall be configured to scan email content and attachments in all emails. If malware is found in an incoming SMTP mail, then the following actions shall be taken: • Infected attachments shall be cleaned. • Infected attachments shall be quarantined if cleaning them was not possible.	10-2
ضبط إعدادات نظام التشغيل والتطبيقات على لوحة التحكم المركزية بتقنيات وآليات الحماية من البرمجيات الضارة وفقاً لإرشادات الإعداد الآمن التي يوفرها المورد. Operating system and applications on the malware protection solution's central console shall be configured as per the relevant vendor's secure configuration guidelines.	11-2
منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت والمعروفة باستضافتها لمحتوى خبيث باستخدام آلية تصفية محتوى الويب. Access to websites and other resources on the Internet known to host malicious content shall be prevented using a web content filtering mechanism.	12-2
تقوم جامعة حائل بمراقبة الأداء للمعايير التالية: • استخدام وحدة التحكم المركزية (CPU) • استخدام الذاكرة • أداء الشبكة	13-2

	• استخدام القرص <Entity name> shall carry out performance monitoring for the following parameters: • CPU Utilization • Memory Utilization • Network Performance • Disk Utilization
14-2	يجب أن يقدم مشرفو تقنيات وآليات الحماية من البرمجيات الضارة تقاريراً شهرية حول حالة الحماية من البرمجيات الضارة إلى إدارة الأمن السيبراني في جامعة حائل. ويجب أن يتضمن التقرير على الأقل ما يلي: • عدد أجهزة الحاسوب والخوادم وأجهزة الحاسوب المحمولة والأنظمة غير المحدثة بأحدث أنماط التواقيع. • أهم 10 برمجيات ضارة تم اكتشافها. • عدد الفيروسات/الديدان الحاسوبية/البرامج الخبيثة المكتشفة. • عدد الفيروسات/الديدان الحاسوبية/البرامج الخبيثة التي تم تنظيفها/عزلها/حذفها. • الإجراء المُتخذ لحل مشكلة الإصابة بالبرمجيات الضارة. • مصدر الإصابة. Malware protection solutions' administrators shall submit periodic reports on a monthly basis on the status of malware protection to Hail University's Cybersecurity Department. The report shall include the following at a minimum: • Number of PCs, servers, laptops and systems not updated with the latest signature patterns. • Top 10 detected malware. • Number of viruses/worms/malicious programs detected. • Number of viruses/worms/malicious programs cleaned/quarantined/deleted. • Action taken to resolve the malware infection. • Source of infection.

3	تحديثات تقنيات وآليات الحماية من البرمجيات الضارة (Malware Protection (Solution Updates
الهدف	ضمان تحديث تقنيات وآليات الحماية من البرمجيات الضارة لحماية الأصول المعلوماتية والتقنية من أحدث البرمجيات الضارة المعروفة.
المخاطر المحتملة	يمكن أن تمر أحدث البرمجيات الضارة المعروفة دون أن يتم كشفها، وقد تؤدي إلى انتهاك الأمن السيبراني لـجامعة حائل في حال عدم تحديث تقنيات وآليات الحماية من البرمجيات الضارة بأحدث التواقيع.
الإجراءات المطلوبة	
1-3	يجب تحديث تقنيات وآليات الحماية من البرمجيات الضارة بشكل مستمر وتلقائي وفقاً لسياسة إدارة التحديثات والإصلاحات. Malware protection solutions shall be automatically updated on a regular basis as per Patch Management Policy.
2-3	يجب التحقق من سلامة المعلومات والملفات الخاصة بتقنيات وآليات الحماية من البرمجيات الضارة دورياً. Malware protection solutions shall be periodically verified for integrity.
3-3	يجب تحديث قاعدة بيانات تواقيع تقنيات وآليات الحماية من البرمجيات الضارة تلقائياً أو يدوياً بشكل منتظم. Malware protection solutions' signature database shall be automatically or manually updated on a regular basis.
4-3	يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة للحصول على نمط التواقيع من الموقع الإلكتروني للمورد. Malware protection solutions shall be configured to acquire the signature pattern from the trusted vendor’s website.
5-3	يجب إعداد تقنيات وآليات الحماية من البرمجيات الضارة "لتوزيع" آخر تحديثات التواقيع على أجهزة المستخدمين والخوادم. Malware protection solutions shall be configured to “push” the latest signature updates to all workstations and servers.

6-3	يجب ضبط إعدادات الأجهزة غير الموجودة ضمن شبكة الأجهزة المحمولة في جامعة حائل لتتضمن خيارات تحديث بديلة بحيث يمكن تحديث التواقيع مباشرة من الموقع الإلكتروني للمورد. Systems which are not on Hail University's mobile device network shall be configured with alternative update options whereby the signatures can be directly updated from the vendor's website.
7-3	يجب أن تدعم تقنيات وآليات الحماية من البرمجيات الضارة استرجاع تحديثات التواقيع في حال أدت آخر التحديثات إلى عدم اتساق برنامج مكافحة الفيروسات وأثرت على قدرته على العمل بالصورة المتوقعة. Malware protection solutions shall support signature update rollback in case the current latest updates make the antivirus software inconsistent and incapable of operating as expected.
4	تتبع التهديدات والثغرات الجديدة (Tracking New Threats and Vulnerabilities)
الهدف	التحديد المبكر للتهديدات الجديدة التي يمكن أن تؤثر على أمن جامعة حائل وضمان اتخاذ الإجراءات المناسبة للحد من المخاطر المرافقة.
المخاطر المحتملة	يمكن أن تتعرض جامعة حائل لانتهاك أمني نتيجة عدم القدرة على كشف البرمجيات الضارة الخبيثة الجديدة وغير المعروفة.
الإجراءات المطلوبة	
1-4	يجب أن تتابع جامعة حائل التهديدات الجديدة الناشئة عن الشفرات الخبيثة ويجب أن تحتفظ بقائمة بكافة السيناريوهات المحتملة للإصابة بالبرمجيات الخبيثة (مثل: كيف يمكن للفيروس أن يؤثر على الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل وما هي طريقة وصوله إليها). Hail University shall keep track of new threats arising from malicious code and shall maintain a list of the possible infection scenarios (e.g., how and in what way the virus can affect Hail University's information and technology assets).
2-4	يجب تحديد السيناريوهات بوضوح ويجب أن تتصدى تقنيات الحماية من البرمجيات الضارة لهذه البرمجيات وتتخلص منها على كافة المستويات.

	Scenarios shall be clearly identified, and the malware protection solution shall fight and remove malware on all levels.
3-4	عند وجود ثغرات جديدة، يجب أن تحدد جامعة حائل الخطوات التي يجب اتخاذها لضمان الحد من المخاطر المحتملة. When a new vulnerability is published, Hail University shall identify the steps that need to be taken to ensure that the associated risks are mitigated.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف علي إدارة الأمن السيبراني.

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني.

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذا المعيار دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

سياسة التشفير

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية الخاصة بـجامعة حائل وللتقليل من المخاطر السيبرانية والتهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

تهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٨-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع الأصول المعلوماتية الإلكترونية الخاصة بـجامعة حائل، وتنطبق على جميع العاملين في جامعة حائل، بما في ذلك الجهات التي تتعامل معها والأطراف الخارجية.

بنود السياسة

1- البنود العامة

1-1 يجب على جامعة حائل تطوير وتوثيق واعتماد إجراءات ومعايير خاصة بالتشفير بناءً على حاجة العمل وعلى تحليل المخاطر في جامعة حائل وبحيث يتوافق المستوى الأمني مع المعايير الوطنية للتشفير الصادرة من قبل الهيئة الوطنية للأمن السيبراني. وتشمل هذه الإجراءات على حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً)، وطرق استخدامها وآلية إصدار المفاتيح ونشرها واستعادتها، بالإضافة إلى إدارة النسخ الاحتياطية للمفاتيح وإجراءات إتلاف مفاتيح التشفير. (ECC-2-8-3-1)

2-1 يجب تشفير البيانات أثناء النقل والتخزين بناءً على تصنيفها وحسب السياسات والإجراءات التنظيمية لـجامعة حائل، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

3-1 يجب استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وفقاً لما تصدره الهيئة بهذا الشأن. (CSCC-2-7-1-3)

4-1 يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء النقل (Data-In-Transit). (CSCC-2-7-1-1)

5-1 يجب تشفير جميع بيانات الأنظمة الحساسة، أثناء التخزين (Data-at-Rest) على مستوى الملفات، وقاعدة البيانات، أو على مستوى أعمدة محددة داخل قاعدة البيانات. (CSCC-2-7-1-2)

6-1 يجب تحديد وتوثيق الأدوار والمسؤوليات المتعلقة بإدارة البنية التحتية لمفاتيح التشفير (Key Management Infrastructure "KMI")، للأدوار التالية على الأقل:

1-6-1 مسؤول مفاتيح وأنظمة التشفير (Keying Material Manager) باعتباره مدير إدارة الأمن السيبراني.

1-6-2 مشرفو التشفير المسؤولون عن حماية مفاتيح التشفير (Key Custodians).

1-6-3 الجهات المعنية بإصدار الشهادات (Certification Authorities "CAs")، بحيث تكون موثوقة وآمنة.

1-6-4 الجهات المعنية بتسجيل الشهادات (Registration Authorities "RAs")، بحيث تكون موثوقة وآمنة.

2- الاستخدام الآمن للتشفير

2-1 يجب تحديد وتوثيق كافة حلول التشفير المستخدمة (بما في ذلك الخوارزميات والبرامج والوحدات (Modules) والمكتبات (Libraries) ومكونات التشفير الأخرى) وتقييمها واعتمادها من قبل إدارة الأمن السيبراني قبل تطبيقها في جامعة حائل.

2-2 يجب التأكد من تطبيق التشفير وفقاً لحلول التشفير المعتمدة لدى جامعة حائل.

2-3 يُمنع استخدام خوارزميات التشفير المطورة داخلياً وفقاً لدليل التشفير الخاص بمشروع أمان تطبيق الويب المفتوح (OWASP).

2-4 يجب استخدام طرق التحقق الآمن (مثل استخدام مفاتيح التشفير العامة والتواقيع الرقمية والشهادات الرقمية) للحد من المخاطر السيبرانية ووفقاً لحلول التشفير المعتمدة في جامعة حائل.

2-5 يجب استخدام التحقق من هوية المستخدم لنقل البيانات السرية للغاية إلى أطراف خارجية باستخدام شهادات التشفير الرقمية (Digital Certificates) المعتمدة، ووفقاً لسياسة حماية البيانات والمعلومات المعتمدة في جامعة حائل.

2-6 يجب استخدام وسيلة تحقق من الهوية متعددة العناصر (Multi-Factor Authentication "MFA") للتحقق من صلاحية المستخدم للوصول إلى الأنظمة الحساسة وفقاً لسياسة حماية البيانات والمعلومات المعتمدة لدى جامعة حائل.

3- إدارة مفاتيح التشفير

3-1 يجب إدارة مفاتيح التشفير بطريقة آمنة خلال عمليات دورة حياتها (Key Lifecycle Management) والتأكد من استخدامها بشكل سليم وفعّال. (ECC-2-8-3-2)

3-2 يجب أن يتم إصدار شهادات التشفير عن طريق جهة إصدار الشهادات الداخلية في جامعة حائل للخدمات المحلية أو عن طريق جهة خارجية موثوقة.

3-3 يجب حفظ معلومات المفاتيح الخاصة (Private Key) في مكان آمن (وخاصة إذا كانت تستخدم للتوقيع الإلكتروني)، ومنع الوصول غير المصرح به، بما في ذلك جهات إصدار الشهادات.

3-4 يجب توفير التقنيات اللازمة لحماية مفاتيح التشفير عند تخزينها (Tamper Resistant Safe).

3-5 يجب حماية المفاتيح الخاصة (Private Key) من خلال تأمينها بكلمة مرور و/أو من خلال تخزينها على وسيط آمن، ووفقاً لإجراءات التشفير المعتمدة.

3-6 يجب تصنيف مفاتيح التشفير الخاصة باعتبارها معلومات "سرية للغاية" وفقاً لسياسة تصنيف البيانات المعتمدة في جامعة حائل.

3-7 يجب تفعيل سجلات الأحداث لحلول إدارة مفاتيح التشفير ومراقبتها دورياً.

8-3 يجب تحديد مدة لاستخدام مفاتيح التشفير وتاريخ الإنشاء وتاريخ الانتهاء لكل مفتاح.

9-3 يجب تجديد مفاتيح التشفير قبل انتهاء صلاحيتها.

10-3 يجب استخدام قائمة محدثة لشهادات التشفير الملغية (Certificate Revocation List) وذلك لضمان عدم استخدام شهادات التشفير منتهية الصلاحية أو التي تعرضت لانتهاك أمني في التعاملات مستقبلاً.

11-3 في حال تعرض مفتاح التشفير الخاص (Private Key) المُستخدم من قبل جامعة حائل إلى انتهاك أمني أو في حال عدم توفر المفتاح (بسبب تلف وسائط تخزين المفاتيح)، يجب إبلاغ الجهة المعنية بإصدار الشهادات على الفور لإلغائه وإعادة إصدار مفتاح التشفير الخاص (Private Key).

12-3 يجب إلزام الجهة المعنية بإصدار الشهادات، في حال تعرضت مفاتيح التشفير الخاصة بها (Private Keys) إلى انتهاك أمني، بإبلاغ جامعة حائل وإلغاء جميع الشهادات فوراً واستبدال المفتاح الخاص بالجهة المعنية بإصدار الشهادات.

13-3 في حال عدم إمكانية تبادل المفاتيح بشكل آمن وموثوق عبر شبكات الاتصالات، يجب نقل مفاتيح التشفير باستخدام قنوات بديلة آمنة ومستقلة (out-of-band channels).

14-3 يجب مراجعة وتحديث متطلبات طول مفاتيح التشفير بناءً على آخر التطورات التقنية ذات العلاقة مرة في السنة على الأقل وبما يتوافق مع معايير التشفير الوطنية.

15-3 مشرفو التشفير هم المسؤولون عن حماية مفاتيح التشفير (Key Custodians) وهم المصرح لهم فقط باستبدال مفاتيح التشفير عند الحاجة.

16-3 يُمنع حفظ مفاتيح التشفير على الذاكرة الرئيسية أو حفظها بنفس الأنظمة المطبق عليها التشفير. وعوضاً عن ذلك، يُوصى بحفظها على أجهزة مستقلة (Peripheral Hardware Devices)، مثل أجهزة حماية مفاتيح التشفير (Hardware Security Modules "HSM")، وأنظمة تخزين المفاتيح (Key Loaders)، أو أي أجهزة أخرى مخصصة لهذا الغرض.

4- متطلبات أخرى

1-4 يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر للاستخدام السليم والفعال للتشفير.

2-4 يجب مراجعة كافة متطلبات الأمن السيبراني الخاصة بالتشفير دورياً. (ECC-2-8-4)

3-4 تتم مراجعة هذه السياسة مرة واحدة في السنة؛ على الأقل.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة السياسة:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.

3- **تنفيذ السياسة وتطبيقها:** عمادة تقنية المعلومات والتعليم الالكتروني وإدارة الأمن السيبراني.

الالتزام بالسياسة

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذه السياسة دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

نموذج معيار إدارة حوادث وتهديدات الأمن السيبراني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السبراني

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة حوادث وتهديدات الأمن السيبراني الخاصة بـجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ١-١٣-٢ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار كافة الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل، وينطبق على جميع العاملين في جامعة حائل.

المعايير

1	خطط الاستجابة للحوادث (Incident Response Plans)
الهدف	ضمان التطبيق الملائم لمنهجية بشكل رسمي ومركز ومتناسق وتشكيل خارطة الطريق لتنفيذ عمليات الاستجابة للحوادث في جامعة حائل في حال التعرض لهجوم يستهدف البيانات الشخصية وبيانات العمل.
المخاطر المحتملة	في حال عدم وضع خطة استجابة للحوادث وتطبيقها في جامعة حائل، قد تواجه جامعة حائل المخاطر المحتملة التالية: • الإخفاق في الاستجابة بشكل مُمنهج (أي باتباع منهجية شاملة في التعامل مع الحوادث) للحوادث التي قد تؤدي إلى إتلاف المعلومات أو سرقتها أو الوصول غير المصرح به إليها أو الإفصاح عنها مما يمكن أن يؤدي إلى انقطاع الخدمات. • عدم القدرة على التعامل بكفاءة مع الحوادث التي يمكن أن تؤدي إلى مخاطر قد تؤثر على سمعة جامعة حائل. • عدم الاستفادة من المعلومات أثناء التعامل مع الحوادث من أجل التحضير بشكل أفضل للتعامل مع الحوادث المستقبلية وتوفير حماية أعلى للأنظمة والبيانات. • اتباع منهجية ضعيفة في التعامل مع القضايا القانونية التي قد تنشأ خلال الحوادث وتهديدات الأمن السيبراني.

