

عمادة تقنية المعلومات
والتعليم الإلكتروني
Deanship of Information
Technology & E-Learning



رؤية
2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA



سياسة أمن العمليات بجامعة حائل

2023/2022م

سَمَاءُ اللَّهِ عَزَّ وَجَلَّ

سياسة أمن العمليات بجامعة حائل

المحتويات	الصفحات
معلومات ذات ملكية فكرية	4
الرعاية على الوثيقة	
معلومات عن الوثيقة	5
الإعداد والتحديث	5
قائمة التوزيع	5
الاعتماد	5
نظرة عامة على السياسة	
الغرض	6
النطاق	6
المصطلحات والتعريفات	7
التغيير والمراجعة والتحديث	8
النفاذ والامتثال	8
الاستثناءات	8
الأدوار والمسؤوليات (مصفوفة المهام RACI)	9
الوثائق ذات الصلة	10
الملكية	10
بيانات السياسة	
توثيق إجراءات التشغيل	11
إدارة التغيير	12
إدارة القدرات	12
الفصل بين بيئات التطوير وبيئات الاختبار والبيئات التشغيلية	13
ضوابط للحماية من البرامج الضارة	13
النسخ الاحتياطي للمعلومات	15
تسجيل الحوادث	16
حماية معلومات السجل	16
سجلات المسؤول والمشغل	16
مزامنة الساعات	17
تثبيت البرامج على أنظمة التشغيل	17
إدارة الثغرات الفنية	18
القيود المفروضة على تثبيت البرامج	19
ضوابط مراجعة نظم المعلومات	20

Deanship of Information
Technology & E-Learning



عمادة تقنية المعلومات
والتعليم الإلكتروني

معلومات ذات ملكية فكرية:

هذه الوثيقة هي عبارة عن معلومات خاصة بعمادة تقنية المعلومات والتعليم الإلكتروني في جامعة حائل.

وهي وثيقة موجهة للجهات المعنية فقط حيث لا يتم توزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة تقنية المعلومات والتعليم الإلكتروني. جميع الحقوق محفوظة لعمادة تقنية المعلومات والتعليم الإلكتروني.

الرقابة على الوثيقة

معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة أمن الاتصالات	عام	2.0	عام

الإعداد والتحديث

الإصدار	المؤلف / المؤلفون	تاريخ الإصدار	التغييرات
0.1			إعداد
0.2			مراجعة
0.3			تحديث
1.0			مسودة
1.1			
1.2			
2.0			

قائمة التوزيع

#	المستفيد
1	إدارة الشؤون القانونية
2	الموقع الإلكتروني للجامعة
3	قسم ضمان الجودة بالعمادة

الاعتماد

الاسم	الصفة	التاريخ	التوقيع
د. خالد بن عبدالعزيز العتيبي	عميد تقنية المعلومات والتعليم الإلكتروني		

نظرة عامة على السياسة:

يستعرض هذا الجزء بالتفصيل الغرض من هذه السياسة ونطاقها وتعريف مصطلحاتها، وتغييرها، ومراجعتها وتحديثها، وإنفاذها/ والامتثال لها، والأدوار والمسؤوليات، واستثناءاتها، والوثائق ذات الصلة بالإضافة الملكية الوثيقة.

الغرض:

الغرض الرئيسي من سياسة أمن الاتصالات هو:

ضمان التشغيل السليم والأمن المرافق معالجة المعلومات، بالإضافة إلى ضمان الحماية من البرمجيات الخبيثة والفيروسات ومن فقدان البيانات بسبب أحصنة طروادة. ومع ذلك، تضمن هذه السياسة سلامة النظم التشغيلية؛ وتمنع استغلال نقاط الضعف التقنية؛ وتقلل تأثير أنشطة التدقيق والمراجعة على النظم التشغيلية.

النطاق:

تنطبق بيانات السياسة المكتوبة في هذه الوثيقة على جميع موارد وحدة المراجعة الداخلية على جميع مستويات الحساسية، بما في ذلك:

- جميع الموظفين بدوام كامل وبدوام جزئي والموظفين المؤقتين الذين يعملون لدى جامعة حائل أو يعملون لصالحها أو بالنيابة عنها.
- الطلاب الذين يدرسون في جامعة حائل.
- المقاولون والاستشاريون الذين يعملون لصالح جامعة حائل أو نيابة عنها.
- جميع الأفراد والجماعات الأخرى الذين تم منحهم إمكانية الوصول إلى أنظمة تقنية المعلومات والتعليم الإلكتروني في جامعة حائل

تغطي هذه السياسة جميع أصول المعلومات المحددة في وثيقة نطاق تقييم المخاطر وسيتم استخدامها كأساس لإدارة أمن المعلومات.

المصطلحات والتعريفات:

• يوفر الجدول تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة.

