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

معتمد
ACCREDITED

جامعة حائل
University of Ha'il

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

سياسة أمن الاتصال بجامعة حائل

2023/2022م


بسم الله الرحمن الرحيم

سياسة أمن الاتصال بجامعة حائل

عمادة تقنية المعلومات
و التعليم الإلكتروني

Deanship of Information
Technology & E-Learning

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.

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 الالكتروني للجامعة
3	قسم ضمان الجودة بالعمادة
4	قسم الشبكات بالعمادة

الاعـــــتماد

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

نظرة عامة على السياسة:

يتناول هذا الجزء بالتفصيل الغرض من هذه السياسة ونطاقها وتعريف مصطلحاتها، وتغييرها، ومراجعتها

وتحديثها، وإنفاذها والامتثال لها والأدوار والمسؤوليات المتعلقة بها، والمستندات ذات الصلة وملكية السياسة.

الغـــرض:

الغرض الرئيسي من سياسة أمن الاتصالات هو:

ضمان حماية المعلومات في الشبكات والمرافق الداعمة لمعالجة المعلومات، والحفاظ على أمن المعلومات المنقولة داخل جامعة حائل ومع أي جهة خارجية.

النطـــاق:

تنطبق بيانات السياسة المكتوبة في هذه الوثيقة على جميع موارد جامعة حائل بجميع مستويات حساسيتها، 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.
- على أمن المعلومات المنقولة داخل جامعة حائل ومع أي جهة خارجية.

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

المصطلحات والتعريفات:

- **يوفر الجدول تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة.**

المصطلح	التعريف
المساءلة	مبدأ أمني يشير إلى ضرورة القدرة على تحديد هوية الأفراد وتحميلهم 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 يمكن الوصول إليها وقابلة للاستخدام عند الطلب من قبل جهة مصرح لها بذلك.
السرية	عدم توفير أو الكشف عن أصل من الأصول أو خدمة من الخدمات الأفراد أو كيانات 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 ما يجب عمله لتحقيق الأهداف المحددة في السياسات والطريقة التي تحقق بها تلك الأهداف.
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.
(المالك (الصاحب	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.
سياسة	خطة عمل يسترشد بها عند اتخاذ القرارات وعمل الإجراءات. وتشتمل السياسة على عملية لتحديد البدائل المختلفة مثل البرامج أو أولويات الإنفاق، والاختيار بينها على أساس التأثير الذي ستحدثه.
خطر	مزيج من عواقب الحدث (بما في ذلك التغييرات في الظروف) واحتمالات حدوثها.
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 الآلي والبرامج الثابتة والأجهزة.

التغيير، المراجعة والتحديث:

الغرض الرئيسي من سياسة أمن الاتصالات هو:

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر مالكها إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية،ولا يجري تغييرات في هذه السياسة إلا ضابط أمن المعلومات على أن تعتمد الإدارة هذه التغييرات. ويجب أن يظل سجل التغيير محدثا بحيث يخضع للتحديث بمجرد إجراء أي تغيير في السياسة.

الإنفاذ والامتثال:

يعد الالتزام بهذه السياسة إلزاميا 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 في نطاقها.

في حالة تجاهل أو انتهاك توجيهات أمن المعلومات، قد تتضرر بيئة جامعة حائل (على سبيل المثال، يحدث فقدان للثقة في الجامعة وسمعتها، أو تتعطل عملياتها أو تحدث بها انتهاكات قانونية)، ويكون الأشخاص الذين تجاهلوا هذه التوجهات أو انتهكوها مسؤولين عما وقعوا فيه من فعل أو ترك مما يؤدي إلى اتخاذ إجراءات تأديبية أو تصحيحية بحقهم (مثل الفصل من الخدمة) ويمكن أن يخضعوا لتحقيقات قانونية.

يجب ضمان معاملة الموظفين الذين يشتبه في انتهاكهم للأوامر الأمنية بطريقة صحيحة وعادلة (مثل الإجراءات التأديبية)، ويجب إبلاغ إدارة الموارد البشرية لمعالجة انتهاكات السياسة عند التعامل مع هذه الانتهاكات.

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 تمديدها. 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 المساءل والمسؤول ومن تتم استشارته أو إبلاغه بكل مهمة هناك حاجة للقيام بها. هناك بعض الأدوار المشاركة في هذه السياسة على التوالي: عمادة تقنية المعلومات والتعليم الإلكتروني، موظف أمن المعلومات (ISO)، إدارة الموارد البشرية / الوحدة الإدارية (HR/A)، والإدارة القانونية، الموظف المسؤول عن إدارة المشروع (PMO، المالك والمستخدم الموظف والمتعاقد)..