الإجراءات المطلوبة	
1-1	تطوير خطة تلبي متطلبات الأعمال الخاصة بـجامعة حائل، وترتبط بالمهام والحجم والهيكلية والوظائف الخاصة بـجامعة حائل، وتحدد الموارد اللازمة والدعم الإداري المطلوب. A plan that meets Hail University's unique business requirements, which relates to University of Ha'il's mission, size, structure, and functions, and lays out the necessary resources and management support, shall be developed.
2-1	تتضمن خطة الاستجابة للحوادث العناصر التالية: • المهام. • الأهداف الاستراتيجية. • موافقة الإدارة العليا. • منهجية جامعة حائل للاستجابة للحوادث. • كيفية تواصل فريق الاستجابة للحوادث مع باقي الإدارات المعنية (داخلياً) والجهات الأخرى (خارجياً). • المقاييس الرئيسية لقدرات الاستجابة للحوادث وفاعليتها. • خارطة طريق لتطوير قدرات الاستجابة للحوادث. • مدى ملائمة قدرات الاستجابة للحوادث للجهة. The following elements shall be included in the incident response plan: • Mission • Strategic goals • Senior management approval • Organizational approach to incident response • How the incident response team communicates with the rest of the organization (internally) and with other organizations (externally) • Metrics for measuring the incident response capability and its effectiveness • Incident response maturity roadmap

• How the incident response capability fits into the overall large organization	
تحديد عاملين إداريين، إضافة إلى من ينوبهم عند الحاجة، لتوفير الدعم اللازم في عمليات التعامل مع الحوادث من خلال تولي الأدوار الرئيسية لاتخاذ القرارات. Management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles, shall be designated.	3-1
دراسة العوامل ذات العلاقة عند اختيار هيكلية فريق الاستجابة للحوادث في سياق احتياجات الجهة والموارد المتوفرة. ومن أمثلة هيكلية فريق الاستجابة للحوادث التالي: • الفريق المركزي للاستجابة للحوادث والذي يتألف من فريق واحد يتعامل مع الحوادث في كافة أقسام جامعة حائل. • الفرق الموزعة للاستجابة للحوادث والتي تتألف من العديد من فرق الاستجابة للحوادث، حيث يكون كل فريق منها مسؤولاً عن شريحة منطقية أو مادية معينة في جامعة حائل. All relevant factors shall be considered during the selection of an incident response team structure, in the context of the organization's needs and available resources. Examples of incident response structures are: • Central Incident Response Team (CIRT), which consists of a single team who handles incidents throughout the University of Ha'il. • Distributed Incident Response Teams (DIRT), which consist of multiple incident response teams, each responsible for a particular logical or physical segment of the University of Ha'il.	4-1
تحديد هيكلية فريق الاستجابة للحوادث الذي يجب أن يكون متوفراً لمساعدة أي فرد يكتشف أو يشتبه بوقوع حادثة لها علاقة بـجامعة حائل. The structure of the incident response team, who shall be available to provide assistance to those who discover or suspect that an incident involving University of Ha'il has occurred, shall be determined.	5-1

6-1	اختيار الأفراد الذين يملكون المهارات الفنية والخبرة والكفاءة المطلوبة للعمل في فريق الاستجابة للحوادث وتمكينه من القيام بأنشطة الاستجابة للحوادث إلى جانب الأنشطة التالية: • كشف الاختراقات: يتوقع من الفريق تحليل الحوادث بسرعة ودقة بناءً على المعرفة المكتسبة من تقنيات كشف الاختراقات. • تقديم الاستشارات: يمكن أن يقدم الفريق الاستشارات لـجامعة حائل فيما يتعلق بالثغرات والتهديدات الجديدة. وعادةً ما تكون الاستشارات مطلوبة عند ظهور تهديدات جديدة مثل الأحداث السياسية البارزة. • رفع مستوى الوعي والتوعية: أن يكون المستخدمون والعاملون الفنيون على اطلاع بكيفية كشف الحوادث والإبلاغ عنها والاستجابة لها. ويمكن تحقيق هذا من خلال وسائل مختلفة مثل ورشات العمل والمواقع الإلكترونية والنشرات الإخبارية والملصقات. • مشاركة المعلومات: يشارك فريق الاستجابة للحوادث عادة في مجموعات مشاركة المعلومات. Individuals with appropriate skills shall be selected to be members in the incident response team. Such individuals shall have the required expertise and proficiency to assist the team in performing not only incident response activities, but also: • Intrusion Detection: the team is expected to analyze incidents more quickly and accurately, based on the knowledge it gains from intrusion detection technologies. • Advisory Distribution: the team may issue advisories within the University of Ha'il regarding new vulnerabilities and threats. Advisories are often needed when new threats are emerging, such as a high-profile political event. • Education and Awareness: it is highly recommended that the users and technical staff are aware of how to detect, report, and respond to incidents. This can be achieved through many means: workshops, websites, newsletters and posters.

	• Information Sharing: incident response teams often participate in information sharing groups.
7-1	إدراج التفاصيل في التحليل الأولي عند وقوع حادثة أمنية وذلك لتحديد نطاقها. وتشمل هذه التفاصيل الشبكات أو الأنظمة أو التطبيقات المتأثرة، والمتسبب بالحادثة، وكيفية وقوعها (مثل الأدوات أو طرق الهجوم المستخدمة والثغرات المستغلة). كما يجب أخذ ما يلي بعين الاعتبار عند إجراء التحليل الأولي: • تحديد خصائص الشبكات والأنظمة التي تم قياس خصائص النشاط المتوقع فيها بحيث يكون من السهل تحديد التغييرات. • فهم السلوكيات الطبيعية. • استخدام سجل مركزي وصياغة سياسة الاحتفاظ بالسجلات. • ربط الأحداث مع بعضها البعض. • الحفاظ على تزامن ساعات المستضيف. • الحفاظ على قاعدة معرفية بالمعلومات واستخدامها. • تشغيل برامج التلصص على المعلومات لجمع معلومات إضافية. • وضع مصفوفة تشخيص للعاملين الأقل خبرة. Upon the occurrence of an incident, the incident details shall be included in the initial analysis to determine its scope. Such details shall include the affected networks, systems, or applications; who or what caused the incident; and how the incident occurred (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited, etc.). When performing an initial analysis, the following shall be considered: • Profiling of networks and systems in which the characteristics of expected activity is measured so that changes to it can be more easily identified • Understanding normal behaviors • Using a centralized logging and creating a log retention policy • Performing event correlation • Keeping all host clocks synchronized • Maintaining and using a knowledge base of information

	• Running packet sniffers to collect additional data • Creating a diagnosis matrix for less experienced staff
8-1	تحديد أولويات الأنشطة اللاحقة، مثل احتواء الحادثة والتحليل العميق لتأثيرات الحادثة، وذلك بناءً على نتائج التحليل الأولي. Subsequent activities, such as incident containment and deeper analysis of the incident impact, shall be prioritized based on the results of the initial analysis.
9-1	توثيق وتسجيل كافة الحقائق المتعلقة بالحادثة عن طريق السجل أو أجهزة الكمبيوتر المحمولة أو التسجيلات الصوتية أو الكاميرات الرقمية. All facts regarding an incident shall be documented and recorded through logbook, laptops, audio recorders or digital cameras.
10-1	توثيق وتسجيل توقيت كل خطوة تم اتخاذها من وقت اكتشاف الحادثة وحتى وقت معالجتها، وتأريخ كل وثيقة تتعلق بالحادثة والتوقيع عليها من قبل الجهة المعنية بالتعامل مع الحوادث. The time for every step taken from the minute the incident was detected to its final resolution shall be documented and recorded. Additionally, every document regarding the incident shall be dated and signed by the incident handler.
11-1	الاحتفاظ بسجلات حول حالة الحادثة باستخدام تطبيق أو قاعدة بيانات مثل نظام تتبع المشكلات، على أن تتضمن هذه السجلات ما يلي: • ملخص الحادثة. • المؤشرات المتعلقة بالحادثة (أي الدلائل التي تشير إلى وقوع الحادثة أو احتمالية وقوعها في المستقبل). • الإجراءات المتخذة من قبل جميع جهات التعامل مع الحوادث فيما يخص الحادثة. • تسلسل العهدة، إن كان مطبقاً. • تقييمات الأثر المتعلقة بالحادثة. • معلومات الاتصال بالأطراف الأخرى المعنية (مثل الجهات المسؤولة عن النظام، أو مشرفي النظام، أو الموردين). • قائمة بالأدلة التي تم جمعها خلال التحقيق في الحادثة.

	• آراء وتعليقات الجهات المعنية بالتعامل مع الحوادث. • الخطوات اللاحقة التي سيتم اتخاذها. Records regarding the status of incidents shall be maintained using an application or a database, such as an issue tracking system. Those records shall include the following: • Summary of the incident • Indicators related to the incident (i.e., a sign that an incident may have occurred or may occur) • Actions taken by all incident handlers on this incident • Chain of custody, if applicable • Impact assessments related to the incident • Contact information of relevant parties (e.g., system owners, system administrators, or vendors) • A list of evidence gathered during the incident investigation • Comments from incident handlers • Next steps to be taken
12-1	وضع معيار لعملية المراجعة المطلوبة من الإدارة العليا لتحديد إمكانية إفصاح جامعة حائل عن أي معلومات تتعلق بالحادثة الأمنية (مثل الجهة التي أبلغت عن الحادثة/المسببات والأنظمة المتأثرة) إلى أطراف خارجية (باستثناء الهيئة الوطنية للأمن السيبراني). A standard for the review process required by the upper management shall be created to determine whether or not University of Ha'il can disclose any information regarding the security incident (such as incident reporter/incident causes and affected systems) to external parties (except NCA).
13-1	حماية بيانات الحادثة وتقييد الوصول إليها إلى جانب تشفير المراسلات المتعلقة بالحادثة (مثل رسائل البريد الإلكتروني). Incident data shall be protected and access to it shall be restricted. Additionally, communications with regards to the incident (e.g., emails) shall be encrypted.

2	تصنيف الحوادث وتحديد أولوياتها (Incidents Classification and Prioritization)
الهدف	ضمان الاستجابة الفعالة والملائمة للحوادث بناءً على تقدير أثرها على الأعمال.
المخاطر المحتملة	في حالات الحوادث، يؤدي عدم تحديد الأولويات بصورة صحيحة إلى تسمية غير واضحة لحوادث أمن الشبكات وتنبيهاته ومشكلاته، مما ينتج عنه تأخير في الاستجابة للحوادث الطارئة، وعدم القدرة على تحديد الحوادث التي يمكن التعامل معها باعتبارها غير طارئة أو التنبيهات التي يمكن تجاهلها (مؤشرات سلبية خاطئة)، إلى جانب سوء تقدير نوع الاستجابة المناسب لحوادث وتنبيهات ومشكلات معينة.
الإجراءات المطلوبة	
1-2	تحديد أولويات الاستجابة لكل حادثة بناءً على تقدير أثرها على الأعمال والجهود المطلوبة للتعافي منها. ويجب أخذ العوامل التالية بعين الاعتبار عند دراسة أثر الحادثة: • الأثر الوظيفي للحادثة: تؤثر الحوادث التي تستهدف أنظمة تقنية المعلومات عادة على وظائف الأعمال التي تقدمها تلك الأنظمة، مما يؤثر سلباً على مستخدميها. يتضمن الجدول أ أمثلة على فئات الآثار الوظيفية يمكن لـجامعة حائل استخدامها لتقييم حوادثها. • الأثر المعلوماتي للحادثة: يمكن أن تؤثر الحوادث على سرية معلومات جامعة حائل وسلامتها وتوافرها. يتضمن الجدول ب أمثلة على فئات الآثار المعلوماتية المحتملة تصف مقدار الانتهاك الأمني الذي تعرضت له المعلومات خلال الحادثة. • إمكانية التعافي من الحادثة: يحدد حجم الحادثة ونوع الموارد المتأثرة بالحادثة مقدار الوقت والموارد المطلوبة للتعافي منها. يحتوي الجدول ج على فئات الجهد المطلوب للتعافي من الحوادث، وتعكس هذه الفئات مستوى الموارد المطلوبة للتعافي ونوعها. Response to each incident shall be prioritized based on the estimated business impact caused by that incident and the estimated efforts required to recover from it. The following factors shall be considered when determining the impact of an incident: • Functional Impact: incidents targeting IT systems typically impact the business functionality that those systems provide, which negatively affects the users of those systems. Table A provides examples of

	functional impact categories that an organization might use for rating its own incidents. • Information Impact: incidents may affect the confidentiality, integrity, and availability of Hail University's information. Table B provides examples of possible information impact categories that describe the extent of information compromise caused by an incident. • Recoverability: the incident scope and the type of resources it affects determine the amount of time and resources required for recovery. Table C provides recoverability effort categories that reflect the resources level and type required to recover from an incident.
2-2	تصنيف جميع الحوادث بناءً على مستوى الحدة (الجدول د). Incidents shall be classified based on severity level (Table D).
3-2	إجراء الأنشطة التالية عند محاولة تحديد المستضيف المسؤول عن هجوم الأمن السيبراني: • التحقق من عنوان بروتوكول الإنترنت للمستضيف المهاجم. • البحث عن المستضيف المهاجم عن طريق محركات البحث. • استخدام قاعدة بيانات الحوادث. • مراقبة قنوات الاتصالات المحتملة التي يستخدمها المهاجم. The following activities shall be conducted when attempting to identify an attacking host: • Validating the attacking host's IP address • Searching for the attacking host on search engines • Using incidents database • Monitoring attacker's possible communication channels

4-2	تحديد إجراء التصعيد في الحالات التي لا يستجيب فيها فريق الاستجابة للحوادث للحادثة ضمن الإطار الزمني المحدد. An escalation procedure shall be established for the instances in which the incident response team does not respond to an incident within the designated timeframe.
3	الإبلاغ عن الحوادث (Incident Reporting)
الهدف	ضمان الالتزام التام بأنظمة الهيئة الوطنية للأمن السيبراني أو بما تصدره، وتعزيز جهود جامعة حائل من خلال توفير حلقة وصل للتعامل مع الحوادث. وتقوم الهيئة الوطنية للأمن السيبراني، إضافة إلى الجهات الأخرى، بتحليل المعلومات التي تقدمها جامعة حائل لتحديد توجهات الهجمات ومؤشراتها. ويمكن تمييز هذه التوجهات بشكل أدق عند مراجعة بيانات العديد من الجهات مقارنة بمراجعة بيانات جهة واحدة.
المخاطر المحتملة	يعتبر الإخفاق في إبلاغ الهيئة الوطنية للأمن السيبراني عن الحوادث نوعاً من عدم الالتزام بالمتطلبات الرسمية التي حددتها الهيئة الوطنية للأمن السيبراني، والتي تتمحور رسالتها حول مراقبة التزام الجهات باستمرار بهدف دعم الدور الهام للأمن السيبراني. ونظراً إلى أنه يتوجب على جميع الجهات الوطنية تطبيق كافة الإجراءات اللازمة لضمان الالتزام المستمر بالضوابط الأساسية للأمن السيبراني وفقاً للبند 3 من المادة 10 من تكليف الهيئة الوطنية للأمن السيبراني، ووفقاً للأمر السامي الكريم رقم 57231 بتاريخ 1439/11/10، فإن الإخفاق في الإبلاغ عن الحوادث يمكن أن يؤدي إلى عقوبات بحق جامعة حائل.
الإجراءات المطلوبة	
1-3	تحديد جهة اتصال رئيسية واحتياطية مع الهيئة الوطنية للأمن السيبراني، والإبلاغ عن كافة الحوادث التي تتوافق مع سياسة إدارة حوادث وتهديدات الأمن السيبراني في جامعة حائل. A primary and secondary Point of Contact (PoC) with NCA shall be designated, and all incidents consistent with Hail University Incident Response Policy shall be reported.
2-3	تحديد طرق وقنوات الاتصال المطلوبة لإطلاع جامعة حائل والجهات المعنية الخارجية، مثل الهيئة الوطنية للأمن السيبراني، على آخر المستجدات. The communication methods and channels required to provide status updates to Hail University and external stakeholders, such as NCA, shall be determined.