المصطلح	التعريف
المساءلة	مبدأ أممي يشير إلى ضرورة القدرة على تحديد هوية الأفراد وتحملهم مسؤولية أفعالهم.
الأصول	المعلومات التي تعتبر ذات قيمة بالنسبة للمؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام المعلومات.
توفر	الحالة التي يكون فيها الأصل أو الخدمة قابلة لأن تصلها جهة مصرح لها بذلك وقابلة لأن تستخدمها أيضا.
إدارة القدرات	عملية تحديد سعة النظام اللازمة لتقديم مستويات أداء محددة من خلال القياس والتحليل لحجم العمل الحالي والمتوقع.
السرية	عدم توفر الأصل أو الخدمة أو عدم كشف أي منهما للأفراد أو جهات أو عمليات غير مصرح بها.
الرقابة	وسيلة لإدارة المخاطر تشمل السياسات والإجراءات والإرشادات التي يمكن أن تكون ذات طبيعة إدارية عليا أو تقنية أو إدارية أو قانونية.
الإرشاد	وصف يوضح الأشياء المطلوب عملها وكيفية تحقيق الأهداف المحددة في السياسات.
الحادثة	حدوث حالة بعينها في النظام أو الخدمة أو الشبكة تشير إلى خرق محتمل لسياسة أمن المعلومات أو فشل إجراءات السلامة أو قد تكون الحالة ذات صلة بالأمن لكنها غير معروفة سابقا.
أمن المعلومات	الحفاظ على سرية المعلومات وسلامتها وتوفرها. وهو يشمل وسائل أخرى مثل التحقق والمساءلة وعدم التنصل والموثوقية.
السلامة	الحفاظ على الأصول والتأكد من دقتها وتناسقها طوال دورة حياتها بأكملها.
البرامج الضارة (الخبثية)	برنامج مصمم لتعطيل تشغيل الحاسب الآلي أو جمع معلومات حساسة أو الوصول إلى أنظمة الحاسب الآلي الخاصة (على سبيل المثال، فيروس أو حصان طروادة).
المالك (صاحب)	أي شخص أو مجموعة من الأشخاص تم تحديدهم من قبل الإدارة لتحمل مسؤولية الحفاظ على سرية الأصول وتوافرها وسلامتها. وقد يتغير المالك أثناء دورة حياة الأصل.
اختبار الاختراقات	طريقة لتقييم تأمين نظام الحاسب الآلي أو الشبكة عن طريق محاكاة هجوم من جهات خارجية ضارة ليس لديها وسائل معتمدة للوصول إلى أنظمة الجامعة) وجهات داخلية خبيثة (لا تتمتع بمستوى معين من الوصول المصرح به)، تتضمن هذه العملية تحليلا نشطا للنظام للتعرف على أي ثغرة أمنية محتملة يمكن أن تنجم عن التكوين السيئ أو غير الصحيح للنظام، سواء كانت عيوب معروفة أو غير معروفة في الأجهزة والبرمجيات أو نقاط ضعف تشغيلية في العملية أو التدابير التقنية المضادة. يتم تنفيذ هذا التحليل من موقع مهاجم محتمل ويمكن أن يتضمن هذه استغلالا نشطا لثغرات أمنية.
السياسة	خطة عمل يسترشد بها عند اتخاذ القرارات والإجراءات. وتشمل السياسة تحديد البدائل المختلفة مثل البرامج أو أولويات الإنفاق، والاختيار بينها على أساس التأثير الذي ستحدثه.
الخطر	مزيج من عواقب الحدث واحتمالات حدوثها (بما في ذلك التغييرات في الظروف).
النظام	جهاز أو نظام مترابط أو أنظمة فرعية من المعدات تستخدم في الحصول على البيانات أو تخزينها أو معالجتها أو إدارتها أو التحكم فيها أو عرضها أو تبديلها أو تبادلها أو نقلها أو استقبالها، بما في ذلك برامج الحاسب آلي والبرامج الثابتة والأجهزة.
التهديد	احتمال التسبب في حادثة غير مرغوب فيها تؤدي إلى إلحاق ضرر بنظام من نظم الجامعة مثل الكشف عن معلومات حساسة أو أصول أو خدمات بطريقة غير مصرح بها أو تدميرها أو إزالتها أو تعديدها أو التسبب في انقطاعها أو إصابة عدد من الأشخاص. وقد يكون التهديد متعمدا أو عرضيا أو ناجم عن أصل طبيعي.
الثغرة	نقطة ضعف في الإجراءات أو العمليات أو الضوابط الأمنية يمكن استغلالها عن طريق التهديد بالوصول غير المصرح به إلى المعلومات أو تعطيل المعالجة الحرجة المتعلقة بها.
تقييم الثغرات	عملية تحديد نقاط الضعف وتحديد أولوياتها (أو ترتيبها في نظام ما. والثغرة من منظور إدارة الكوارث تعني تقييم التهديدات الناجمة عن مخاطر محتملة على السكان والبنية التحتية.