الأدوار / المسؤوليات	تقنية المعلومات	ضابط أمن المعلومات	الإدارة القانونية	الموارد البشرية/ الوحدات الإدارية	الموظف المسؤول عن إدارة المشروع	المالك	المستخدم
تحديد الاتفاقيات التي لا يجوز لموظفي جامعة حائل والأطراف الثالثة أن يفصحوا عنها.	R	C	C	C	R,A	I	
تطبيق الضوابط الصحيحة لحماية سرية المعلومات الحساسة وسلامتها وتوافرها وصحتها.	R,A	C				I	
الالتزام بسياسات وإجراءات أمن المعلومات المتعلقة بحماية المعلومات.	C	C					R,A
إدارة البنية التحتية لأمن الشبكة (مثل أجهزة الالتقاط والمفاتيح وجدران الحماية).	R,A	C		I		I	

اتصف مصفوفة راكي (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) ه (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 لهذه 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 تغيير الإدارة.
- 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 سبع جوانب رئيسة هي:

- ضوابط الشبكة.
- أمن خدمات الشبكة.
- الفصل في الشبكات.
- سياسات واجراءات نقل المعلومات.
- اتفاقيات نقل المعلومات.
- المراسلة الإلكترونية.
- اتفاقية السرية أو عدم الإفصاح.

ضوابط الشبكة:

١. تحدد عمادة تقنية المعلومات والتعليم الإلكتروني وتنفذ التدابير المضادة المناسبة من أجل:
   أ. التحكم في سرية وسلامة المعلومات الحساسة التي تمر عبر الشبكات العامة.
   ب. حماية الأنظمة والتطبيقات المتصلة بالشبكة.
   ج. الحفاظ على توفر خدمات الشبكة واتصالها بأجهزة الحواسيب.

٢. لا يجوز لجميع موظفي جامعة حائل وزوارها توصيل أي جهاز (على سبيل المثال أجهزة الحاسب الشخصية أو أجهزة الحاسب المحمول أو معدات الشبكات) بشبكة جامعة حائل، دون الحصول على إذن وموافقة مناسبين من قسم تقنية المعلومات.

٣. يجب على عمادة تقنية المعلومات والتعليم الإلكتروني السماح بكل حركات الشبكة المستندة إلى متطلبات الاتصالات التجارية المتعلقة بعمل جامعة حائل.

٤. يجب على عمادة تقنية المعلومات والتعليم الإلكتروني تطبيق آليات مناسبة للتحكم بتوجيه وتدفق المعلومات لمنع تسريب المعلومات لمسارات الشبكة المصممة

٥. تتأكد عمادة تقنية المعلومات والتعليم الإلكتروني من وجود إدارة وإشراف في محكم على بنية نطاق الأمن (مثل جدار الحماية وإعداداته الحالية، حيث يجب تغطية ما يلي، على سبيل المثال لا الحصر:
   أ. توثيق قواعد نطاق الأمن ومراجعتها بشكل منتظم.
   ب. توثيق تغييرات التكوين والحصول على موافقة الإدارة.
   ج. الحصول على موافقة الإدارة قبل تطبيق أي تغييرات على قواعد نطاق الأمن.
   د. العناية الكافية أثناء تطبيق التغييرات على قواعد نطاق الأمن لضمان الحد الأدنى من التشويه لبيئة جامعة حائل.

٦. يجب تقييد قدرة المستخدمين على الاتصال من خلال بوابات الشبكة والتي تقوم بتصفية حركة المرور عن طريق جداول أو قواعد محددة مسبقا. وتشمل هذه القيود على سبيل المثال لا الحصر الأشياء التالية:

أ. المراسلة (مثل البريد الإلكتروني).

ب. نقل الملفات.

ج. الوصول التفاعلي.

د. الوصول إلى التطبيقات.

أمن خدمات الشبكة:

١. تحمي عمادة تقنية المعلومات والتعليم الالكتروني البنية التحتية لشبكة جامعة حائل من خلال تنفيذ تدابير واجراءات مناسبة. وتشمل عناصر أمن خدمات الشبكة، على سبيل المثال لا الحصر ما يلي:

أ. التقنية المطبقة لضمان أمن خدمات الشبكة ممثلة في التحقق والتشفير وضوابط اتصال الشبكة.