3-3	وضع سياسة تحدد المدة الزمنية التي يجب على مشرفي النظام وأفراد فريق العمل الآخرين إبلاغ فريق الاستجابة للحوادث عن الأحداث الشاذة خلالها، وآليات الإبلاغ (بما في ذلك قنوات الإبلاغ مثل رقم الهاتف و/أو عنوان البريد الإلكتروني)، ونوع المعلومات التي يجب إدراجها عند الإبلاغ عن الحوادث. A policy which states the maximum time during which system administrators and other workforce members must report anomalous events to the incident response team shall be developed. The mechanisms for such reporting (including the reporting channels such as phone number and/or email address), and the type of information that should be included in the incident notification shall be included in the policy as well.
4-3	وضع خطط تدريبية وسيناريوهات استجابة للحوادث وتطبيقها من أجل اختبار قنوات الاتصال التي تستخدمها فرق الاستجابة للحوادث، وتقييم مهارات اتخاذ القرار لديهم إلى جانب قدراتهم الفنية وذلك بهدف زيادة الوعي والمرونة في الاستجابة للتهديدات. Routine incident response exercises and scenarios shall be planned and conducted to test the communication channels used by the incident response team, in addition to its decision-making skills and technical capabilities to increase awareness and improve agility in responding to real-world threats.
5-3	تحديد أطر زمنية معينة والالتزام بها عند إبلاغ الهيئة الوطنية للأمن السيبراني عن حوادث الأمن السيبراني. Specified timeframes shall be determined and adhered to when reporting incidents to NCA.
4	خطة التعافي من الحوادث واستمرارية الأعمال (Incident Recovery and Business Continuity Plan)
الهدف	ضمان تعافي واستعادة عمل الأنظمة بشكل طبيعي، واستعادة وظائف المستضيف المتأثر وبياناته، وإلغاء إجراءات الاحتواء المؤقت (في الحوادث المرتبطة بالبرمجيات الضارة)، وضمان توافق إجراءات وسياسات الاستجابة للحوادث وعمليات استمرارية الأعمال، مما يخدم رسالة جامعة حائل وأهدافها العامة.
المخاطر المحتملة	يمكن أن يؤدي الإخفاق في تطبيق إجراءات خطة التعافي واستمرارية الأعمال بشكل ملائم إلى تكرار الهجمات في المستقبل مما قد يضر بسمعة جامعة حائل وعلامتها

	التجارية، وعملياتها وعلاقاتها مع العملاء والموردين، بالإضافة إلى الآثار القانونية والمالية المصاحبة.
الإجراءات المطلوبة	
1-4	إصدار بلاغ باستجابة لحادثة أمنية وإسنادها إلى فريق الاستجابة للحوادث عند الإبلاغ عن حادثة أمنية. An incident response ticket shall be assigned to the incident response team the moment a security incident is reported.
2-4	القيام بالأنشطة اللازمة لاستعادة الأنظمة المتأثرة، وتشمل هذه الأنشطة على سبيل المثال لا الحصر ما يلي: • استعادة الأنظمة من النسخ الاحتياطية السليمة. • إعادة بناء الأنظمة من الصفر. • استبدال الملفات التي تعرضت لانتهاكات أمنية بنسخ سليمة. • تثبيت التحديثات والإصلاحات. • تغيير كلمات المرور وتشديد أمن محيط الشبكة (مثل مجموعة قواعد جدار الحماية، وقوائم التحكم بالوصول إلى مُوجّه الحدود). Necessary activities shall be taken to restore the affected systems. Such activities shall include, but shall not be limited to, the following: • Restoring systems from clean backups • Rebuilding systems from scratch • Replacing compromised files with clean versions • Installing patches • Changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists, etc.).
3-4	ضمان معالجة حادثة الأمن السيبراني وتصحيحها ضمن الأطر الزمنية المحددة، وفي حال عدم القدرة على ذلك، يجب على فريق الاستجابة للحوادث تصعيد الحادثة وفقاً لتصنيف الحوادث الأمنية وقواعد وإجراءات تصعيد الحوادث المعتمدة في إدارة الأمن السيبراني. Cybersecurity incidents shall be resolved and corrected within the pre-defined timeframes, otherwise, the incident

response team shall escalate the incident as per the classification of security incidents and incidents escalation rules and procedures at the Cybersecurity Department.	
تخصيص الميزانية والموارد اللازمة للتعافي من حوادث الأمن السيبراني، حيث تكون جامعة حائل هي المسؤولة عن توفير التمويل الكافي لـإدارة الأمن السيبراني، والتي تستخدمه بدورها من أجل التقليل من الأضرار والتعافي من الحوادث. The budget and resources required to recover from a cybersecurity incident shall be allocated. University of Ha'il shall be held responsible for providing sufficient fund to the Cybersecurity Department, which will in turn utilize it to minimize the damage and ultimately, recover from the incident.	4-4
في بعض الحالات، يجب أن تدرس الجهات المعنية بالتعامل مع الحوادث الجهد المطلوب للتعافي فعلياً من الحادثة، وتقارن هذا الجهد بالقيمة الناتجة عن جهود التعافي، وأي متطلبات مرتبطة بالتعامل مع الحوادث. In some cases, incident handlers shall consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.	5-4
تخزين تفاصيل حوادث الأمن السيبراني التي تقع (مثل نوع الحادثة وفئتها، والمستخدمين الذين أبلغوا عنها، والخدمات والأصول والمعلومات المتأثرة بها، وكيفية اكتشافها، وأي وثائق مساندة) وحفظها ومراجعتها دورياً. Details regarding cybersecurity incidents (e.g., incident type and category, incident reporters, affected services/assets/information, incident detection method, and any other supporting documents) shall be stored, maintained and reviewed periodically.	6-4
عقد اجتماعات لمناقشة "الدروس المستفادة" مع كافة الأطراف المعنية بعد وقوع حادثة كبيرة من أجل دراسة التهديدات الجديدة وتحسين التقنيات المستخدمة والدروس المستفادة كجزء من عملية التعافي. "Lessons learned" meetings shall be held with all relevant parties after the occurrence of a major incident to address new threats, improved technology, and lessons learned as part of the recovery process.	7-4

8-4	إطلاع مسؤولي التخطيط لاستمرارية الأعمال على طبيعة الحوادث وتأثيراتها حتى يتمكنوا من تحديد تقييمات الأثر على الأعمال وتقييمات المخاطر وخطط عمليات الاستمرارية بصورة مناسبة. Business continuity planning professionals shall be informed about the nature of the incidents and their impacts so they can fine-tune business impact assessments, risk assessments, and continuity of operations plans.
9-4	إشراك مختصي التخطيط لاستمرارية الأعمال في جامعة حائل من المراحل الأولى من عمليات اكتشاف حوادث الأمن السيبراني والاستجابة لها لتقليل انقطاع الأعمال خلال الظروف الشديدة؛ حيث من الممكن الاستفادة منهم في التخطيط للاستجابة لحالات معينة مثل هجمات تعطيل الشبكات (Denial of Service "DoS"). Business continuity planning professionals within University of Ha'il shall be engaged at the earliest stages of incident detection and response to minimize operational disruption during severe circumstances as they may provide valuable assistance in planning responses to certain situations, such as during Denial of Service (DoS) attacks.
5	الحفاظ على المعلومات الاستباقية بشأن التهديدات (Threat Intelligence Feeds Maintenance)
الهدف	ضمان اطلاع جامعة حائل على التهديدات وجوانب الاستغلال وكيفية توفير الحماية ضد هذه التهديدات بصورة ملائمة، وذلك من خلال تزويدها بمعلومات استباقية حول التهديدات، حيث تشمل هذه المعلومات بيانات منظمة وتحليلات للهجمات الأخيرة والحالية والمحتملة والتي يمكن أن تشكل تهديداً سيبرانياً لـجامعة حائل.
المخاطر المحتملة	يمكن أن يؤدي الإخفاق في اطلاع جامعة حائل على التهديدات وجوانب الاستغلال بصورة ملائمة إلى مخاطر شديدة قد تتسبب بسرقة المعلومات أو الوصول غير المصرح به لها أو الكشف عنها.
الإجراءات المطلوبة	
1-5	جمع المعلومات عن تهديدات الأمن السيبراني مثل المؤشرات (كعنوان بروتوكول الإنترنت للأوامر المشبوهة، واسم النطاق لنظام أسماء النطاقات، والعنوان "URL" الذي يرتبط بمحتوى خبيث) من مجموعة من المصادر، بما في ذلك مستودعات المصادر المفتوحة والمعلومات الاستباقية عن التهديدات التجارية والشركاء الخارجيين، وتنظيمها في قاعدة بيانات معرفية.

	Cybersecurity threat information, such as indicators (e.g., Internet Protocol "IP" address of a suspected command, a suspicious Domain Name System "DNS" domain name, a Uniform Resource Locator "URL" that references malicious content), shall be collected from a variety of sources, including open source repositories, commercial threat feeds, and external partners, and organized in a knowledge base.
2-5	تنظيم وتخزين المؤشرات في قاعدة بيانات معرفية بصيغة حرة مثل قواعد بيانات "Wikis"، وقواعد البيانات المنظمة بهدف تخزين مجموعات المؤشرات وتنظيمها وتتبعها والاستفسار عنها. وتشمل المعلومات المتوفرة في القاعدة المعرفية عموماً ما يلي: • مصدر المؤشر وتاريخ أو وقت الحصول عليه. • القواعد التي تحكم استخدام المؤشر أو مشاركته. • فترة صلاحية المؤشر. • معلومات حول ما إذا كانت الهجمات المصاحبة للمؤشر قد استهدفت جهات أو قطاعات معينة. • أي سجلات مصاحبة للمؤشر لتعداد الثغرات الشائعة (CVE)، وتعداد المنصات الشائعة (CPE)، وتعداد نقاط الضعف الشائعة (CWE)، وتعداد الإعدادات الشائعة (CCE). • المجموعات والجهات المعادية والأسماء الوهمية المصاحبة للمؤشر. • التكتيكات والأساليب والإجراءات التي تستخدمها الجهات المعادية عموماً. • دوافع الجهات المعادية أو نواياها. • الأفراد أو سمات الأفراد المستهدفين بالهجمات المصاحبة. • الأنظمة المستهدفة بالهجمات. Indicators shall be organized and stored in a knowledge base in a free form, such as wikis and structured databases, to store, organize, track, query, and analyze collections of indicators. Information which is commonly recorded in a knowledge base shall include the following: • Indicator source and indicator collection date or time • Rules governing the use or sharing of an indicator

• Indicator validity duration • Information regarding whether or not attacks associated with an indicator have targeted specific organizations or sectors • Any Common Vulnerability Enumeration (CVE), Common Platform Enumeration (CPE), Common Weakness Enumeration (CWE), Common Configuration Enumeration (CCE) records associated with an indicator • Groups, actors or aliases associated with an indicator • TTPs commonly used by an actor • Motives or intent of an associated actor • Individuals or types of individuals targeted in associated attacks • Systems targeted in attacks	
مشاركة المعلومات المتعلقة بالتهديدات ومؤشرات الانتهاك مع الهيئة الوطنية للأمن السيبراني. Threat intelligence and breach indicators shall be shared with NCA.	3-5

الجدول أ - فئات الآثار على الخدمات

Table A – Functional Impact Categories

الفئة	التعريف
لا يوجد None	لا يوجد تأثير على قدرة جامعة حائل على تقديم الخدمات لكافة المستخدمين. No effect on Hail University's ability to provide all services to all users.
منخفض Low	ما زالت جامعة حائل قادرة على تقديم كافة الخدمات الأساسية لكافة المستخدمين ولكنها تفتقد إلى الفعالية. Minimal effect; Hail University can still provide all critical services to all users but has lost efficiency.
متوسط Medium	لم تعد جامعة حائل قادرة على تقديم الخدمات الأساسية لمجموعة فرعية من المستخدمين. Hail University has lost the ability to provide critical services to a subset of system users.
مرتفع High	لا تستطيع جامعة حائل تقديم بعض الخدمات الأساسية لأي من المستخدمين. Hail University is no longer able to provide some critical services to any users.

الجدول ب - فئات الآثار على المعلومات

Table B– Informational Impact Categories

الفئة	التعريف
لا يوجد None	لم يتم تسريب المعلومات أو تغييرها أو حذفها، ولم تتعرض لأي انتهاك أمني. No information was exfiltrated, changed, deleted, or otherwise compromised
انتهاك الخصوصية Privacy Breach	الوصول إلى المعلومات القابلة لتحديد الشخصية (PII) للعاملين والمستفيدين وغيرهم أو تسريبها. Sensitive Personally Identifiable Information (PII) of employees, beneficiaries, etc. was accessed or exfiltrated.
انتهاك المعلومات المملوكة Proprietary Breach	الوصول إلى المعلومات المملوكة، مثل معلومات البنية التحتية الحساسة المحمية (PCII)، أو تسريبها. Unclassified proprietary information, such as Protected Critical Infrastructure Information (PCII), was accessed or exfiltrated.
انتهاك سلامة المعلومات Integrity Loss	تغيير المعلومات المحمية أو المملوكة أو حذفها. Sensitive or proprietary information was changed or deleted.

الجدول ج - فئات التعافي من آثار الحوادث

Table C– Recoverability Effort Categories

الفئة	التعريف
اعتيادي Regular	يمكن التنبؤ بالوقت اللازم للتعافي بالاستعانة بالموارد الحالية. Recovery time is predictable with existing resources.
تكميلي Supplemented	يمكن التنبؤ بالوقت اللازم للتعافي بالاستعانة بموارد إضافية. Recovery time is predictable with additional resources.
ممتد Extended	لا يمكن التنبؤ بالوقت اللازم للتعافي وهناك حاجة إلى موارد إضافية ومساعدة خارجية. Recovery time is unpredictable; additional resources and outside help are needed.
غير قابل للتعافي Not Recoverable	من غير الممكن التعافي من الحادثة (مثل حوادث تسرب بيانات حساسة أو نشرها)، ويجب البدء بالتحقيق فيها. Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly), and an investigation on the incident shall be conducted.

الجدول د - تصنيف الحوادث وفقاً لمستوى الحدة

Table D – Classification of Incidents Based on Severity Level

مستوى الحدة	الوصف	وقت الاستجابة المستهدف	وقت الحل المستهدف
مرتفع جداً Very High	• تهديد أو أثر مباشر على صورة جامعة حائل أو سمعتها أو مصداقيتها. • تأثر العديد من وحدات الأعمال الوظيفية بصورة كبيرة. • تأثر موقع الأعمال بصورة كبيرة. • الحاجة إلى تفعيل إجراءات استمرارية الأعمال. • Direct threat or damage to Hail University's image, reputation or credibility. • Sever impact on multiple business functional units. • Critical impact on business location. • Continuity measures may need to be invoked.	فوري	ساعتان
مرتفع High	انقطاع كبير يؤثر على وحدات الأعمال الوظيفية أو الخدمات الرئيسية أو موقع الجهة Severe outage affecting single business functional units, key services or location.	ساعة - ساعتان	5-4 ساعات
متوسط Medium	تدهور متوسط في سير عمل وحدات الأعمال الوظيفية أو المواقع أو الأصول التقنية والمعلوماتية، إضافة إلى أثر يتراوح ما بين المتوسط والمرتفع على وحدات الأعمال غير الهامة في جامعة حائل. Moderate degradation to business functional units, locations, and IT assets, in addition to moderate to high impact on non-critical business units within University of Ha'il.	3-2 ساعات	9-8 ساعات
منخفض Low	• المشكلة صغيرة وعلى نطاق بسيط. • تؤثر المشكلة على عدد قليل من الموارد. • يمكن تحمل المشكلة لفترة زمنية محددة.	5 ساعات	24 ساعة

مستوى الحدة	الوصف	وقت الاستجابة المستهدف	وقت الحل المستهدف
	• Small issue with a localized scope. • Few resources are affected by the issue. • Issue can be tolerated for a particular period of time.		

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني.

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الالكتروني.

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذا المعيار باستمرار.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

نموذج معيار اختبار الاختراق

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لاختبار وتقييم مدى فعالية قدرات تعزيز الأمن السيبراني في جامعة حائل وذلك من خلال محاكاة تقنيات الهجوم السيبراني وأساليبه الفعلية، واكتشاف نقاط الضعف الأمنية غير المعروفة التي قد تؤدي إلى الاختراق السيبراني لـجامعة حائل من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

يهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-١١-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع أنظمة جامعة حائل الحساسة ومكوناتها التقنية، وجميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) ومكوناتها التقنية والتي تشمل البنية التحتية، والمواقع الإلكترونية، وتطبيقات الويب، وتطبيقات الهواتف الذكية واللوحية، والبريد الإلكتروني، والدخول عن بعد، وتنطبق هذه السياسة على جميع العاملين في جامعة حائل.