التغيير، المراجعة والتحديث:

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر المالك إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية، والجهة الوحيدة المخول لها إجراء تغييرات في هذه السياسة هو ضابط أمن المعلومات على أن تعتمد الإدارة هذه التغييرات، ويجب أن يظل سجل التغيير محدثًا بحيث يتم تحديثه بمجرد إجراء أي تغيير.

الإنفاذ والامتثال:

يعد الالتزام بهذه السياسة إلزاميًا ويجب مراجعته بشكل دوري من قبل ضابط أمن المعلومات، ويجب على جميع وحدات جامعة حائل (من عمادات، وإدارات، وكليات، وأقسام ومراكز) ضمان مراقبة الامتثال المستمر للسياسة في حدود دائرة اختصاصها.

في حالة تجاهل أو انتهاك توجيهات أمن المعلومات، قد تتضرر بيئة جامعة حائل (على سبيل المثال، يحدث فقدان للثقة في الجامعة وتتضرر سمعتها، أو تتعطل عملياتها أو تحدث انتهاكات قانونية فيها)، ويكون الأشخاص المخطئون مسؤولين عن تجاهل توجيهات الأمن ومخالفتها مما يؤدي إلى اتخاذ إجراءات تأديبية أو تصحيحية بحقهم (مثل الفصل من الخدمة) ويمكن أن يخضعوا لتحقيقات قانونية.

يجب التأكد من أن الموظفين الذين يشبه في انتهاكهم للأوامر الأمنية تتم معاملتهم بطريقة صحيحة وعادلة (مثلاً

اتخاذ إجراءات تأديبية ضدهم). ويجب إبلاغ إدارة الموارد البشرية بالأمر والتعامل مع انتهاكات السياسة لمعالجتها.

الاستثناءات:

يجب أن ينظر أمن المعلومات في الاستثناءات على أساس فردي. كما يجب أن يرفق مع طلب الاستثناء حالة العمل المنطقية التي استدعت تقديمه وطلب الموافقة عليه، والجهة المخول لها الموافقة على هذا الطلب هي ضابط أمن المعلومات على أن تعتمد هذه الموافقة عمادة تقنية المعلومات والتعليم الإلكتروني. ويجب أن يشتمل كل طلب استثناء المبررات والمزايا المنسوبة إلى الاستثناء من الامتثال للسياسة.

تبلغ فترة الاستثناء من الامتثال للسياسة أربعة أشهر كحد أقصى، ويجب إعادة تقييم هذه المدة واعتماد تمديداتها. إذا لزم الأمر. لمدة أقصاها ثلاث فترات متتالية، ولا يجوز الاستثناء من هذه السياسة لأكثر من ثلاث فترات متتالية.

الأدوار والمسؤوليات (مصفوفة المهام RACI):

يوضح الجدول مصفوفة المهام (RACI) التي تحدد من هو المسائل أو المسؤول أو الذي يجب أن يستشار أو يبلغ بكل مهمة يجب تنفيذها.

هناك بعض الأدوار التي تشترك فيها عدة أطراف في هذه السياسة؛ وهي على التوالي: عمادة تقنية المعلومات والتعليم الإلكتروني، موظف (ضابط) أمن المعلومات، مكتب إدارة المشاريع، المالك والمستخدم (ويشمل الموظف والمتعاقد).

المستخدم	المالك	الإدارة القانونية	ضابط أمن المعلومات	تقنية المعلومات	الاسم المسؤوليات
		R,I	C	R,A	تحديد والحفاظ على متطلبات القدرات لجميع الأنشطة الجديدة والمستمرة المشروع تقنية المعلومات.
I	R,A		C	R,A	تحديد حقوق الوصول المطلوبة للمستخدمين للأصول.
			C	R,A	أداء مراقبة النظام / التطبيق / شبكة الأمن.
I			C	R,A	إدارة البنى التحتية الأمنية الحرجة (على سبيل المثال، البنية التحتية لمكافحة الفيروسات).

المستعمل	المالك	مكتب إدارة المشاريع	ضابط أمن المعلومات	تقنية المعلومات	الاسم المسؤوليات
I			C	R,A	تصميم وتنفيذ أمن الشبكات والنظام.
I			C	R,A	تطبيق الضوابط المناسبة لحماية سرية وسلامة وتوافر وصحة المعلومات الحساسة
I			C	R,A	تنسيق الرد على الانتهاكات الفعلية أو المشتبه فيها في سرية أنظمة جامعة حائل الحرجة أو سلامتها أو توفرها.
	C,I		C	R,A	تنفيذ التغييرات وتثبيت التصحيح على النظام / التطبيق / الشبكة وفقا للإجراءات إدارة التغيير وإدارة التصحيح.
R,A,I			C	C	الالتزام بسياسات وإجراءات أمن المعلومات المتعلقة بحماية المعلومات.
R	I		C	A,C	الإبلاغ عن الحوادث الأمنية الفعلية أو المشتبه بها لعمادة الاتصالات وتقنية المعلومات.