ب. الضوابط الفنية المطلوبة للاتصال الأمن بخدمات الشبكة وفقا لقواعد اتصال الشبكة والأمن مثل جدار الحماية وVPN وIPS / IDS

ج. إجراءات استخدام خدمة الشبكة لتقييد الوصول إلى خدمات الشبكة أو التطبيقات، عند الضرورة.

فصل الشبكات:

١. تقسم عمادة تقنية المعلومات والتعليم الالكتروني شبكة جامعة حائل إلى قطاعات أو مناطق أو مجالات منطقية بناء على المعايير التالية، على سبيل المثال لا الحصر:

أ. متطلبات الوصول (على سبيل المثال، الإدارة، القسم، الأكاديمية، الموظفون، تقنية المعلومات، الطلاب، الأطراف الثالثة).

ب. التكلفة النسبية وتأثير الأداء على دمج التكنولوجيا المناسبة.

ج. قيمة وتصنيف المعلومات المخزنة أو المعالجة في الشبكة (على سبيل المثال، حرجة، حساسة).

د. مستويات الثقة (على سبيل المثال، DMZ. Internet Trusted

ه. خطوط العمل (مثل الخدمة والدعم).

٢. تم فصل الشبكة الداخلية عن الشبكة الخارجية مع وجود ضوابط أمنية مختلفة لمحيط كل شبكة.

سياسات وإجراءات نقل المعلومات:

١. يجب تحديد ضوابط رسمية تحكم مدى أهمية المعلومات لحماية نقلها من خلال استخدام مرافق الاتصالات. ويجب أن يخضع نقل المعلومات السرية لحماية تتناسب مع مدى سريتها.

٢. يجب على جميع المستخدمين أن يقوموا بإنشاء البيانات الورقية أو الإلكترونية وتخزينها وتعديلها ونسخها وحذفها

٣. أو إتلافها بطريقة تتماشى مع سياسات جامعة حائل التي تحكم وتحمي سرية هذه البيانات وسلامتها وتوفرها.

٤. يجب على مالكي الأصول ضمان تطبيق واتباع الآليات المناسبة لحماية نقل معلوماتهم.

اتفاقيات نقل المعلومات:

قبل نقل المعلومات إلى جهة خارجية يجب التوصل إلى اتفاقية رسمية ملائمة لمستوى الخدمة ويحدد بموجبها مستوى الضوابط الأمنية المناسبة لنقل هذه المعلومات حيث تشتمل هذه الاتفاقية على سبيل المثال لا الحصر على ما يلي:

أ. مسؤوليات الإدارة.

ب. التبادلات اليدوية والإلكترونية.

ج. حساسية المعلومات الهامة التي يتم تبادلها.

د. متطلبات الحماية.

هـ. متطلبات الإخطار.

و. معايير التغليف والنقل.

ز. تحديد ساعي لنقل المعلومات

ح. المسؤوليات والالتزامات.

ط. ملكية البيانات والبرامج.

ي. مسؤوليات الحماية والتدابير

ك. متطلبات التشفير.

المراسلة الإلكترونية:

يجب وضع ضوابط أمنية لحماية الرسائل الإلكترونية (على سبيل المثال، البريد الإلكتروني من الوصول غير المصرح به أو التعديلات أو رفض الخدمة.

اتفاقية السرية أو عدم الإفصاح:

١. يتم تحديد المتطلبات المتعلقة بالسرية والتزامات عدم الإفصاح (بالنسبة لموظفي الجامعة والأطراف الثالثة) ومراجعتها بانتظام. وعلى عمادة تقنية المعلومات والتعليم الإلكتروني بالتعاون مع إدارات الدعم المختلفة (على سبيل المثال، مسؤول أمن المعلومات، مكتب إدارة المشاريع، إدارة الموارد البشرية / الوحدة الإدارية والإدارة القانونية) أن تقوم بما يلي:
   أ. تحديد المعلومات المراد حمايتها ومستويات الحساسية المطلوبة.
   ب. تحديد المدة المتوقعة للالتزام.
   ج. تحديد شروط إرجاع أو إتلاف المعلومات عند إنهاء الالتزام.
   د. تحديد المسؤوليات والمتطلبات المتعلقة بالتوقيع من أجل منع الكشف غير المصرح به للمعلومات.
   ه. نشر العقوبات المطبقة في حالة فشل المستخدم في احترام الالتزام.
٢. يجب أن تراعي التزامات السرية وعدم الإفصاح الشروط القانونية المعمول بها في جامعة حائل من أجل تلبية متطلبات حماية أصول الجامعة.