المعايير

1	المتطلبات العامة
الهدف	تحديد المتطلبات العامة لاختبار الاختراق (Penetration Testing) التي يجب أن يتبعها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.
المخاطر المحتملة	يمكن أن يؤدي اختبار الاختراق غير المخطط له بشكل صحيح إلى مخرجات غير كافية أو غير دقيقة، أو قد يؤثر على كفاءة الأنظمة.
الإجراءات المطلوبة	
1-1	يجب تطوير خطة لاختبار الاختراق يوضح فيها نطاق العمل وتاريخ البدء والانتهاء وآلية وسيناريوهات تنفيذ عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية. A plan for penetration testing that covers in-scope systems and applications, start date, end date, methodology, and real-world attack scenarios shall be developed.
2-1	يجب التأكد من أن خطة العمل لاختبار الاختراق متوافقة مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

	Penetration testing action plan shall be designed based on the relevant legislative and regulatory requirements.
3-1	يجب التأكد من أن اختبار الاختراق يسير وفقاً لمنهجية محددة ووفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة. Penetration testing shall follow a defined methodology, conducted as per the relevant legislative and regulatory requirements
4-1	يجب صياغة وثيقة قواعد التنفيذ قبل البدء بالاختبار والتي تغطي نطاق الاختبار ومدته والأنظمة المستهدفة والبنود والشروط. Rules of engagement document shall be developed prior to the test, and it shall cover test scope, duration, target systems, and terms and conditions.
5-1	يجب إعداد تقرير لنتائج اختبار الاختراق يوضح تأثير المخاطر وآلية معالجتها والمسؤول عن تطبيقها والفترة الزمنية اللازمة لتنفيذها، على أن يتضمن التقرير الأقسام التالية على الأقل: • الملخص التنفيذي. • مقدمة لإعداد التقارير. • المنهجية المتبعة في تصنيف الثغرات. • الأصول المستهدفة، وسيناريوهات الهجمات (Attack Scenarios). • تقرير تفصيلي لنتائج اختبار الاختراق. A report shall be developed after finalizing the penetration testing activity. The report shall include the following sections at minimum: • Executive Summary • Reporting Introduction • Approach and Methodology • Target Assets and Attack Scenarios • Detailed Findings
6-1	بعد الانتهاء من تقرير اختبار الاختراق، يجب إعداد خطة عمل لتنفيذ التوصيات، على أن يتضمن التقرير ما يلي على الأقل:

	• المسؤول التقني عن الأصل (Technical Owner). • مالك الأصل (Business Owner). • الإجراءات المطلوبة لتنفيذ التوصيات. • الفترة الزمنية اللازمة لتنفيذ التوصيات. An action plan shall be developed after finalizing the penetration testing report in order to implement the recommendations. The report shall include the following at minimum: • Technical Owner • Business Owner • Required Actions • Clear Deadlines
7-1	يجب التأكد من أن تقنيات المستخدمين وأدواتهم وحساباتهم، وكذلك الأجهزة المستخدمة في اختبار الاختراق أو كانت جزءاً منه، خاضعة للتحكم والمراقبة وذلك لضمان استخدامها لغرض اختبار الاختراق فقط. Any user, system or workstation that was used in, or was part of, the penetration testing exercise shall be controlled and monitored to ensure that they are used only for the purpose of the testing exercise.
8-1	يجب تعطيل أو إزالة التقنيات والأدوات وحسابات المستخدمين بعد الانتهاء من عملية اختبار الاختراق. Any user, system or workstation that was used in, or was part of, the penetration testing exercise shall be removed or restored to normal behavior and access after the testing exercise.
9-1	يجب إعداد تقرير لكل اختبار اختراق غير ناجح أو غير مكتمل توضح فيه الصعوبات التي واجهت فريق الاختبار لدراسة العوائق وحلها وإعادة الاختبار مرة أخرى. A report shall be developed for each failed or incomplete penetration testing exercise. The report shall highlight the limitations faced by the test team to understand and resolve them, and redo the exercise.

2	آلية اختبار الاختراق
الهدف	تحديد آلية اختبار الاختراق والأدوات والتقنيات المستخدمة التي يجب أن يتبعها فريق اختبار الاختراق الداخلي أو الخارجي قبل بدء عملية اختبار الاختراق.
المخاطر المحتملة	يمكن أن يؤدي اختبار الاختراق غير المدروس إلى حصول ثغرات جديدة أو وصول غير مصرح به أو استمرار وجود نقاط ضعف أمنية في البيئة لا يتم اكتشافها مما يؤدي إلى نتائج غير دقيقة، كما يمكن أن يؤدي إلى تسرب البيانات أو كشفها أو إلحاق الضرر بالأنظمة والخدمات والمكونات التقنية.
الإجراءات المطلوبة	
1-2	يجب إجراء اختبار الاختراق دورياً. (ECC-2-11-3-2) Penetration testing shall be performed periodically.
2-2	يجب إجراء اختبار الاختراق لجميع الخدمات المقدمة خارجياً ومكوناتها التقنية دورياً وحسب جدول محدد ووفقاً لمنهجية وإجراءات محددة. (ECC-2-11-3-1) Penetration testing shall be conducted for all Internet-facing systems on a scheduled and regular basis, and following defined methodology and procedures. (ECC-2-11-3-1)
3-2	يجب إجراء اختبار الاختراق لجميع الأنظمة الحساسة ومكوناتها التقنية بانتظام وبحسب جدول محدد (كل 6 أشهر) ووفقاً لمنهجية وإجراءات محددة. (CSCC-2-10-1-1) Penetration testing shall be conducted for all critical systems on a scheduled and regular basis (every 6 months), and shall follow defined methodology and procedures. (CSCC-2-10-1-1)
4-2	يجب التأكد من تنفيذ اختبار الاختراق وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، مع الأخذ بالاعتبار الإرشادات التالية: 2-4-1 توفير المتطلبات الخاصة ببدء اختبار الاختراق الواردة في إجراءات اختبار الاختراق. 2-4-2 تحديد آلية الاختبار والتي تتضمن اختبار الصندوق الأسود (اختبار اختراق دون توفير معلومات للجهة التي تجري الاختبار)، واختبار الصندوق الأبيض (اختبار اختراق مع توفير جميع المعلومات للجهة التي تجري الاختبار)، واختبار الصندوق الرمادي (اختبار اختراق مع توفير بعض المعلومات للجهة التي تجري الاختبار). 2-4-3 تحديد الأنظمة أو الخدمات أو المكونات التقنية المستهدفة بالاختبار وأي معلومات أو صلاحيات يجب توفيرها قبل بدء اختبار الاختراق.

4-4-2 الاطلاع على تقارير اختبارات الاختراق السابقة والمستندات المساعدة (إن وجدت) مثل مخططات الشبكة والمعايير التقنية الأمنية واستخدامها كمدخلات لعملية اختبار الاختراق لفهم طبيعة الأعمال للنظام أو التطبيق أو المكون التقني. 5-4-2 التأكد من عمل محاكاة لتقنيات الهجوم السيبراني وأساليبه الفعلية خلال عملية اختبار الاختراق تشمل بحد أدنى ما يلي: • الهندسة الاجتماعية. • اختبار الاختراق على مستوى الشبكة. • اختبار الاختراق على مستوى التطبيق. • اختبار الاختراق للشبكة اللاسلكية. • الدخول غير المصرح به. 6-4-2 إنشاء منصة أو بيئة تحاكي الأنظمة أو الخدمات المستهدفة باختبار الاختراق لعمل الاختبار عليها بدلاً من الأنظمة والخدمات الإنتاجية (أي الحقيقية). 7-4-2 توثيق النتائج لكل خطوة من خطوات اختبار الاختراق.	
Penetration testing exercise shall be conducted as per the relevant legislative and regulatory requirements and shall take into account the following guidelines: 2-4-1 The exercise shall meet specific penetration testing requirements, which are mentioned in the procedures. 2-4-2 The exercise shall define the testing approach (whether black box, white box, or grey box). 2-4-3 The systems/applications, services, or technical components targeted for testing shall be identified, as well as any system/application specific information, requirements or permissions targeted for testing. 2-4-4 Previous testing reports and supporting documents such as network diagrams and Technical Security Standards shall be reviewed and utilized as inputs for the testing exercise to understand how a system, application or technical component functions. 2-4-5 Simulation of real-world attack scenarios shall be conducted in the penetration testing and it shall include, at minimum, the following:	

• Social Engineering • Network Level Penetration Testing • Application Level Penetration Testing • Wireless Penetration Testing • Unauthorized Access 2-4-6 A test bed or an environment that mimics critical systems or production environment shall be created. 2-4-7 Results shall be documented for each step in the testing exercise.	

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الالكتروني و إدارة الأمن السيبراني

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذا المعيار دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذا المعيار.

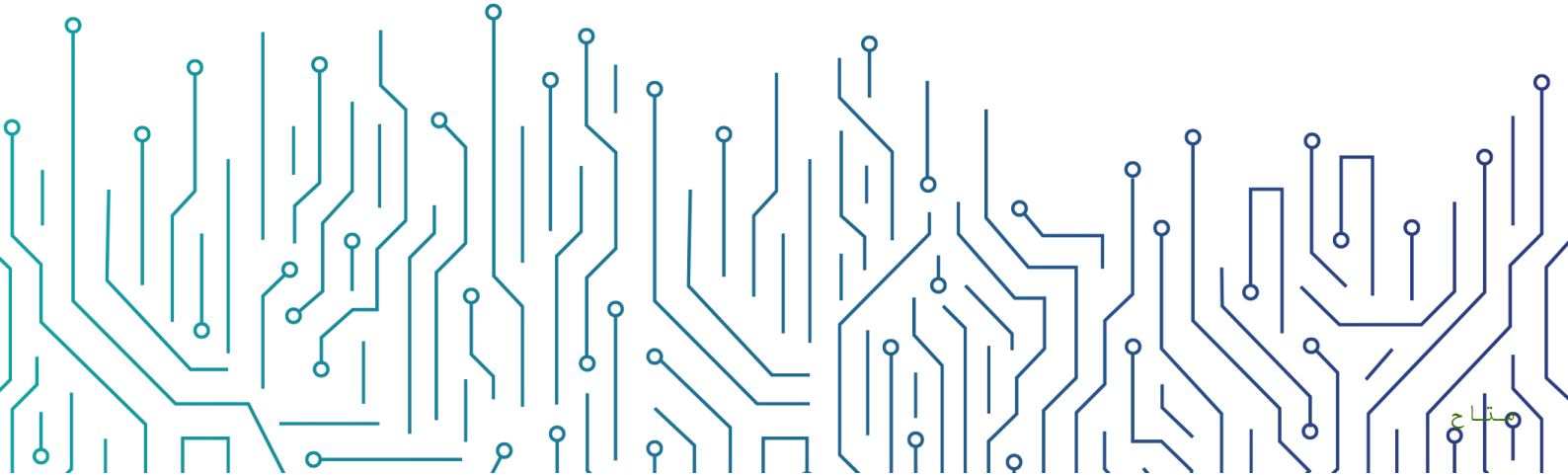
3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

نموذج معيار أمن الخوادم

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني



متاح

قائمة المحتويات

الأهداف

الغرض من هذا المعيار هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بإدارة الخوادم الخاصة بـجامعة حائل لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

ويهدف هذا المعيار إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهو مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

يغطي هذا المعيار جميع الخوادم الخاصة بـجامعة حائل، وينطبق على جميع العاملين في جامعة حائل.

المعايير

1	الوصول الآمن (Secure Access)
الهدف	ضمان حماية الخوادم ووظائفها من الوصول غير المصرح به.
المخاطر المحتملة	ينطوي الوصول غير المصرّح به إلى الخوادم على مخاطر عالية قد تؤدي إلى تسريب البيانات أو سرقتها أو تعطيل الخدمات أو انتهاكات أمنية تسمح لمنفذيها باستخدامها لشن المزيد من الهجمات السيبرانية ضد جامعة حائل وبنيتها التحتية.
الضوابط	
1-1	استخدام مبدأ الحماية الذي يمنح مشرفي ومُشغّلي الخوادم الحد الأدنى من صلاحيات الوصول إلى مختلف أنواع أنظمة البريد الإلكتروني. Least-privilege security principle shall be used to provide access to different types of email systems to server administrators and operators.
2-1	حصر الوصول إلى الخوادم على مشرفي الخوادم فقط وذلك من خلال منح حق الوصول لحسابات المشرفين المختلفين وبروتوكول الإنترنت لأجهزة المستخدمين باستخدام قوائم التحكم بالوصول (ACLs). Access on servers shall be restricted to server administrators by only allowing access to administrators' individual accounts

and workstation IPs using network Access Control Lists (ACLs).	
إيقاف أو تغيير الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة. Default/non-interactive/unneeded accounts shall be disabled or renamed.	3-1
إلى جانب ضرورة إدخال اسم المستخدم وكلمة المرور، إلزام المستخدم باستعمال آليات أخرى للتحقّق من الهوية مثل السمات الحيوية، والمفاتيح المادية، وكلمات المرور المؤقتة، والبطاقات الذكية، وشهادات التشفير، وغيرها. In addition to a user/password combination, users shall be required to use other authentication mechanisms such as biometrics, hardware keys, one-time passwords, smart cards, certificates, etc.	4-1
إعداد متطلبات تعقيد كلمة المرور الخاصة بالخادم وفقاً لسياسة إدارة هويات الدخول والصلاحيات في جامعة حائل. Server password complexity requirements shall be configured in accordance with Hail university's Identity and Access Management Policy.	5-1
تطبيق تقنيات التشفير مثل «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية آليات التحقّق من الهوية أثناء إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) المُوصى بها. للمزيد من التفاصيل، يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة حائل. Encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), shall be implemented to protect authentication mechanisms during transmission. In addition, recommended next generation encryption protocols and cipher suites shall be used. For more details, refer to Hail university's Cryptography Standard.	6-1
تطبيق نظام إدارة الصلاحيات الهامة والحسّاسة (PAM) لمنح حق الوصول المؤقت إلى الخوادم القائم على نوع الجلسة المطلوبة.	7-1

	A Privilege Access Management (PAM) system shall be implemented to enforce session-based temporary access to servers based on request.
8-1	ضبط وإعداد وقت انتهاء الجلسة وحد إغلاق الجلسة عند عدم الاستخدام وفقاً لسياسات الأمن السيبراني في جامعة حائل. Session timeout and session idle lockout shall be configured in accordance with Hail university's cybersecurity polices.
9-1	ضبط وإعداد كلمات مرور مُحمِّل تشغيل (Bootloader) نظام الإدخال/الإخراج الأساسي (BIOS). BIOS bootloader passwords shall be configured.
10-1	إلزام مشرفي ومُشغّلي الخوادم باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى الخوادم الحساسة. Server administrators and operators shall be required to use multi-factor authentication to access critical servers.
11-1	تقييد وصول المشرفين والمشغلين إلى الخوادم الحساسة وحصره على أجهزة الحاسب ذات الصلاحيات والامتيازات الهامة والحساسة (PAWs). Access to critical servers shall be restricted by administrators and operators to be provided through Privileged Access Workstations (PAW) only.
12-1	تقييد الوصول إلى الخوادم وحصره على المشرفين والمشغلين وذلك عن طريق خوادم الوصول إلى المناطق الآمنة (Jump Servers) أو إدارة الصلاحيات الهامة والحسّاسة (PAM). 1-12-1 استخدام خوادم منفصلة للوصول إلى المناطق الآمنة (Jump Servers) لمشرفي ومستخدمي النظام. 2-12-1 استخدام التحقّق من الهوية متعدّد العناصر من أجل الوصول عبر خوادم الوصول إلى المناطق الآمنة (Jump Server) المستخدمة من قبل مشرفي النظام وذلك من خلال تطبيق قوائم التحكم بالوصول (ACLs). 3-12-1 تقييد الوصول إلى خوادم الوصول إلى المناطق الآمنة (Jump Servers) وحصره على المشرفين والمشغلين المصرح لهم فقط. 4-12-1 تقييد الوصول إلى الشبكة وحصره على خوادم الوصول إلى المناطق الآمنة (Jump Servers) من خلال تطبيق قوائم التحكم بالوصول (ACLs).

	5-12-1 وضع خوادم الوصول إلى المناطق الآمنة (Jump Servers) في منطقة إدارة الشبكة. 6-12-1 إلغاء تفعيل خاصية الوصول إلى الإنترنت على خوادم الوصول إلى المناطق الآمنة (Jump Servers). 7-12-1 إلغاء تفعيل الخدمات الخطرة وغير اللازمة (مثل إرسال رسائل البريد الإلكتروني واستلامها) على خوادم الوصول إلى المناطق الآمنة (Jump Servers). 8-12-1 تفعيل جميع مستويات التسجيل إضافةً إلى سجل التدقيق والسجلات الأمنية محلياً وعلى نظام تسجيل أحداث مركزي. Access to servers shall be restricted by administrators and operators and shall only be provided through a jump server or PAM. 1-12-1 A separate jump server shall be used for system administrators and users. 1-12-2 The use of multi-factor authentication shall be required for the access of jump servers used by system administrators by implementing ACLs. 1-12-3 Access to jump servers shall be restricted to the accounts of authorized administrators and operators only. 1-12-4 Network access shall be restricted to jump servers by implementing ACLs. 1-12-5 Jump servers shall be placed in the network management zone. 1-12-6 Internet access on jump servers shall be disabled. 1-12-7 Unnecessary and risky services (such as sending and receiving emails) shall be disabled on jump servers. 1-12-8 All levels of logging, as well as audit trail and security logs, shall be enabled locally and to a centralized event logging system.
2	مراجعة الإعدادات والتحصين (Secure Hardening Configuration)
الهدف	تحديد متطلبات الأمن الأساسية للخوادم لضمان تصميم الخوادم وإعدادها وتشغيلها بطريقة آمنة.

المخاطر المحتملة	يعتبر الإعداد الخاطئ للخوادم والتصميم الضعيف من الثغرات الأمنية الشائعة التي يمكن استغلالها لتهديد سرية وسلامة وتوافر بيانات جامعة حائل وسير عملها.
الضوابط	
1-2	إجراء اختبارات أمنية دورية (مثل تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في جامعة حائل. Regular security testing (such as vulnerability assessments and penetration testing) shall be performed in accordance with Hail university's Vulnerability Management Policy.
2-2	إجراء التحديثات والإصلاحات على الخوادم بانتظام وفقاً لسياسة إدارة التحديثات والإصلاحات في جامعة حائل لضمان تحديث جميع أنظمة التشغيل وبرمجيات التطبيقات على الخوادم. Servers shall be regularly patched and updated in accordance with Hail university's Patch Management Policy to ensure that all servers' OSs and application software are up-to-date.
3-2	حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من الخوادم مثل خدمات الطباعة، وبروتوكول تل نت (telnet)، وغيره. Unnecessary/unrequired applications and services on servers, such as printing services, telnet, etc., shall be removed or disabled.
4-2	استخدام مبدأ الحماية الذي يمنح مشرفي ومُشغّلي الخوادم الحد الأدنى من صلاحيات الوصول إلى مختلف أنواع الأنظمة. Least-privilege security principle shall be used to provide access to different types of systems to server administrators and operators.
5-2	حصر الوصول إلى الشبكة بمناطق الخوادم ومناطق إدارة الخوادم. Network access shall be restricted to server zones and server management zones.
6-2	حذف أو إلغاء تفعيل خصائص نظام التشغيل والتطبيق وملفات الإعدادات غير الضرورية أو غير اللازمة.