اتصف مصفوفة راعي (RACI) الخاصة بتحديد المسؤوليات والأدوار المختلفة التي يشارك بها أعضاء الفريق في إنجاز مهام العمل، وهي مفيدة بشكل خاص في توضيح الأدوار والمسؤوليات عند تنفيذ عمليات تتعدد فيها الوظائف أو الإدارات. يرمز الحرف (R) إلى الموظف الذي ينفذ مهمة من المهام، أما الحرف (A) فيرمز للشخص المسؤول (أو جهة الاعتماد) حيث يوقع هذا الشخص أو يعتمد المهمة المناطة إلى الموظف * (R) أما الحرف (C) فيرمز إلى المستشار الذي يقدم رأياً حول ما هو مراد تنفيذه، ويرمز الحرف (I) إلى الشخص الذي يكون على علم ودراية بالمهمة وهو الذي تصله أحدث المعلومات عن سير المهمة.

الوثائق ذات الصلة:

فيما يلي جميع السياسات والإجراءات ذات الصلة بهذه السياسة:

- سياسة أمن المعلومات
- سياسة إدارة الأصول
- سياسة التحكم في الوصول
- سياسة إدارة حوادث أمن المعلومات.
- سياسة الامتثال
- سياسة إدارة المخاطر
- إجراءات النسخ الاحتياطي والاستعادة
- إجراءات إدارة التغيير
- إجراءات إدارة التصحيح
- إجراءات إدارة الوصول المادي والمنطقي
- إجراءات الحصول على النظام وتطويره وصيانته.

الملكية:

هذه الوثيقة مملوكة وتحافظ عليها عمادة تقنية المعلومات والتعليم الإلكتروني بجامعة حائل وهي التي تحافظ عليها.

بيانات السياسة

تقدم الأجزاء الفرعية التالية بيانات السياسة في أربعة عشر جانباً رئيسياً هي:

- توثيق إجراءات التشغيل.
- إدارة التغيير.
- إدارة القدرات.
- فصل بيئات التطوير والاختبار والتشغيل.
- ضوابط للحماية من البرامج الضارة.
- النسخ الاحتياطي للمعلومات.
- تسجيل الحوادث.
- حماية معلومات السجل.
- سجلات المسؤول الإداري والمشغل.
- تزامن الساعة.
- تثبيت البرامج على أنظمة التشغيل.
- إدارة نقاط الضعف الفنية.
- القيود المفروضة على تثبيت البرامج.
- ضوابط تدقيق نظم المعلومات.

توثيق إجراءات التشغيل:

1. تبادر عمادة الاتصالات وتقنية المعلومات ومسؤول أمن المعلومات بإعداد العمليات والإجراءات والإرشادات والمعايير أو تشرف على إعدادها وفقاً للأنشطة التشغيلية لجامعة حائل، قد يشمل توثيق إجراءات التشغيل على سبيل المثال لا الحصر ما يلي:

أ. إعادة تشغيل النظام واسترجاعه.

ب. تركيب النظام وتهيئته.

ج. الدعم الاحتياطي.

د. صيانة الأجهزة.

هـ. غرفة الخادم.

و. إدارة التعامل مع البريد.

ز. الرقابة.

2. عند تنفيذ البرامج المطورة حديثاً أو المحدثات أو نقلها من بيئة اختبار إلى بيئة إنتاج يجب أن تتبع إجراءات توثيق صحيحة.

إدارة التغيير:

١. تقوم عمادة تقنية المعلومات والتعليم الإلكتروني بالتعاون مع ضابط أمن المعلومات بإعداد إجراء إداري رسمي يحدد جميع الأدوار والمسؤوليات لضمان السيطرة الكافية على جميع التغييرات.
٢. تشمل الإجراءات التفصيلية لإدارة التغيير والضوابط المناسبة لها ما يلي - على سبيل المثال لا الحصر:
 - أ. وضع معايير القبول بالتنسيق مع مالك الأصول.
 - ب. قيام ضابط أمن المعلومات بتقييم المخاطر التي قد تنجم عن التغييرات الرئيسية الجديدة المقترحة.
 - ج. عدم استخدام التغييرات الطارئة على مرافق أو أنظمة أو تطبيقات تقنية المعلومات والاتصالات إلا في الظروف القاسية وبموافقة الإدارة.
 - د. تطبيق إجراءات التحكم في المستندات دائماً.
 - هـ. عدم تطبيق تصحيحات لمعالجة الأخطاء البرمجية إلا بعد التأكد من أنها ضرورية على أن يتم ذلك بترخيص من الفريق الفني والإدارة والمورد.
 - و. اختبار التطوير الذي يحدث في البرمجيات أو الأنظمة بدقة قبل نشر هذه البرمجيات والأنظمة المطورة في بيئة إنتاج جامعة حائل.

إدارة القدرات:

١. يجب مراعاة متطلبات الأداء والسعة الجديدة للأنظمة في مرحلة التخطيط والتصميم. ومن أمثلة إدارة الطلب على السعة - على سبيل المثال لا الحصر - ما يلي:
 - أ. حذف البيانات القديمة (مساحة القرص).
 - ب. إيقاف تشغيل التطبيقات أو النظم أو قواعد البيانات أو البيئات.
 - ج. تقوية منطق التطبيق أو استفسارات قاعدة البيانات.
 - د. تقييد استخدام عرض النطاق الترددي في خدمات الأعمال غير الهامة التي تستهلك المزيد من الموارد (مثل بث الفيديو).
٢. تقوم عمادة تقنية المعلومات والتعليم الإلكتروني بالتعاون مع مكتب إدارة المشاريع بتحديد متطلبات القدرات المتعلقة بجميع الأنشطة الجديدة والمستمرة ويحتفظ بها.

الفصل بين بيئات التطوير وبيئات الاختبار والبيئات التشغيلية:

١. يجب تنفيذ الفصل بين بيئات الاختبار والإنتاج لتقليل فرص إساءة استخدام الأنظمة بإهمال أو بشكل متعمد.
٢. عند الاقتضاء، لا تستخدم بيانات حية لإجراء اختبارات على أي أصول، سواء في بيئة الإنتاج أو في بيئة الاختبار.
٣. يجب أن تضمن عمادة الاتصالات وتقنية المعلومات تطبيق جميع التغييرات بدقة واختبارها في بيئة اختبار قبل التصريح بالتغيير في بيئة الإنتاج.

ضوابط للحماية من البرامج الضارة:

١. على عمادة تقنية المعلومات والتعليم الإلكتروني ضمان بقاء البنية التحتية للكشف عن البرامج الضارة نشطة وغير معطلة ولا يمكن تعطيلها في أي نقطة دخول محتملة.
٢. على عمادة تقنية المعلومات والتعليم الإلكتروني تطبيق الضوابط المناسبة لمنع انتقال البرمجيات الضارة إلى المستخدمين المتصلين بالبنية التحتية الخاصة بشبكة جامعة حائل.
٣. يجب تحديد وتنفيذ مستوى مناسب من الضوابط لحماية سلامة البرامج والمعلومات، حيث قد تشمل هذه الضوابط على سبيل المثال لا الحصر ما يلي:
 - أ. ضوابط كشف ووقاية واسترداد للحماية من البرامج الضارة.
 - ب. إجراءات مناسبة لتوعية المستخدمين.
٤. يجب أن تطبق برمجية مكافحة فيروسات مركزية- حيثما كان ذلك مناسباً - على مختلف المستويات في البنية التحتية للشبكة والنظم (مثل الخوادم وأجهزة الحاسب المكتبية وأجهزة الحاسب الآلي المحمولة والبوابات في الشبكة المحيطة) في إطار منهج متدرج للحد من دخول البرامج الضارة إلى بيئة جامعة حائل على أن يؤخذ في الحسبان ما يلي:
 - أ. يجب أن تظل ملفات التوقيع في برامج مكافحة الفيروسات محدثة باستمرار لتكون محمية من البرامج الضارة الجديدة التي تنشأ بانتظام.

- ب.** يجب توصيل خادم مكافحة الفيروسات المركزي في جميع الأوقات بخادم تحديث تعريف الفايروس الخاص بالبائع، على أن يجري تحديث ملفات توقيع الخوادم يوميا، بمجرد توفر إصدارات البائع المعمول بها ومن ثم دفعها إلى جميع مستخدمي محطات العمل في جامعة حائل.
- ج.** يجب أن تكون محطات العمل والأجهزة المفعلة على الشبكة والخوادم معدة لأن تصل للشبكة في هيئة تمكنها من الحصول على أحدث ملف للتوقيع بمجرد اتصالها بشبكة جامعة حائل، سواء كان اتصالا فعلياً أو عبر شبكة افتراضية خاصة (VPN).
- د.** يجب إزالة جميع البرمجيات الضارة المكتشفة على أنظمة جامعة حائل على الفور، ولا يسمح للأنظمة التي عليها برمجيات ضارة لم تزل أو تعطل أن تتصل بشبكة الجامعة.
- هـ.** يجب أن تعد برمجية مكافحة الفيروسات بحيث تزيل جميع البرامج الضارة التي تم اكتشافها على النظام تلقائياً.
- و.** يحظر تماماً تثبيت أي برمجية غير مصرح بها أو غير قانونية على أي نظام من أنظمة جامعة حائل على أن يؤخذ في الاعتبار ما يلي:
- أ.** لا يجوز استخدام جميع أقراص الذاكرة الخارجية (USB) أو الأقراص المضغوطة أو أقراص دي في دي (DVD) أو الوسائط القابلة للإزالة على أي جهاز حاسب آلي تابع لجامعة حائل، ما لم تكن معتمدة من عمادة تقنية المعلومات والتعليم الإلكتروني.
- ب.** يجب تهيئة جميع خوادم ومحطات عمل جامعة حائل لمسح الوسائط الخارجية القابلة للإزالة بحثاً عن الفيروسات بمجرد توصيل هذه الأدوات بالأجهزة.
- ج.** يجب تنظيف الوسائط المصابة بالفيروسات قبل تركيبها لتكون وحدات تخزين للبيانات على خوادم ومحطات عمل جامعة حائل.
- د.** قبل توزيع أي برمجيات أو معلومات في شكل محوسب، على المستخدمين أولاً إخضاع هذه البرمجيات أو المعلومات للفحص المناسب، بما في ذلك المسح الشامل للتأكد من عدم وجود أي فيروسات تهاجم الحاسب الآلي.
- 7.** يجب أن يتفهم العاملون بجامعة حائل مسؤوليتهم المتعلقة بإبلاغ عمادة تقنية المعلومات والتعليم الإلكتروني بأي مشكلات ذات صلة بوجود شفرة ضارة (إن وجدت). كما يجب عليهم الإبلاغ عن أي سلوك غير طبيعي أو غير معتاد في النظام مثل:
- أ.** معالجة بطيئة للتطبيقات.
- ب.** وجود نشاط مستمر أو مطول في الأقراص الثابتة أو الشبكة.