Unnecessary/unrequired OS and application features and configuration files shall be removed/disabled.	
حجب إمكانية الوصول إلى مجلدات الشبكة والملفات غير الضرورية أو غير اللازمة. Access to unnecessary/unrequired network and file directories shall be blocked	7-2
استخدام ضوابط الأجهزة وحجب الوصول إلى وسائط التخزين القابلة للإزالة. Hardware controls shall be used and access to removable media shall be blocked.	8-2
إنشاء البنية التحتية للخوادم تبعاً لبنية متعدّدة الطبقات محمية باستخدام جدران حماية ذات طبقة مزدوجة. وإدراج خادم ويب في منطقة الإنترنت المحايدة، وخوادم التطبيقات في منطقة الإنتاج، وخوادم قواعد البيانات في المنطقة الموثوقة أو منطقة قاعدة البيانات. Server's infrastructure shall be implemented following N-tier architecture protected by a dual layer of firewalls. Specifically, webservers shall be placed in the Internet DMZ, Application Servers shall be placed in the Production Zone, and Database Servers shall be placed in the Trusted/Database zone.	9-2
العزل المادي أو المنطقي لخوادم الأنظمة الحساسة عن الخوادم أو الأنظمة الأخرى. فعلى سبيل المثال، يمكن تحقيق العزل المادي من خلال استضافة الخوادم في بيئة مادية منفصلة ومختلفة تماماً، ويمكن تحقيق العزل المنطقي من خلال تطبيق الخوادم في مناطق منفصلة داخل الشبكة دون السماح بالوصول إليها من أي منطقة أخرى. Critical system servers shall be logically and physically isolated from other servers or systems. For example, physical isolation can be achieved by hosting the servers in a completely different separate physical environment, while logical isolation is achieved by implementing servers in a separate zone inside the network without allowing access from any other zone.	10-2
ضبط إعدادات وتحصين الخوادم بما في ذلك التحصين على مستوى التطبيقات وقاعدة البيانات ونظام التشغيل. Server configuration hardening shall be configured, including application, database, and operating system level hardening.	11-2
إنشاء نسخ أو قوالب آمنة لكافة الخوادم بناءً على معايير الإعدادات المعتمدة، وإعادة نسخ الخوادم باستخدام أحد قوالب نسخ الخوادم في حال تعرضها لانتهاك أمني.	12-2

Secure server images or templates shall be created for all servers based on the approved configuration standards. Any server or system that becomes compromised shall be reimaged using one of these server image templates.	
تخزين نسخ الخوادم في بيئة آمنة على خوادم معدة بصورة آمنة والتحقق بانتظام من هذه النسخ باستخدام أدوات مراقبة سلامة المعلومات. Server images shall be stored in a secure environment on securely configured servers and shall be regularly validated using integrity monitoring tools.	13-2
تطبيق الفصل المنطقي أو المادي للخوادم بين بيئات الإنتاج والتطوير والاختبار. Logical or physical segregation for servers among production, development and testing environments shall be implemented.	14-2
النسخ الاحتياطي والأرشفة (Backup and Archiving)	3
ضمان سلامة بيانات الخوادم وتوافرها وقابلية استعادتها والتأكد من عدم العبث بها أو فقدانها بالخطأ أو تخريبها.	الهدف
في حال حذف بيانات الخوادم أو فقدانها بالخطأ أو العبث بها أو تخريبها أو تعرّضها إلى هجوم إلكتروني، لن تتمكّن جامعة حائل من استرداد البيانات مما سيؤثّر على أنشطة أعمالها الاعتيادية.	المخاطر المحتملة
الضوابط	
عمل نسخة احتياطية كاملة للخوادم وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة حائل. يجب أن تشمل النسخ الاحتياطية على الأقل نسخاً احتياطية لنظام تشغيل الخوادم، ونسخاً احتياطية لإعدادات التطبيقات، ونسخاً احتياطية لإعدادات قواعد البيانات، وقواعد البيانات والمعلومات المخزنة. Full backup for server shall be performed in accordance with Hail university's Backup and Recovery Management Policy. Backups must include, at minimum, servers operating system backup, applications configuration backup, database configuration backup, and stored databases and information.	1-3
تشفير النسخ الاحتياطية للخوادم في جامعة حائل. Hail university's server backups shall be encrypted.	2-3

3-3	إضافة ترتيب تسلسلي للنسخ الاحتياطية عن الخوادم الخاصة بجامعة حائل وتسجيل وقتها وتاريخها وجدولتها. Hail university's server backups shall be serialized, time-dated and indexed.
4-3	تخزين النسخ الاحتياطية عن الخوادم الخاصة بـجامعة حائل في موقعين خارجيين محميّين منفصلين على الأقل. Hail university's server backups shall be stored in at least two geographically distinct protected off-sites.
5-3	اختبار إمكانية استرجاع النسخة الاحتياطية كل ثلاثة أشهر وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة حائل. Backup recovery shall be regularly tested every quarter or in accordance with Hail university's Backup and Recovery Management Policy.
6-3	تطبيق آليات توثيق النسخ الاحتياطية وسلامتها لضمان نسخ بيانات أجهزة المستخدمين أو أرشفتها بطريقة صحيحة. Backup verification and integrity mechanisms shall be implemented to ensure that data is being correctly backed up or archived.
7-3	أرشفة النسخ الاحتياطية لخوادم جامعة حائل في موقع تخزين غير مرتبط بالشبكة طوال فترة التخزين المعتمدة وفقاً لسياسة إدارة النسخ الاحتياطية في جامعة حائل. University of Ha'il's server backups shall be archived in an offsite storage location for the entire approved retention period and as per Hail university's Backup and Recovery Management Policy.
4	حماية الخوادم (Server Protection)
الهدف	ضمان حماية الخوادم من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقاً وأي نوع آخر من الهجمات الخبيثة.
المخاطر المحتملة	يمكن أن تؤدي الهجمات الخبيثة الناجحة على الخوادم إلى تعريض جامعة حائل لاختراق أمني أو وصول غير مصرح به أو الكشف عن البيانات في حال تركت الخوادم دون حماية.

الضوابط	
1-4	ضبط وإعداد حد إغلاق نظام التشغيل ووظائف التطبيقات عن طريق الحد الأدنى من الصلاحيات والامتيازات المطلوب للتشغيل في الظروف الاعتيادية، مثل إلغاء تفعيل تغيير وقت النظام يدوياً، والإغلاق/إعادة التشغيل، وتعديل ملفات النظام، وإنشاء/تعديل/حذف الملفات، وغيرها. OS and application functionality lockout shall be configured with the least privilege required to operate in normal conditions. For example, changing system time manually, shutting down/restarting, editing system files, creating/modifying/deleting files, etc., shall be disabled.
2-4	تطبيق خاصية السماح بقائمة محددة من التطبيقات على الخوادم لتمكين عمل تطبيقات وبرمجيات محددة فقط وفقاً للحاجة. Application whitelisting shall be enabled on servers to allow only specific applications and software to run based on need.
3-4	إعداد أنظمة السماح بقائمة محددة من التطبيقات بحيث لا يمكن للمستخدمين إلغاء تفعيل الأنظمة باستثناء مديري النظام عند أدائهم لمهام إدارية معينة تقتضي إلغاء تفعيل السماح بقائمة محددة من التطبيقات مؤقتاً. Application whitelisting agents shall be configured so that users cannot disable the agents with the exception of administrators when performing specific administrative tasks that would require disabling application whitelisting temporarily.
4-4	تعريف الملفات التنفيذية المعتمدة (exe, com, pif, وغيرها) ومكتبات البرمجيات (dll, ocx, وغيرها) والنصوص (ps1, bat, vbs, وغيرها) وبرامج التثبيت (msi, msp, وغيرها). A list of approved executables (exe, com, pif, etc.), software libraries (dll, ocx, etc.), scripts (ps1, bat, vbs, etc.), and installers (msi, msp, etc.) shall be defined.
5-4	تطبيق خاصية السماح بقائمة محددة من التطبيقات لاستخدام قواعد التجزئة المشفرة أو قواعد شهادات الناشر أو قواعد المسار للسماح باستخدام التطبيقات أو منعها.

Application whitelisting shall be implemented to use cryptographic hash rules, publisher certificate rules or path rules to allow or restrict the use of applications.	
ضبط وإعداد مجلدات التطبيقات وفقاً لتصاريح نظام الملفات لمنع أي تعديل غير مصرح به على المجلد أو تصاريح الملفات. Application folders shall be configured with file system permissions to prevent unauthorized modification of folder and file permissions.	6-4
تمكين وظيفة الحماية على الخوادم لاستخدامها في إجراءات الحد من المخاطر على نظام التشغيل وإجراءات الحد من المخاطر لتطبيقات معينة. Exploit protection functionality shall be enabled on servers with both operating system mitigation measures and application-specific mitigation measures.	7-4
تطبيق نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Prevention System "HIPS") على جميع الخوادم. Host-based Intrusion Prevention System (HIPS) shall be implemented on all servers.	8-4
تطبيق جدار حماية من البرمجيات المستضافة على جميع الخوادم. Software host firewall shall be implemented on all servers.	9-4
تطبيق برامج مكافحة الفيروسات على جميع الخوادم. Antivirus shall be implemented on all servers.	10-4
تطبيق حماية النهاية الطرفية (Endpoint Protection) على جميع الخوادم. Endpoint protection shall be implemented on all servers.	11-4
تطبيق برامج الحماية من التهديدات المتقدمة المستمرة (APT) على جميع الخوادم. Advanced Persistent Threat agents shall be implemented on all servers.	12-4
تطبيق برمجيات التحكم بأجهزة النهاية الطرفية على كافة الخوادم لمنع الاستخدام غير المصرح به للأجهزة.	13-4

	Endpoint device control software shall be implemented on all servers to prevent the use of unauthorized devices.
14-4	تطبيق منع تسّرب البيانات (DLP) عند الضرورة. Data Leakage Prevention (DLP) shall be implemented where required.
15-4	تطبيق جميع المتطلبات بموجب سياسة الحماية من البرمجيات الضارة المعتمدة في جامعة حائل. All requirements under Hail university's Malware Protection Policy shall be implemented.
5	تسجيل الأحداث وسجل التدقيق (Event and Audit Logging)
الهدف	ضمان الحفاظ على سريّة بيانات الخوادم والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.
المخاطر المحتملة	إمكانية التأكّد من سلامة البيانات وموثوقيتها على الخوادم لحماية جامعة حائل من الهجمات الخبيثة والكشف عن المعلومات المهمّة والحسّاسة والوصول غير المصرّح به.
الضوابط	
1-5	ضبط وإعداد سجل الخوادم وسجل التدقيق ليتم ترحيلها إلى نظام تسجيل مركزي وفقاً لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني في جامعة حائل. Server logging and audit trail shall be configured to be forwarded to a centralized logging system as per Hail university's Cybersecurity Event Logs and Monitoring Management Policy and Standard.
2-5	إعداد الخوادم ليتزامن وقتها مع ثلاثة خوادم زمنية إضافية على الأقل في غضون أجزاء من الثانية بطريقة ممكنة تقنياً مما يسمح باتساق الأختام الزمنية في السجلات. Servers shall be configured to synchronize time to at least three redundant central time servers within milliseconds where technically possible so that timestamps in logs are consistent.
3-5	ضبط إعدادات الخوادم ذات الخطورة العالية التي تعتمد عادةً على التسجيل المركزي لحفظ سجلات أنظمة التشغيل في حال تعطّل اتصال الشبكة.

	High risk servers that normally rely on centralized logging shall be configured to maintain local logs in the event that network connectivity fails.
6	التشفير (Cryptography)
الهدف	ضمان الحفاظ على سريّة بيانات الخوادم والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة.
المخاطر المحتملة	إمكانية التأكّد من سلامة البيانات وموثوقيتها على الخوادم لحماية جامعة حائل من الهجمات الخبيثة والكشف عن المعلومات المهمّة والحسّاسة والوصول غير المصرّح به.
الضوابط	
1-6	تطبيق تقنيات التشفير مثل «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية آليات التحقّق من الهوية أثناء إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) المُوصى بها. لمزيد من التفاصيل، يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة حائل. Encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), shall be implemented to protect authentication mechanisms during transmission. In addition, recommended next generation encryption protocols and cipher suites shall be used. For more details, refer to Hail university's Cryptography Standard.
2-6	تشفير وسائط التخزين في الخوادم بما في ذلك الأقراص الصلبة، ووسائط التخزين الملحقة بالشبكة (NAS)، ووسائط التخزين المتصلة بشبكة التخزين (SAN)، أو أي نوع آخر من وسائط التخزين المتصلة. Servers storage media shall be configured, including hard disks, Network Attached Storage (NAS), Storage Area Network (SAN) connected storage, or any other type of connected storage.
3-6	استخدام بروتوكول إدارة الخوادم الذي يدعم التشفير أو يقوم بضبط إعدادات التشفير لبروتوكولات إدارة الخوادم، مثل بروتوكول النفاذ إلى الدليل البسيط (LDAP) على أمن طبقة النقل (TLS)، والنسخة الثالثة من بروتوكول إدارة الشبكة البسيط (SNMPv3) لغايات المصادقة والخصوصية، وبروتوكول كيربيروس (Kerberos) مع أمن طبقة النقل (TLS)، وسجل النظام المشفر، وغيرها.

	Server management protocol that supports encryption or configures encryption for server management protocols, such as LDAP over TLS, SNMPv3 with authentication and privacy, Kerberos with TLS, encrypted syslog, etc., shall be used.
4-6	إعداد التشفير لتطبيقات الخوادم وبروتوكولات الاتصال بقواعد البيانات، مثل بروتوكول نقل النص التشعبي الآمن (HTTPS)، وواجهة برمجة التطبيقات الآمنة (API)، وتشفير البيانات الشفاف (TDE)، أو برنامج (SQL) على أمن طبقة النقل (TLS)، وبروتوكول نقل الملفات الآمن (SFTP)، وبروتوكول النقل الآمن (SSHv2)، وغيرها. Encryption for server application and database communication protocols, such as HTTPS, Secure API, TDE or SQL with TLS, SFTP, SSHv2, etc., shall be configured.
7	أمن البيئة الافتراضية (Virtual Security)
الهدف	تحديد المتطلبات الهامة للخوادم الموجودة في البيئة الافتراضية لضمان تصميم الخوادم الافتراضية وإعدادها وتشغيلها بطريقة آمنة.
المخاطر المحتملة	يعتبر الإعداد الخاطئ والتصميم الضعيف للبيئة الافتراضية والافتقار إلى الأنظمة الافتراضية الآمنة من الثغرات الأمنية التي يمكن استغلالها لتهديد سرية وسلامة وتوافر بيانات جامعة حائل وسير عملها.
الضوابط	
1-7	إعداد وضبط الحدود لكافة أشكال استخدام مصادر البيئة الافتراضية الموجودة على الخوادم. Limits for all server VM resources use shall be configured.
2-7	تطبيق حل إعدادات الخوادم الافتراضية مركزي. A centralized server VM configuration solution shall be implemented.
3-7	فصل الأجهزة الطرفية غير المستخدمة في بيئة الأنظمة الافتراضية لكافة الخوادم. Unused peripheral devices in the virtualization environment shall be disconnected for all servers.
4-7	تطبيق وإعداد جدار الحماية وخصائص منع التسلل والاختراق للحركة بين الخوادم الافتراضية حتى لو كانت موجودة في نفس الخادم أو المستضيف المادي (الحركة بين الخوادم "East-West traffic").

Firewalling and intrusion inspection and prevention features shall be implemented and configured for traffic between virtual servers even within the same physical server or host (East-West traffic).	
إعداد شبكات محلية افتراضية (VLANs) للاتصال بين الخادم المستضيف والخادم الضيف بصورة تختلف عن الاتصالات بين الخوادم الافتراضية. Separate VLANs for communication between host and guest server VMs shall be configured to be different than server VM to server VM communication.	5-7
إعداد متحكم منفصل بواجهة شبكة (NIC) في جميع الخوادم الافتراضية للإدارة المتصلة بشبكة افتراضية محلية مستقلة للإدارة. A separate NIC shall be configured on all server VMs for management connected to a separate out-of-band management VLAN.	6-7
إعداد بروتوكولات الإنترنت الثابتة على الخوادم الافتراضية. Static IPs shall be configured on server VMs.	7-7
استخدام البروتوكولات الإدارية التي تدعم التشفير مثل أمن طبقة النقل (TLS)، وبروتوكول النقل الآمن (SSH)، وبروتوكول نقل النص التشعبي الآمن (HTTPS)، وغيرها. Management protocols that support encryption, such as TLS, SSH, HTTPS, etc., shall be utilized.	8-7
تقييد إدارة بيئة الأنظمة الافتراضية وحصرها على المشرفين المعنيين فقط. تشمل إدارة الأنظمة الافتراضية: • إنشاء الخوادم الافتراضية وتثبيتها وبدء تشغيلها ونقلها وإغلاقها وإزالتها. • إعداد وتغيير المتحكم بواجهة الشبكة (NIC) والشبكة المحلية الافتراضية (VLAN) ومفتاح التحويل الافتراضي (Vswitch). • إدارة الخوادم الافتراضية وإعدادات الوصول. Virtualization environment management shall be restricted to respective administrators only. Virtualization management includes: • VM creation, deployment, initialization, migration, shutdown, or deletion.	9-7

	• NIC, VLAN and Vswitch configuration and change. • VM administration and access configuration
10-7	عمل نسخة احتياطية على الخوادم الافتراضية وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة حائل. Regular VM backup shall be performed in accordance with Hail university's Backup and Recovery Management Policy.
11-7	إلغاء تفعيل مشاركة الملفات بين البيئات الافتراضية للخوادم والمستضيف. File sharing between host and server VMs shall be disabled.
12-7	تطبيق وإعداد نظام أمان ذو طبقة مزدوجة للبيئة الافتراضية وعزل بيئة الإنتاج عن بيئات الاختبار الافتراضية. Layer-2 security shall be configured for the virtual environment, and production environment shall be separated from VMs test environments.
13-7	إعداد شعارات التحذير والتصريح على خوادم المضيف والضيف لإنذار الأشخاص غير المصرح لهم من الاستخدام غير السليم للخادم. Warning and authorization banners shall be configured on both host and guest servers to warn unauthorized users who improperly use a server.
14-7	تسجيل جميع الأنشطة المتعلقة بالأجهزة الافتراضية بما في ذلك الإنشاء والنشر والترحيل والحذف. All activities related to virtual machines, including creation, deployment, migration and deletion, shall be logged.
8	إدارة الخوادم (Central Management)
الهدف	تحديد المتطلبات الأمنية لإدارة الخوادم لضمان إدارة وتشغيل الخوادم بطريقة آمنة وضمان تطبيق وتنفيذ جميع المتطلبات الأمنية.
المخاطر المحتملة	يؤدي الافتقار إلى الإدارة الآمنة وعدم تطبيق المتطلبات الأمنية على الخوادم إلى زيادة احتمالية التعرض للهجمات ووجود الثغرات ونقاط الضعف في بيئة جامعة حائل، حيث يمكن استغلال هذه الثغرات في الهجمات أو الاختراقات الخبيثة التي تعرض الخوادم والبيانات في جامعة حائل إلى انتهاكات أمنية.

الضوابط	
1-8	إعداد خادم الإدارة المركزية أو خادم النطاق ليطبق سياسات الإعدادات والتحصين المعتمدة في جامعة حائل على جميع الخوادم. Central management server or domain server shall be configured to enforce Hail university's Configuration and Hardening policies on all servers.
2-8	تثبيت أدوات إدارة إعدادات النظام التي تقوم تلقائياً بتنفيذ وإعادة تثبيت إعدادات الضبط والتهيئة للأنظمة في فترات زمنية محددة ومنتظمة. System configuration management tools that automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals shall be deployed.
3-8	تطبيق نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة محتوى الأمن (Security Content Automation Protocol "SCAP") للتأكد من عناصر الإعدادات الأمنية كافة وجدولة الاستثناءات المعتمدة والإبلاغ عن حدوث أي تغييرات غير مصرّح بها. Configuration monitoring system compliant with Security Content Automation Protocol (SCAP) shall be implemented to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني.

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني.

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الاكتروني.

الالتزام بالمعيار

1- يجب على المشرف على إدارة الأمن السيبراني ضمان التزام جامعة حائل بهذا المعيار دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.

جامعة حائل
University of Ha'il

معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني

مقيّد - داخلي

التاريخ:	04/05/2023
الإصدار:	3.0
المرجع:	الهيئة الوطنية للأمن السيبراني

قائمة المحتويات

الأهداف

يهدف هذا المعيار إلى توفير متطلبات الأمن السيبراني التقنية المبنية على أفضل الممارسات والمعايير لإدارة سجلات الأحداث ومراقبة الأمن السيبراني والعمل على حماية جامعة حائل من التهديدات الداخلية والخارجية.

يتبع هذا المعيار المتطلبات التشريعية والتنظيمية الوطنية وأفضل الممارسات الدولية ذات العلاقة، وهو متطلب تشريعي في الضابط رقم ١-٣-٣ والضابط رقم ٢-١٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل

يغطي هذا المعيار جميع تقنيات إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) في جامعة حائل، وينطبق على جميع العاملين في جامعة حائل.

المعايير

1	صيغة السجل (Log Format)
الهدف	استخدام صيغة قياسية ومتسقة للسجل تشتمل على جميع المعلومات المطلوبة.
المخاطر المحتملة	قد يصعب الربط بين عدة سجلات مختلفة إذا تم حفظها بصورة غير متسقة، وهذا يؤدي إلى زيادة المخاطر الناتجة عن المعلومات الخاطئة، وبالتالي يُعقِّد التعامل مع الأحداث الأمنية وحلها.
الإجراءات المطلوبة	
1-1	يجب أن تشتمل صيغة سجل الأحداث على المعلومات التالية: 1-1-1 **نوع سجل الأحداث:** مثل النظام، والأمن، والتدقيق، والنقطة الأساسية (Kernel)، والتصريح، والبريد، وغيرها. 1-1-2 **موقع** الحدث أو مصدر السجل ونظامه. 1-1-3 **تاريخ** سجل الحدث **وختمه الزمني.** 1-1-4 **حالة الحدث:** مثل ناجح، أو فاشل، أو نشط، أو غير نشط، أو مسموح، أو مرفوض، أو غيره. 1-1-5 **مستوى خطورة الحدث:** مثل طارئ، أو تنبيه، أو حرج، أو خطأ، أو تحذير، أو إشعار معلوماتي، أو إشعار تصحيحي. 1-1-6 **رسالة الحدث:** رسالة فعلية من الحدث. Events log format shall include:

	1-1-1 **Event Log Type:** Such as System, Security, Audit, Kernel, Authorization, Mail, etc. 1-1-2 **Location** of the event or source/system of the log. 1-1-3 **Date** and **Timestamp** of the event log. 1-1-4 **Event Status:** Success, Failure, Up, Down, Allow, Deny, etc. 1-1-5 **Event Severity:** Emergency, Alert, Critical, Error, Warning, Notice, Informational, etc. 1-1-6 **Event Message:** Actual message of the event.
2-1	إدراج تفاصيل إضافية في السجلات حيثما ينطبق ذلك، مثل: المستخدم وعنوان الإنترنت ومنفذ المصدر، وعنوان ومنفذ الوجهة، وعناصر أخرى مفيدة. Additional details shall be included in logs wherever applicable, such as user, source address/port, destination address/port, and other useful elements.
2	الأختام الزمنية (Timestamps) - الخوادم الزمنية المتزامنة الإضافية (Redundant Time Servers Synchronized)
الهدف	استخدام نظام زمني ثابت للأصول المعلوماتية والتقنية الداخلية.
المخاطر المحتملة	قد يصعب المقارنة بين مجموعتين مختلفتين من السجلات إذا تم حفظها بصورة غير متسقة، ويؤدي ذلك إلى زيادة المخاطر الناتجة عن المعلومات الخاطئة وبالتالي يُعقِّد التعامل مع الأحداث الأمنية وحلها.
الإجراءات المطلوبة	
1-2	تزامن الأصل المعلوماتي والتقني مع ثلاثة خوادم زمنية إضافية على الأقل في غضون أجزاء من الثانية. The information and technology asset shall be synchronized to at least three redundant central time servers within milliseconds.
3	تسجيل الأحداث (Event Logging)
الهدف	التأكّد من توثيق وتسجيل الأحداث السيبرانية والأنشطة غير المصرّح بها التي تشهدها البيئة.

المخاطر المحتملة	من الضروري تسجيل بعض الأحداث الأساسية التي تُنفذ في البيئة، وإذا تعذّر على جامعة حائل تسجيل الأحداث التي حدّدتها متطلّبات الضابط، فسيؤدي ذلك إلى زيادة المخاطر الناتجة عن الأحداث غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في البيئة، والتي قد تؤثّر على أعمال الجهة بناءً على مستوى خطورة الحدث.
الإجراءات المطلوبة	
1-3	تسجيل جميع الأحداث المُحدّدة في متطلّبات هذا الضابط والتي تشمل: 1-1-3 محاولات الدخول الناجحة. 2-1-3 محاولات الدخول غير الناجحة، بالإضافة إلى تحديد ما إذا كانت محاولة الدخول قد تضمّنت إدخال كلمة مرور خاطئة. 3-1-3 جميع عمليات تسجيل الخروج. 4-1-3 الإضافات والمحذوفات والتعديلات على حسابات وصلاحيات المستخدم. 5-1-3 تغيير المستخدم لهويته خلال فترة زمنية معيّنة على الإنترنت. 6-1-3 محاولات لتنفيذ مهام غير مصرّح بها. 7-1-3 أنشطة الحسابات التي تملك صلاحيات هامة وحسّاسة. 8-1-3 إجراء تعديلات على إعدادات النظام (محدّدات النظام). 9-1-3 حق الوصول لقراءة أو تعديل معلومات سريّة للغاية التي يُحتمل تعرّضها للسرقة. 10-1-3 تسريب مواد متعلّقة بمعلومات سريّة للغاية خارج جامعة حائل. 11-1-3 الأحداث المتعلقة بالاتصالات الواردة والصادرة والتي تتضمّن أنشطة غير عادية أو غير مصرّح بها بما في ذلك وجود برامج ضارة (رموز البرامج الخبيثة "Malicious Code" وبرامج التجسّس "Spyware" والبرامج الدعائية "Adware"). 12-1-3 الإضافات والمحذوفات والتعديلات على معايير سجل الأمن والتدقيق. 13-1-3 الأخطاء (أي المشاكل التقنية في الأصول المعلوماتية والتقنية) التي قد تحدث نتيجة حادث أمني. 14-1-3 تشغيل الأنشطة أو إيقافها عن طريق خدمة معيّنة. 15-1-3 تعطّل النظام أو إعادة تشغيله. 16-1-3 تغيير كلمة المرور. 17-1-3 تفعيل جميع السجلات للأنظمة الحسّاسة.

	All the events specified under these control requirements shall be logged: 3-1-1 Successful login attempts. 3-1-2 Unsuccessful login attempts, along with the identification of whether the login attempt involved an invalid password. 3-1-3 All logoffs. 3-1-4 Additions, deletions and modifications to user accounts/privileges. 3-1-5 Users switching IDs during an online session. 3-1-6 Attempts to perform unauthorized functions. 3-1-7 Activities performed by privileged accounts. 3-1-8 Modifications to system settings (parameters). 3-1-9 Read or write access to protected information, where there is a potential for theft of that information. 3-1-10 Exfiltration of materials related to protected information outside Hail university. 3-1-11 Detections in inbound and outbound communications for unusual or unauthorized activities including the detection of malware (such as malicious code, spyware, and adware). 3-1-12 Additions, deletions and modifications to security/audit log parameters. 3-1-13 Faults (technical problems in information and technology assets) that could potentially be attributed to a security event. 3-1-14 Activation or deactivation of activities by a specific service. 3-1-15 System crashes or restarts. 3-1-16 Password changes. 3-1-17 Enablement of all critical systems logs.
4	مصادر الأحداث (Event Sources)
الهدف	التأكّد من مراقبة جميع سجلات الأحداث المتعلّقة بالأصول المعلوماتية والتقنية الخاصة بـجامعة حائل لكشف أي نشاط غير مصرّح به في الشبكة والذي قد يتسبب بحدث أمني.
المخاطر المحتملة	إن عدم التمكّن من كشف أي نشاط غير مصرّح به سيمنع جامعة حائل من التعامل بطريقة مناسبة مع الأحداث المشبوهة قبل أن تتفاقم وتصبح أكثر خطورة.

الإجراءات المطلوبة	
1-4	تهيئة مصادر سجل الأحداث وأنظمة تسجيل الدخول لنقل السجلات عبر بروتوكولات موثوقة وشائعة الاستخدام لنقل سجل الأحداث، مثل: (Syslog)، و(Windows Instrumentation Interface)، و(SNMP Traps)، وغيرها. The event log sources and logging systems shall be configured to transport logs over reliable and commonly used event log transport protocols such as syslog, Windows Instrumentation Interface (WMI), SNMP traps, etc.
2-4	جمع كافة سجلات الأحداث من المصادر المُحدّدة ضمن هذا المطلب: 1-2-4 الأنظمة بما فيها أنظمة التشغيل وقواعد البيانات ووسائط التخزين والشبكات والتطبيقات، التي تغطي أحداث النظام وسجلات الأمن والتدقيق. 2-2-4 الأنظمة الحسّاسة بما فيها أنظمة التشغيل وقواعد البيانات ووسائط التخزين والشبكات والتطبيقات، التي تغطي أحداث النظام وسجلات الأمن والتدقيق. 3-2-4 أحداث الحسابات ذات الصلاحيات الهامة والحسّاسة. 4-2-4 الأحداث الخاصة بالتصفّح والاتصال بالإنترنت والشبكة اللاسلكية. 5-2-4 الأحداث الناتجة عن نقل البيانات إلى وسائط تخزين خارجية. 6-2-4 سجلات الأحداث الصادرة من تقنيات إدارة تغييرات الملفات (File Monitoring Integrity). 7-2-4 سجلات الأحداث المُولّدة من تغييرات إعدادات النظام وتحديثات وإصلاحات النظام والتغييرات على التطبيقات. 8-2-4 أنشطة مشبوهة مثل الأنشطة التي يكتشفها نظام منع الاختراقات (Prevention System Intrusion). 9-2-4 أحداث تُولّدها الحلول الأمنية بما فيها البرامج المضادة للبرمجيات الخبيثة (Antivirus, Antimalware, Advanced Persistent Threat "APT") وتقنيات الوصول عن بُعد (Remote-Access Technologies) (مثل: الشبكة الافتراضية الخاصة " Virtual Private Network")، ووسطاء الويب (Web Proxies)، وبرنامج إدارة الثغرات، ونظام منع الاختراقات في المستضيف (Host Intrusion System Prevention)، وخوادم التحقّق من الهوية (Authentication Servers)، وغيرها. 10-2-4 أحداث تُولّدها أجهزة حماية الشبكة بما في ذلك جدران الحماية والمُوجّهات (Routers) ومديري حركة الشبكة (Traffic Managers)، وغيرها.

4-2-11 أحداث تُولّدها البيئة الافتراضية وأدواتها وبنيتها التحتية الأساسية. 4-2-12 تفعيل تسجيل الاستفسارات (Query Logging) في نظام أسماء النطاقات (Domain Name System) حيثما أمكن ذلك من الناحية التقنية. 4-2-13 سجلات الأحداث التي تُولّدها أنظمة التحكّم الصناعي (Industrial Control Systems). All event logs shall be collected from the sources specified under this requirement: 4-2-1 Systems, including Operating Systems, Databases, Storage, Networks, Applications, etc., covering system events and security/audit logs. 4-2-2 Critical Systems, including Operating Systems, Databases, Storage, Networks, Applications, etc., covering system events and security/audit logs. 4-2-3 Events of privileged accounts. 4-2-4 Logs generated in the events of Internet browsing, Internet connections and Wi-Fi connections. 4-2-5 Events generating from data transfer to external storage. 4-2-6 File Integrity Monitoring (FIM) event logs. 4-2-7 Event logs generated from system configuration changes, system updates and patches, and application changes. 4-2-8 Abnormal activities such as those detected by Intrusion Prevention System (IPS). 4-2-9 Events generated by security solutions including Antimalware, Remote-Access Technologies (such as Virtual Private Network VPN), Web Proxies, Vulnerability Management Software, Host Intrusion Prevention System (HIPS), Authentication Servers, etc. 4-2-10 Events generated by perimeter devices including firewalls, routers, traffic managers, etc.	