النسخ الاحتياطي للمعلومات:

١. يجب على عمادة تقنية المعلومات والتعليم الإلكتروني بالتعاون مع مالكي (أصحاب الأصول تحديد متطلبات النسخ الاحتياطي والاستعادة لجميع المعلومات والتطبيقات وأنظمة التشغيل وقواعد البيانات وإعدادات المستخدم وإعدادات الأجهزة بما يتماشى مع النصوص القانونية والتنظيمية وتوصيات الشركة المانعة وخطورة المعلومات والعوامل الأخرى ذات الصلة.
٢. لتلبية ومعالجة متطلبات النسخ الاحتياطي، وإدارة بيئة احتياطية، يجب أن تؤخذ الأشياء التالية في الاعتبار:
 - أ. تقليل جهد الإدارة في التعامل مع أشرطة النسخ الاحتياطي للمعلومات.
 - ب. دمج وسائط النسخ الاحتياطي والتخزين في موقع مركزي.
 - ج. أن تكون برمجية النسخ الاحتياطي بسيطة بالقدر الذي يستل النسخ الاحتياطي واستعادة البيانات، بحيث يمكن تكليف مشغل النسخ الاحتياطي بأداء هذه المهام.
 - د. تثبيت حل مركزي للنسخ الاحتياطي لإدارة سياسة النسخ الاحتياطي للمعلومات وإعداد متطلباته وتشغيله.
٣. على عمادة تقنية المعلومات والتعليم الإلكتروني الاحتفاظ بسجلات النسخ الاحتياطي ومراجعتها وتحديثها (على سبيل المثال، نسخة احتياطية لشبكة سيمانتيك نت)
٤. يجب تشفير النسخ الاحتياطي الذي يحتوي على معلومات حساسة حيثما كان ذلك ممكناً.
٥. يجب الاحتفاظ بجميع وسائط التخزين الاحتياطية في مكان آمن ولا يسمح بالوصول إليها إلا للعاملين في جامعة حائل المصرح لهم فقط.



تسجيل الحوادث:

١. يجب على ضابط (مسؤول أمن المعلومات ضمان تنفيذ مستويات محددة وكافية لتسجيل الأحداث وصار ذلك ممكنة في أنظمة وتطبيقات وقواعد بيانات جامعة حائل.
٢. يجب على ضابط (مسؤول أمن المعلومات التأكد من أن الأحداث المتعلقة بإنشاء حساب المستخدم وحذفه وإلغاء حقه في الوصول إلى معلومات الجامعة وخدماتها قد سجلت بطريقة مفصلة لمدة ثلاث سنوات على الأقل.
٣. يجب وضع إجراءات مفصلة لمراقبة استخدام مرافق تقنية المعلومات والتعليم الإلكتروني على أن تشمل هذه الإجراءات على سبيل المثال لا الحصر ما يلي:
 - أ. بيانات مفصلة عن الشخص الذي يراقب هذه الأنشطة وطبيعة المعلومات الإدارية المنتجة والجهة التي ستقدم لها هذه المعلومات.
 - ب. الفترات التي يتكرر فيها رصد الأنشطة.
 - ج. تفاصيل الإجراء الذي تم تنفيذه في حالة حدوث أي خرق أمني.

حماية معلومات السجل:

١. يجب أن تضمن عمادة تقنية المعلومات والتعليم الإلكتروني أن الضوابط الحالية تهدف إلى حماية سجل المرفق من التعرض لتغييرات غير مصرح بها ومشاكل تشغيلية. وتشمل هذه الضوابط على سبيل المثال لا الحصر ما يلي:
 - أ. تعديلات على أنواع الرسائل المسجلة.
 - ب. ملفات السجل التي يتم تحريرها أو حذفها.
 - ج. السعة التخزينية لوسائط ملف السجل التي يتم تجاوزها، مما يؤدي إما إلى عدم تسجيل الأحداث أو الكتابة فوق الأحداث المسجلة السابقة.