	4-2-11 Events generated by virtualization environments and their underlying tools and infrastructure. 4-2-12 Enable Domain Name System (DNS) query logging wherever technically applicable. 4-2-13 Event logs generated by Industrial Control Systems (ICS).
5	مراقبة الأحداث (Events Monitoring)
الهدف	كشف أي نشاط غير مصرّح به في الشبكة والذي قد يسبب حدث أمني.
المخاطر المحتملة	إن عدم التمكّن من كشف أي نشاط غير مصرّح به في الشبكة يمنع الجهة من التعامل بالطريقة المناسبة مع الأحداث المشبوهة قبل أن تتفاقم وتصبح أكثر خطورة.
الإجراءات المطلوبة	
1-5	يجب مراجعة تنبيهات الأحداث الأمنية الناتجة عن جدران الحماية يومياً للكشف عن أي محاولات وصول غير مصرح بها أو سلوك غير عادي. وتستطيع جامعة حائل مراقبة التنبيهات الصادرة عن جدران الحماية على سبيل المثال من خلال مراقبة السجلات يومياً أو من خلال مراقبة جوانب النظام الأخرى مثل أنماط محاولة الوصول، وخصائص الوصول، وغيرها من الإجراءات. Security event alerts generated from firewalls shall be reviewed on a daily basis to detect any unauthorized access attempts or unusual behavior. Hail university can monitor alerts from firewalls, for example, by observing logs daily or by observing other system aspects such as access attempt patterns, characteristics of access, etc.
2-5	تفعيل مراقبة الشبكة اللاسلكية وذلك لكشف نقاط الوصول اللاسلكية غير المصرّح بها. وقد تتجاوز الإشارات اللاسلكية حدود النطاق الخاضع للمراقبة، وعلى ذلك تتخذ الجهات خطوة استباقية للبحث عن الاتصالات اللاسلكية غير المصرّح بها، بما في ذلك إجراء عمليات مسح مكثّفة عن نقاط الوصول اللاسلكية غير المصرّح بها، وهذه العمليات المسحية لا تقتصر فقط على الأصول التي تحتوي على أصول معلوماتية وتقنية، بل تشمل كذلك المناطق الواقعة خارج مبانيها عند الضرورة، وذلك للتحقّق من عدم اتصال نقاط الوصول اللاسلكية غير المصرّح بها بالأنظمة. Wireless network monitoring shall be enabled to detect unauthorized wireless access points. Wireless signals may radiate beyond the confines of organization-controlled facilities. Organizations shall proactively search for

unauthorized wireless connections including performing thorough scans for unauthorized wireless access points. Scans shall not be limited to those areas within facilities containing information and technology assets, but also shall include areas outside facilities as needed to verify that unauthorized wireless access points are not connected to the systems.	
تطبيق آليات مراقبة المستضيف (Host-based Monitoring Mechanisms) على النهايات الطرفية للأصول المعلوماتية والتقنية ذات الخطورة العالية. وتشمل مكوّنات الأصول المعلوماتية والتقنية التي يُمكن تطبيق آليات مراقبة المستضيف عليها الخوادم وأجهزة المستخدمين والأجهزة المحمولة. Host-based monitoring mechanisms shall be implemented on endpoint system components for high-risk information and technology assets. Information and technology asset components where host-based monitoring can be implemented include servers, workstations, and mobile devices.	3-5
تطبيق آليات المراقبة القائمة على ملف تعريف الملف والسلوك (Signature-based and Behavior-based Code)، مثل البرامج المضادة للفيروسات وتقنية كشف النهايات الطرفية والاستجابة لها (Endpoint Detection and Response) وأدوات كشف التهديدات المتقدمة المستمرة (APT Tools) على الأصول المعلوماتية والتقنية لكشف رمز البرامج الخبيثة. Signature-based and behavior-based code monitoring mechanisms (such as Antivirus, EDR, and APT tools) shall be implemented on information and technology assets to detect malicious code.	4-5
ضمان مواصلة تحديث آليات المراقبة القائمة على ملفات التعريف والسلوك بشكل مستمر. Signature-based and behavior-based code monitoring mechanisms shall be kept current with all available signatures or indicators.	5-5
تُنشَر أجهزة المراقبة لمتابعة الاتصالات على المكوّنات الخارجية للنظام (مثل: محيط النظام) وعلى المكوّنات الداخلية الرئيسية (مثل: الواجهات المنطقية والمادية داخل الأصول المعلوماتية والتقنية) لاكتشاف العيوب واكتشاف التسريب المخفي للمعلومات وتتبع أنواع محدّدة من الأنشطة التي تهم جامعة حائل. على سبيل المثال: الأجزاء الشبكية حيث تقع الأنظمة التي يُمكن الوصول إليها من الإنترنت.	6-5

	Monitoring devices shall be deployed to monitor communications at the external boundary of the system (e.g., system perimeter) and at key internal boundaries (e.g., logical/physical interfaces within the information and technology asset) to discover anomalies, detect covert exfiltration of information and track specific types of transactions of interest to Hail university. For example, Network segments where systems that are accessible from the Internet are located.
7-5	تطبيق أدوات المراقبة للكشف عن مؤشرات الهجمات المنفّذة ضد الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل والتي تؤدي إلى حجب *الخدمة*. Monitoring tools shall be employed to detect indicators of *denial of service* attacks against Hail university's information and technology assets and infrastructure.
6	التنبيه بالأحداث (Event Alerting)
الهدف	التأكّد من تفعيل وضبط خاصية التنبيه بالأحداث وإبلاغ العاملين المعنيين في جامعة حائل بشأنها ليتمكّنوا من التعامل مع أي حادث أمني بأكبر قدر من الفاعلية.
المخاطر المحتملة	قد يؤدي عدم ضبط خاصية التنبيه بالأحداث في أنظمة التسجيل إلى التعامل مع الأحداث الأمنية بطريقة خاطئة أو حتّى عدم التعامل معها كلياً.
الإجراءات المطلوبة	
1-6	إصدار التنبيهات للأصول المعلوماتية والتقنية عند وقوع أحداث المراقبة الأمنية المحدّدة مسبقاً و/أو عند استيفاء مستويات المؤشرات المتعلّقة بأي نشاط ضار محتمل. Alerts for information and technology assets shall be generated when previously defined security monitoring events occur and/or thresholds for indications of potentially malicious activity are met.
2-6	ضبط وسائل التنبيه لإبلاغ العاملين المعنيين، بما في ذلك البريد الإلكتروني والرسائل النصية القصيرة وأنظمة شاشات المراقبة، وغيرها. Alerting methods, including email, SMS, video wall systems, etc., shall be configured to notify the appropriate personnel.
7	مستويات التنبيه (Alert Threshold)
الهدف	اتباع نهج مُوثّق بشأن الحالات التي ينبغي تشغيل التنبيهات فيها.

المخاطر المحتملة	قد يؤدي عدم توثيق نطاق التنبيهات والغرض منها إلى عدم تهيئتها بالشكل المناسب، وقد تمر الأحداث الضارة المحتملة دون أن يلاحظها أحد.
الإجراءات المطلوبة	
1-7	تحديد وتوثيق المستويات المحدّدة للتنبيه عن أحداث مراقبة الأمن، ومراجعة مستوى التنبيه وتحديثه دورياً لمواكبة الهجمات الأمنية المستجدة. Specific thresholds for alerting on security monitoring events shall be identified and documented. Thresholds shall be periodically revised and updated to stay current with trending security attacks.
8	التنبيه بالأحداث الناتجة عن جدار الحماية (Firewall Event Alerting)
الهدف	إبلاغ العاملين المعنيين المؤهلين للتعامل مع الأحداث الأمنية المحتملة والناتجة عن جدران الحماية.
المخاطر المحتملة	إن لم يتم إبلاغ العاملين المعنيين بالأحداث الناتجة عن جدار الحماية، فإن جامعة حائل لن تكون على دراية بالمحاولات الخبيثة المحتملة غير المصرّح بها للاتصال بالشبكة، وبالتالي إذا تمكّن هذا النشاط من اختراق جدار الحماية، ستتعرّض أعمال جامعة حائل لمخاطر ضارة ناتجة عن الحادث الأمني.
الإجراءات المطلوبة	
1-8	ضبط التنبيهات أو أدوات المراقبة لتنويه العاملين المعنيين بالأحداث المتعلّقة بالأمن والناتجة عن جدار الحماية. Alarms or monitoring tools shall be configured to alert the appropriate personnel of security-related events originating from the firewall.
9	التنبيه بالأحداث الناتجة عن التطبيقات (Application Event Alerting)
الهدف	التأكّد من توثيق وتسجيل الأحداث الأمنية والأنشطة غير المصرّح بها التي تشهدها البيئة.
المخاطر المحتملة	من الضروري تسجيل بعض الأحداث المحورية المتعلّقة بالتطبيقات الخاصة بجامعة حائل، فإذا تعذّر على جامعة حائل تسجيل الحوادث المتعلّقة بالتطبيق والتي حدّدتها متطلّبات الضابط، سيؤدي ذلك إلى زيادة المخاطر الناتجة عن الحوادث الأمنية غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في التطبيق، والتي قد تؤثّر على أعمال الجهة بناءً على مستوى خطورة الحادث.

الإجراءات المطلوبة	
1-9	تسجيل جميع طلبات العميل واستجابات الخادم. All client requests and server responses shall be logged.
2-9	تسجيل جميع معلومات الحساب (مثل: محاولات التحقّق الناجحة وغير الناجحة والتغييرات على الحساب). All account information (e.g., successful and failed authentication attempts and account changes) shall be logged.
3-9	تسجيل جميع المعلومات المتعلّقة بالاستخدام (مثل: عدد الأنشطة التي تحدث في فترة معيّنة). All usage information (e.g., the number of transactions occurring in a certain period) shall be logged.
4-9	تسجيل جميع الإجراءات التشغيلية المهمّة (مثل: تشغيل وإغلاق التطبيقات وأعطال التطبيقات والتغييرات على إعدادات التطبيقات). All significant operational actions (e.g., application startup and shutdown, application failures, and application configuration changes) shall be logged.
10	مراقبة البرمجيات الضارة في الاتصالات (Malware in Communication Monitoring)
الهدف	تحديد وجود البرمجيات الضارة (مثل: رمز البرامج الخبيثة وبرامج التجسّس والإعلانات المتسلّلة) في اتصالات جامعة حائل قبل أن تتسبّب بأي ضرر.
المخاطر المحتملة	إذا لم يتم كشف أي استخدام غير مصرّح به للأنشطة بما في ذلك وجود البرمجيات الضارة، لن تكون جامعة حائل على دراية بوجود البرمجيات الضارة قبل أن تنتشر، مما يعرّض عملها لخطر هجوم أمني واسع النطاق.
الإجراءات المطلوبة	
1-10	مراقبة الاتصالات الواردة والصادرة الخاصة بجامعة حائل (مثل: رسائل البريد الإلكتروني والملفات المرفقة وعمليات التحميل) لضمان خلوها من البرمجيات الضارة (مثل: البرمجيات الضارة وبرامج التجسّس والبرامج الدعائية). Inbound and outbound Hail university's communications (such as *emails, file attachments, downloads*) shall be monitored for malware (such as *malicious code, spyware and adware*).

11	تحليلات مراجعة سجل الأحداث (Event Log Review Analytics)
الهدف	يُمكن أن يسهم تحليل السجل ونظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) في اكتشاف الأنشطة المشبوهة وتعزيز قدرات الاستجابة لحوادث الأمن السيبراني وكشف الهجمات التي تجاوزت الأنظمة الأمنية الأخرى.
المخاطر المحتملة	إن عدم التمكّن من كشف أحداث وحوادث الأمن السيبراني سيزيد من المخاطر الناتجة عن عدم ملاحظة الهجمات السيبرانية مما يؤدي إلى انتهاك الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل.
الإجراءات المطلوبة	
1-11	إرسال جميع الأحداث إلى نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني من أجل إدارة السجلات وتحليل محتواها وعلاقتها ببعضها والتنبيه عليها. All event logs shall be forwarded to a centralized log analytics or Security Information and Event Management (SIEM) system for log correlation, analysis and alerting.
2-11	إجراء مراجعة دورية لسجلات الأحداث لمراقبة السلوكيات والأحداث المشبوهة واكتشافها. Regular review on SIEM shall be performed to monitor and detect abnormal behavior and anomalies.
3-11	ضبط نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني دورياً لتحديد الأحداث القابلة للتطبيق وتقليل الأحداث الناتجة عنها بطريقة أفضل. SIEM system shall be tuned on a regular basis to better identify actionable events and decrease event noise.
4-11	مراجعة سجلات الأحداث والتنبيهات دورياً باستخدام أساليب يدوية وتقنيات آلية. Event logs and alerts shall be periodically reviewed, using manual and automated techniques.
5-11	الكشف عن الأحداث غير المصرّح بها والمتعلّقة بالأصول المعلوماتية والتقنية. Significant unauthorized activity related to information and technology assets shall be detected.
6-11	كشف سوء استخدام حسابات المستخدم ذات الصلاحيات الهامة والحسّاسة. Misuse of privileged user accounts shall be detected.

12	تحويل السجل وتحليله (Log Conversion and Parsing)
الهدف	التأكّد من مراقبة جميع سجلات الأحداث المتعلّقة بالأصول المعلوماتية والتقنية الخاصة بـجامعة حائل لكشف أي نشاط غير مصرّح به في الشبكة والذي قد يسبب حدثاً أمنياً.
المخاطر المحتملة	من الضروري تسجيل بعض الأحداث المحورية التي تُنفذ في البيئة، فإذا تعذّر على جامعة حائل تسجيل الأحداث التي حدّدتها متطلّبات الضابط، سيؤدي ذلك إلى زيادة المخاطر الناتجة عن الأحداث غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في البيئة، والتي قد تؤثّر على أعمال الجهة بناءً على مستوى خطورة الحادث.
الإجراءات المطلوبة	
1-12	استخدام أدوات لتحويل السجلات غير المدعومة من نظام التسجيل الخاص بـجامعة حائل إلى صيغة قياسية أو مدعومة للسجل. Log conversion utilities shall be used to convert logs unsupported by Hail university's logging system to a standard or supported log format.
2-12	تطبيق برنامج تسجيل مزوّد بآليات التحليل لاسترجاع السجلات من الأنظمة غير المدعومة بطريقة مناسبة. Logging software with parsing mechanisms shall be implemented to retrieve logs properly from unsupported systems.
13	المراقبة المستمرة (Continuous Monitoring)
الهدف	تفعيل المراقبة المستمرة لجميع سجلات الأصول المعلوماتية والتقنية للكشف عن الأنشطة الخبيثة والحفاظ على فاعلية المراقبة مع الوقت.
المخاطر المحتملة	إذا لم تضع الجهة خطّة مراقبة لهذه الأنشطة وتوثّقها، فقد يرتفع خطر عدم وجود مراقبة مخصصة أو كافية لهذا الغرض، مما يزيد من مخاطر عدم الكشف عن الأنشطة الخبيثة.
الإجراءات المطلوبة	
1-13	تطوير وإعداد خطّة للمراقبة المستمرة (والتي تشمل على سبيل المثال: الجوانب التي يجب مراقبتها في نطاق العمل، وآلية المراقبة، واختبار فاعلية المراقبة) للأصول المعلوماتية والتقنية وتحديثها عند الحاجة. A plan for the continuous monitoring (which includes monitoring scope, frequency, and effectiveness testing) of the

	information and technology assets shall be developed and configured, and it shall be updated if needed.
14	أمن نظام التسجيل (Logging System Security)
الهدف	ضمان حماية وأمن البنية التحتية الأساسية لنظام التسجيل بما في ذلك محرّكات جمع سجلات الأحداث وتجميعها وربطها.
المخاطر المحتملة	من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية البنية التحتية لنظام التسجيل في جامعة حائل إلى استفادة المهاجمين من نقاط الضعف الكامنة في أنظمة التسجيل واستغلال ثغراتها للوصول غير مصرّح به إلى شبكة جامعة حائل وبياناتها.
الإجراءات المطلوبة	
1-14	إجراء اختبارات أمنية دورية (مثل: تقييم الثغرات الأمنية واختبار الاختراق) وفقاً لسياسة إدارة الثغرات الأمنية المتّبعة في جامعة حائل. Regular security testing (such as vulnerability assessments and penetration testing) shall be performed as per Hail university's Vulnerability Management Policy.
2-14	تنفيذ إصلاحات وتحديثات دورية على أنظمة التسجيل وفقاً لسياسة إدارة التحديثات والإصلاحات المتّبعة في جامعة حائل، وضمان تحديث جميع الأنظمة. Logging systems shall be regularly patched and updated as per Hail university's Patch Management Policy, and all systems shall be up-to-date.
3-14	حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من أنظمة التسجيل (مثل: خدمات الطباعة وبروتوكول تل نت "Telnet"، وغيرها). Unnecessary/unrequired applications and services on logging systems (e.g., *printing services, telnet, etc.*) shall be removed/disabled.
4-14	ضبط وتحصين أنظمة التسجيل بما في ذلك التطبيقات وقاعدة البيانات والتحصين على مستوى نظام التشغيل. يُرجى الرجوع إلى معيار أمن الخادم ومعيار أمن قاعدة البيانات المعتمدين في جامعة حائل. Logging systems hardening, including *application, database, and operating system level hardening,* shall be configured. Refer to Hail university's Server Security Standard and Database Security Standard.

5-14	تقييد الوصول لأنظمة التسجيل وحصره على مديري نظام التسجيل فقط. Access on logging systems shall be restricted to logging system administrators only.
6-14	حذف أو إلغاء تفعيل الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة. Default/non-interactive/unneeded accounts shall be removed/disabled.
7-14	إلزام مشرفي ومُشغّلي أنظمة التسجيل باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى أنظمة التسجيل. Logging systems administrators and operators shall be obliged to use multi-factor authentication to access the logging systems.
8-14	استخدام مبدأ الحد الأدنى من الصلاحيات والامتيازات الذي يمنح مديري ومُشغّلي أنظمة التسجيل امتيازات الوصول إلى مختلف أنواع أنظمة التسجيل. The least-privilege security principle shall be used to provide logging system administrators and operators with access to different types of logging systems.
9-14	تقييد الوصول لأنظمة التسجيل من خلال المنطقة الإدارية أو الشبكة المحلية الافتراضية الإدارية (Management VLAN) فقط. Access to logging systems shall be restricted to management zone or management VLAN only.
10-14	حذف أو إلغاء تفعيل خصائص نظام التسجيل وملفات الإعدادات غير الضرورية أو غير اللازمة. Unnecessary/unrequired logging system features and configuration files shall be removed/disabled.
11-14	حجب إمكانية الوصول إلى الملفات المشتركة عبر الشبكة والملفات غير الضرورية أو غير اللازمة. Access to unnecessary/unrequired network and file directories shall be blocked.
12-14	استخدام ضوابط الأجهزة وحجب الوصول إلى وسائط التخزين القابلة للإزالة.

	Hardware controls shall be used and access to removable media shall be blocked.
13-14	تثبيت برامج أنظمة تسجيل الأحداث على خوادم مخصصة لها. Logging systems software shall be installed on dedicated servers.
14-14	استخدام محرّك لجمع الأحداث في كل منطقة من مناطق بنية الشبكة، والسماح فقط لهذه المحرّكات بالتواصل مع نظام التسجيل المركزي أو أنظمة تجميع السجلات، على أن تتوفر في المناطق التالية على الأقل: 1-14-14 وضع محرّك لجمع الأحداث في *المنطقة المحايدة (DMZ)*. 2-14-14 وضع محرّك لجمع الأحداث في *منطقة قاعدة البيانات*. 3-14-14 وضع محرّك لجمع الأحداث في *منطقة التطبيقات*. 4-14-14 وضع محرّك لجمع الأحداث في *منطقة خدمات المؤسسة*. 5-14-14 وضع محرّك لجمع الأحداث في *منطقة المستخدم*. 6-14-14 وضع محرّك لجمع الأحداث في *منطقة الإدارة*. A log collector shall be implemented in each zone in the network architecture, and only these collectors shall be allowed to communicate with the centralized logging system or logging aggregation systems. A log collector shall be placed, at a minimum, in the following zones: 14-14-1 Place a log collector in the *DMZ*. 14-14-2 Place a log collector in the *database zone*. 14-14-3 Place a log collector in the *application zone*. 14-14-4 Place a log collector in the *corporate services zone*. 14-14-5 Place a log collector in the *user zone*. 14-14-6 Place a log collector in the *management zone.*
15	اختبار ومراجعة نظام المراقبة (Monitoring System Testing and Review)
الهدف	الحفاظ على القدرات التشغيلية والفاعلية في الكشف عن المحاولات غير المصرّح بها للوصول إلى الأصول المعلوماتية والتقنية.

المخاطر المحتملة	إذا لم تنجح أنظمة المراقبة في الكشف عن الأنشطة غير المصرّح بها، فإن ذلك سيزيد من احتمالية عدم ملاحظة النشاط الخبيث، والذي قد يؤدي إلى وقوع حادث أمني خطير.
الإجراءات المطلوبة	
1-15	إجراء مراجعات واختبارات على أدوات المراقبة الأمنية الخاصة بـجامعة حائل عن طريق أفراد مصرّح لهم بذلك للتأكّد من الالتزام بسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدة في جامعة حائل ونجاحها في تلبية أهداف المراقبة. Reviews and tests shall be performed by authorized individuals on Hail university 's security monitoring tools to validate that they comply with Hail university 's Cybersecurity Event Logs and Monitoring Management Policy and successfully meet the monitoring objectives.
16	الاحتفاظ بسجلات الأحداث (Retaining Event Logs)
الهدف	تجنّب حذف سجلات الأحداث الأمنية خلال الفترة التي يُمكن أن تُستخدَم خلالها.
المخاطر المحتملة	إذا حُذِفَت سجلات الأحداث الأمنية قبل تدقيقها أو التحقيق فيها، لن تتمكّن جامعة حائل من حماية أو فحص الأنشطة التي حدثت في الأصول المعلوماتية والتقنية الخاصة بها.
الإجراءات المطلوبة	
1-16	القيام بالنسخ الاحتياطي للسجلات دورياً ووفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة حائل. Periodic backup of logs shall be performed as per Hail university’s Backup and Recovery Management Policy.
2-16	الاحتفاظ بسجلات الأحداث لمدة 12 شهراً على الأقل، ولمدة 18 شهراً بالنسبة للأصول الحسّاسة كحد أدنى أو لفترة أطول، وفقاً لسياسة الأمن السيبراني المعتمدة في جامعة حائل. Event logs shall be retained for at least twelve (12) months for all assets, and at least eighteen (18) months for critical assets, or for a longer period, as per Hail university’s Cybersecurity Policy.
3-16	تقييد أرشفة وحذف سجلات الأحداث وحصره على المستخدمين المصرّح لهم وذلك فقط بعد انتهاء المدّة الزمنية المحدّدة للاحتفاظ بالسجلات، والسماح للمديرين المعنيين بالأصول المعلوماتية والتقنية بإجراء عملية أرشفة سجلات الأحداث وحذفها. The archival and deletion of event logs shall be restricted to authorized users and only after the expiration of the retention

	period. Appropriate information and technology asset administrators shall be authorized to carry out event log archival and deletion.
4-16	اختبار إمكانية استعادة واسترجاع النسخ الاحتياطية دورياً وفقاً لسياسة إدارة النسخ الاحتياطية المعتمدة في جامعة حائل. Backup retrieval and recovery shall be regularly tested as per Hail university's Backup and Recovery Management Policy.
17	توفير عملية بديلة لتسجيل الأحداث (Alternate Logging Capability)
الهدف	تمكين جامعة حائل من مواصلة تسجيل الأنشطة المتعلّقة بالأحداث الأمنية الحسّاسة حتّى في حال تعطّل الوسيلة الأساسية لتسجيل الأحداث (مثل: التسجيل المركزي).
المخاطر المحتملة	إذا تعطّلت وسيلة تسجيل الأحداث الأساسية المتعلّقة بأصل عالي الخطورة ولم تتوفّر عملية تسجيل بديلة، فإنه قد يتعذّر إنشاء سجل تدقيق أو تحديد النشاط الخبيث وذلك لعدم وجود سجلات يُمكن أن تستخدمها جامعة حائل للقيام بإجراءات المراقبة والتحقيق، علماً بأن الأصول الأعلى خطورة تؤثّر بشكل أكبر على أعمال الجهة في حال وقوع حادث أمني معيّن.
الإجراءات المطلوبة	
1-17	ضبط الأنظمة الحساسة، بالإضافة إلى إرسال السجلات إلى نظام تسجيل أحداث مركزي، لتحفظ سجلات الأحداث على أجهزتها في حال تعطّل الاتصال بالشبكة. In addition to sending logs to a centralized logging system, high risk information and technology assets shall be configured to maintain local logs in the event of network connectivity failure
18	توافر سجل الأحداث (Event Log Availability)
الهدف	ضمان استمرارية تشغيل وسيلة تسجيل الأحداث وقابلية استخدامها للأصول المعلوماتية والتقنية الحسّاسة.
المخاطر المحتملة	إذا لم تتوفّر وسيلة تسجيل الأحداث، فإن ذلك سيزيد من احتمالية عدم ملاحظة النشاط الخبيث وعدم القدرة على إجراء تحقيق بشأن الحادث والذي قد يؤدي إلى وقوع حادث أمني خطير.
الإجراءات المطلوبة	

1-18	ضبط الأصول المعلوماتية والتقنية الخاصة بـجامعة حائل والتي تحتوي على معلومات **محمية**، أو معلومات مصنفة من خلال تقييم إدارة المخاطر على أنها تتطلب تسجيل أحداثها، لإرسال الأحداث الخاصة بها بشكلٍ دائم. Hail university's information and technology assets with **protected** information, or designated through risk management assessment as requiring event logs, shall be configured to generate event logs at all times.
2-18	إعداد أنظمة تسجيل إضافية متعدّدة مزوّدة بقدرات توفير الخدمة على مدار الساعة ودون انقطاع. Multiple redundant logging systems with failover capabilities shall be configured.
19	تصنيف السجلات (Log Classification)
الهدف	يجب حماية جميع سجلات أحداث الأمن السيبراني بطريقة آمنة.
المخاطر المحتملة	إذا طبّقت السجلات ضوابط مُخصّصة لبيانات ذات تصنيف أدنى على الرغم من احتواء هذه السجلات على بيانات مُصنّفة بأنها **سريّة للغاية**، فستكون هذه البيانات أكثر عرضة لخطر انتهاكها لأن الضوابط المحدّدة لحمايتها تعتبر أقل صرامة.
الإجراءات المطلوبة	
1-19	التعامل مع أنظمة التسجيل المركزي باعتبار أنها تحتوي بحدٍّ أدنى على بيانات **سرية** و**مقيدة** خاصة بـجامعة حائل وأنها ملتزمة بجميع الضوابط ذات العلاقة بسريّة المعلومات. Centralized logging solutions shall be treated as if they contain, at a minimum, Hail university's **Secret** and **Restricted** data, and as if they comply with all relevant confidentiality controls.
2-19	بالنسبة إلى أي سجل للتطبيقات أو للأنشطة يحتوي على بيانات مُصنّفة على أنها **سرية للغاية**، يجب فرض الضوابط المطلوبة لهذا النوع من البيانات. For any application log or transaction record(s) that contains data classified as **Top Secret**, the controls required for that classification of data shall be enforced.
20	أمن السجلات وسلامتها (Log Integrity and Security)
الهدف	اعتماد آلية قادرة على كشف التعديلات على سجلات الأحداث الأمنية للتأكد من الاحتفاظ بها في حالتها الأصلية.

المخاطر المحتملة	إذا كان من الممكن تعديل سجلات الأحداث الأمنية دون وجود أي وسيلة لكشف هذا التعديل، فيمكن للمستخدم أن يُخفي نشاطه الخبيث داخل الأصل المعلوماتي والتقني. وفي هذه الحالة، إذا أُجري تحقيق بناءً على الأنشطة الضارة التي قام بها المستخدم، فلن يكون هناك دليل لمحاكمة المستخدم، ولن تُوجّه جامعة حائل ادعاءات مبرّرة بحق المستخدم ذي النوايا الضارة أو الخبيثة. كما أنه في حال انتهاك سلامة السجلات، فإنها قد تعتبر غير مقبولة في إجراءات المحكمة.
الإجراءات المطلوبة	
1-20	الحفاظ على سلامة السجل الأصلي، وتوفير آليات لحماية سلامة السجل بما فيها *ضابط تقييد الوصول ومستودعات البيانات المحظورة*، وغيرها. Original log integrity shall be maintained. Mechanisms to protect log integrity can include *strict access control*, *restricted data repositories*, etc.
2-20	تطبيق وسائل لتشفير السجلات في حالتي الإرسال والتخزين، مثل أمن طبقة النقل (Transport Layer Security)، واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suite) المُوصى بها (مثل: التشفير بمجموعة suite B). يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة حائل. Methods to encrypt logs during transmission and at rest shall be implemented, such as Transport Layer Security (TLS). Recommended next generation encryption protocols and cipher suites (such as suite B cryptography) shall be used. Refer to Hail university's Cryptography Standard.
3-20	تطبيق وسائل يُمكنها كشف التعديلات على السجلات في حالتي الإرسال والتخزين مثل خوارزميتي دالة التجزئة (Hashing) واختزال الرسالة (Message Digest) التشفيريتين، وذلك بالإضافة إلى آليات لكشف التعديل أو محاولات التعديل التي تعتمد على أساليب معيّنة مثل تقليل حجم السجل وتغيير دالة تجزئة الملف ووصول العمليات من غير النظام (مثل: كافة العمليات لكتابة واختزال السجلات باستثناء الآلية منها). يُرجى الرجوع إلى معيار التشفير المعتمد في جامعة حائل للاطلاع على متطلّبات السلامة والتجزئة. Methods that can detect modification of logs during transmission and at rest, such as hashing and message digest algorithms, shall be implemented. Mechanisms to detect modification or attempts of modification can rely on certain triggers such as reduction in log size, change in file hash, access by non-system processes (e.g., everything except automated processes for writing and digesting logs). Refer to

	Hail university's Cryptography Standard for integrity and hashing requirements.
4-20	تقييد الوصول إلى ملفات السجل ووسائط تخزين السجلات على نظام التسجيل فقط. ومنح المديرين حق الوصول إلى السجلات لأغراض استكشاف الأخطاء وإصلاحها في الفترة المخصّصة للصيانة فقط. Access to log files and logs storage shall be restricted to the logging system only. Access to logs shall be provided to administrators for troubleshooting purposes only during the troubleshooting or maintenance period.
5-20	ضبط إعدادات التحكّم بمعدل إرسال السجلات (Log Rate Limiting) لمنع تعرّض نظام التسجيل إلى هجمات حجب الخدمة، وضبط مستواه عند حد معقول. Rate limiting shall be configured to prevent *denial of service* attacks for the logging system. Additionally, it shall be configured to a reasonable threshold.
21	موارد تسجيل الأحداث (Logging Resources)
الهدف	تجنّب فقدان السجلات جرّاء استبدال البيانات المُخزّنة على وسائط التخزين.
المخاطر المحتملة	إن عدم التمكّن من توفير مساحة كافية لتخزين أقصى حدّ ممكن من السجلات قد يؤدي إلى استبدال المعلومات المُخزّنة في السجل وفقدان بيانات قيّمة ومهمّة خاصة بجامعة حائل. وفي هذه الحالة، من الممكن أن تُحذَف السجلات الحسّاسة بالكامل ولن تتمكّن جامعة حائل من الاعتماد على هذه السجلات في حال توجيه دعوى قضائية أو إجراء تحقيق معيّن، وهذا الأمر قد يؤثّر على أعمالها.
الإجراءات المطلوبة	
1-21	توفير موارد كافية (مثل: موارد النظام ووسائط تخزين البيانات ونطاق الشبكة) لاستيعاب أنشطة التسجيل المحدّدة. ويجب أن تحتوي أجهزة تخزين السجلات على سعة تخزين كافية لجمع السجلات. Sufficient resources (e.g., *system resources, data storage, and network bandwidth*) shall be provided to accommodate prescribed logging activities. Log storage devices shall have sufficient log storage for collecting logs.
22	التغييرات على إعدادات التسجيل (Logging Configuration Changes)

الهدف	الحد من إمكانية إجراء أي تغييرات غير مصرّح بها أو ضارة على عملية تسجيل الأحداث الجاري تنفيذها في مكوّنات النظام.
المخاطر المحتملة	إذا لم تُفرَض أي قيود على المسؤول عن إدخال التغييرات على إعدادات السجل ومكان وموعد إجرائها، فإنه يُمكن أن يقوم مُستخدم خبيث بإيقاف التسجيل على الأجهزة الحسّاسة لتنفيذ هجوم غير ملحوظ.
الإجراءات المطلوبة	
1-22	تقييد إمكانية تغيير إعدادات سجل الأحداث الأمنية، بما فيها نطاق العمل وآلية المراقبة، وحصرها على المستخدمين المصرّح لهم فقط. Security event log configuration changes, including scope and monitoring frequency, shall be restricted to authorized users.
23	استخدام أجهزة المراقبة (Use of Monitoring Devices)
الهدف	منع الكشف عن البيانات الحسّاسة والتأثير على شبكة جامعة حائل (مثل: استنزاف موارد الشبكة أو استخدام أدوات ضارة/خبيثة في البيئة).
المخاطر المحتملة	إذا لم تصرّح الإدارة المعنية بالأمن السيبراني في جامعة حائل ولم تسمح لموظفين معيّنين باستخدام أدوات أو أجهزة المراقبة والفحص، من الممكن أن تُستخدَم إحدى الأدوات بطريقة تضر البيئة وتزيد خطر انتهاك البيانات أو وقوع حادث أمني.
الإجراءات المطلوبة	
1-23	تقييد استخدام أجهزة أو أدوات المراقبة والفحص على المستخدمين المصرّح لهم. The use of monitoring and scanning devices or tools shall be limited to authorized users.
2-23	تصنيف نتائج جميع أنشطة المراقبة والفحص ضمن المعلومات السريّة بحدٍّ أدنى. The results of all monitoring and scanning activities shall be classified as Confidential, at minimum.

الأدوار والمسؤوليات

1- **راعي ومالك وثيقة المعيار:** المشرف على إدارة الأمن السيبراني

2- **مراجعة المعيار وتحديثه:** إدارة الأمن السيبراني

3- **تنفيذ المعيار وتطبيقه:** عمادة تقنية المعلومات والتعليم الإلكتروني وإدارة الأمن السيبراني .

الالتزام بالمعيار

1- يجب على المشرف على إدارة الامن السيبراني ضمان التزام جامعة حائل بهذا المعيار دورياً.

2- يجب على كافة العاملين في جامعة حائل الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جامعة حائل.