سجلات المسؤول والمشغل:

١. على عمادة تقنية المعلومات والتعليم الإلكتروني التأكد من مراجعة سجلات مسؤول النظام والمشغل بصورة دورية.
٢. على عمادة تقنية المعلومات والتعليم الإلكتروني التأكد من أن جميع مسؤولي النظام ومشغليه ليس لديهم إذن لتعديل أو إلغاء تنشيط سجلات أنشطتهم الخاصة.

مزامنة الساعات:

١. يجب أن تضمن عمادة تقنية المعلومات والتعليم الإلكتروني أن تاريخ ووقت مسارات مراجعة وتدقيق جميع الأنظمة والخوادم ومكونات الشبكة قد كانت متزامنة (في وقت واحد) لتسهيل تتبع هوية المستخدم وأنشطته.
٢. يجب مزامنة جميع الأنظمة والخوادم وساعات أجهزة الشبكة باستخدام بروتوكول وقت الشبكة (NTP) المقبول دولياً.

تثبيت البرامج على أنظمة التشغيل:

١. يجب تنفيذ الإجراءات للتحكم في تثبيت البرمجيات على أنظمة جامعة حائل، ولتقليل أخطار انقطاع الخدمات أو تلفها.
٢. يجب تقوية تأمين جميع الأنظمة من خلال التكوين الآمن المتوافق مع معايير أفضل الممارسات الدولية.
٣. يجب تطبيق الضوابط الأمنية الخاصة بنقطة النهاية لتقييد استخدام أجهزة النظام والأجهزة الطرفية.
٤. على مسؤولي تقنية المعلومات (على سبيل المثال، مسؤول النظام، مسؤول التطبيق، مسؤول قاعدة البيانات ومشرف الشبكة) مراعاة ما يلي:
 - أ. أن يكونوا هم الجهة الوحيدة المعتمدة لإجراء تحديثات للبرمجيات والتطبيقات ومكتبات البرامج التشغيلية.
 - ب. التأكد من توثيق إجراءات التكوين الرسمية (formal configuration) والاحتفاظ بها.
٥. أي قرار يقضي بتطوير أي مكون من مكونات تقنية المعلومات إلى إصدار جديد يجب أن يأخذ في الاعتبار متطلبات جامعة حائل في مجال الأعمال والأمن.
٦. يجب أن تكون إجراءات التشغيل الخاصة بأنظمة جامعة حائل موثقة بشكل واضح وأن يتم الاحتفاظ بسجل للأنشطة بتفاصيلها وأنواعها ويجب أن يراقب سجل الأنشطة دورياً وفقاً لسياسات وإجراءات الجامعة.

إدارة الثغرات الفنية:

1. على عمادة تقنية المعلومات والتعليم الإلكتروني إجراء تقييم سنوي للثغرات الفنية و (أو) عند حدوث تغيير كبير لتحديد نقاط الضعف في تكوينات الأنظمة أو التعرف على التصحيحات التي تحتاجها تلك الأنظمة.
2. على الإدارة مراجعة تقارير تقييم الثغرات الفنية، وعلى مسؤول أمن المعلومات وضع خطة لمعالجة المخاطر التي يمكن أن تنتج عن هذه المخاطر وتحديد أولويات المعالجة.
3. يجب تحديد الأدوار والمسؤوليات المتعلقة بإدارة الثغرات التقنية بوضوح.
4. يجب على ضابط أمن المعلومات ومسؤولي تقنية المعلومات والاتصالات القيام بما يلي:
 - أ. اتخاذ خطوات استباقية لتحديد نقاط الضعف في تقنية الأنظمة وتقليلها قبل أن يتم استغلالها.
 - ب. تحديد الضوابط المناسبة لتخفيف المخاطر والتهديدات بعد إجراء تقييم للثغرات وعمل اختبار الاختراق.
 - ج. اتخاذ الخطوات اللازمة لتوفير أمن الأنظمة والبنية التحتية للشبكة.
5. لا يجوز تثبيت أي تصحيحات جديدة في بيئة إنتاج ما لم يتم اختبارها وتقييمها بشكل صحيح في بيئة اختبار بموافقة البائع.
6. يجب على الموظفين الذين يؤدون واجبات إدارة الثغرات الأمنية ضمان ما يلي:
 - أ. يجب استخدام أدوات المسح الأمني على أساس محدد لتحديد الثغرات التي يمكن استغلالها من قبل أشخاص يقومون بمسح غير مصرح به باستخدام أدوات مماثلة، على ألا تؤثر أدوات المسح الأمني المستخدمة على أداء شبكة جامعة حائل.
 - ب. يجب استخدام أدوات متعددة بتقنيات مختلفة لتحديد أكبر قدر ممكن من الثغرات عند الاقتضاء.
 - ج. يجب إخطار مالك الأصول وأخذ موافقته على التأثيرات المحتملة لنشاط المسح على البيئة المستهدفة قبل بدء المسح.
 - د. يجب مراقبة مصادر الطرف الثالث المعلومات الثغرات الفنية للتأكد من ملاءمتها للأنظمة (على سبيل المثال، موقع البائعين، وتنبهات الأمن، وتصحيحات النظام، وطرق المعالجة، وتحديثات الفيروسات).

- ه. إذا أصدر بائع تصحيحاً لإصلاح عنصر تحكم متعلق بالأمن، فيعتبر إصدار التصحيح بمثابة إخطاراً ضمناً بالضعف وفي هذه الحالة يجب أن تتخذ إجراءات تخفيف المخاطر.
- و. جميع الأجهزة المعتمدة الملحقة بشبكة جامعة حائل وتشغيل أنظمة التشغيل التي بها ثغرات أمنية محددة تم تصحيحها لمعالجة الثغرات المعروفة وفقاً لتوصيات البائع.
- ز. في حالة تعذر تصحيح أي جهاز أو نظام متصل بشبكة أو أنظمة جامعة حائل، يتم تخفيف الثغرة الأمنية بواسطة تحكم أمني بديل مقبول.
- ص. يجب أن تكون إجراءات التشغيل الخاصة بأنظمة جامعة حائل موثقة بشكل واضح وأن يتم الاحتفاظ بسجل للأنشطة بتفاصيلها وأنواعها ويجب أن يراقب سجل الأنشطة دورياً وفقاً لسياسات وإجراءات الجامعة.

القيود المفروضة على تثبيت البرامج:

- ا. يجب على عمادة تقنية المعلومات والتعليم الإلكتروني تحديد وتنفيذ القواعد المناسبة للتحكم في تثبيت البرامج من قبل المستخدمين. يعتبر ما يلي:
 - أ. نوع عمليات التثبيت المسموح بها للبرامج (على سبيل المثال، التصحيحات المحدثة والأمان للبرامج المعتمدة).
 - ب. نوع عمليات تثبيت البرمجيات المحظورة (على سبيل المثال، البرمجيات المخصصة لاستخدام الموظفين فقط).

ضوابط مراجعة نظم المعلومات:

١. يجب على عمادة الاتصالات وتقنية المعلومات اتخاذ الإجراءات التالية:
 - أ. منع سوء الاستخدام المحتمل لأدوات مراجعة الأنظمة (على سبيل المثال، لاستخراج معلومات سرية دون إذن صحيح).
 - ب. التأكد من الحفاظ على سلامة النظم والبيانات المرتبطة بها.
 - ج. تجنب الانقطاعات المحتملة للأنظمة نتيجة لاستخدام هذه الأدوات.
٢. يجب أن يكون استخدام أدوات مراجعة الأنظمة (مثل برمجية المراقبة وبرمجيات استخراج البيانات ومعالجتها والأدوات المساعدة) وفقاً للشرطين التاليين.
 - أ. خضوع أدوات المراجعة للترخيص والقيود والضوابط وفقاً لإرشادات محددة.
 - ب. أن تكون أدوات المراجعة منفصلة عن الأنظمة التشغيلية ولا يحتفظ به في مكتبات الأشرطة أو مناطق المستخدمين، ما لم يتم توفير مستوى مناسب من الحماية الإضافية.
٣. لا يجوز أن يقوم الأشخاص المسؤولون عن تنفيذ الضوابط والمحافظة عليها بأنشطة التدقيق.
٤. يجب أن يتمتع للأشخاص الذين يقومون بأنشطة التدقيق وصول محدود (على سبيل المثال، حق الوصول إلى البرمجيات والبيانات لقراءتها فقط). ويقتصر الوصول بخلاف القراءة فقط على النسخ المعزولة من ملفات النظام ويجب محوه عند اكتمال أنشطة المراجعة.
٥. يجب مراقبة وتسجيل جميع عمليات الوصول أثناء أنشطة المراجعة لإنتاج مسار مرجعي. كما يجب توثيق جميع الإجراءات والمتطلبات والمسؤوليات.
٦. إذا شاركت أطراف ثالثة في أداء أنشطة المراجعة (قد ينشأ خطر يتمثل في إساءة استخدام أدوات التدقيق من قبل هذه الأطراف الثالثة، والمعلومات التي يتم الوصول إليها من قبل هذه الجهات الخارجية)، فيجب أن تؤخذ ضوابط تقييم المخاطر وتقييد الوصول المادي في الحسبان لمعالجة هذا الخطر وأي تبعات تنجم عنه، مثل القيام بتغيير فوري لكلمات المرور التي تم الكشف عنها للمراجعين.



عمادة تقنية المعلومات
والتعليم الإلكتروني
Deanship of Information
Technology & E-Learning



جامعة حائل
University of Hail

رؤية VISION
2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA