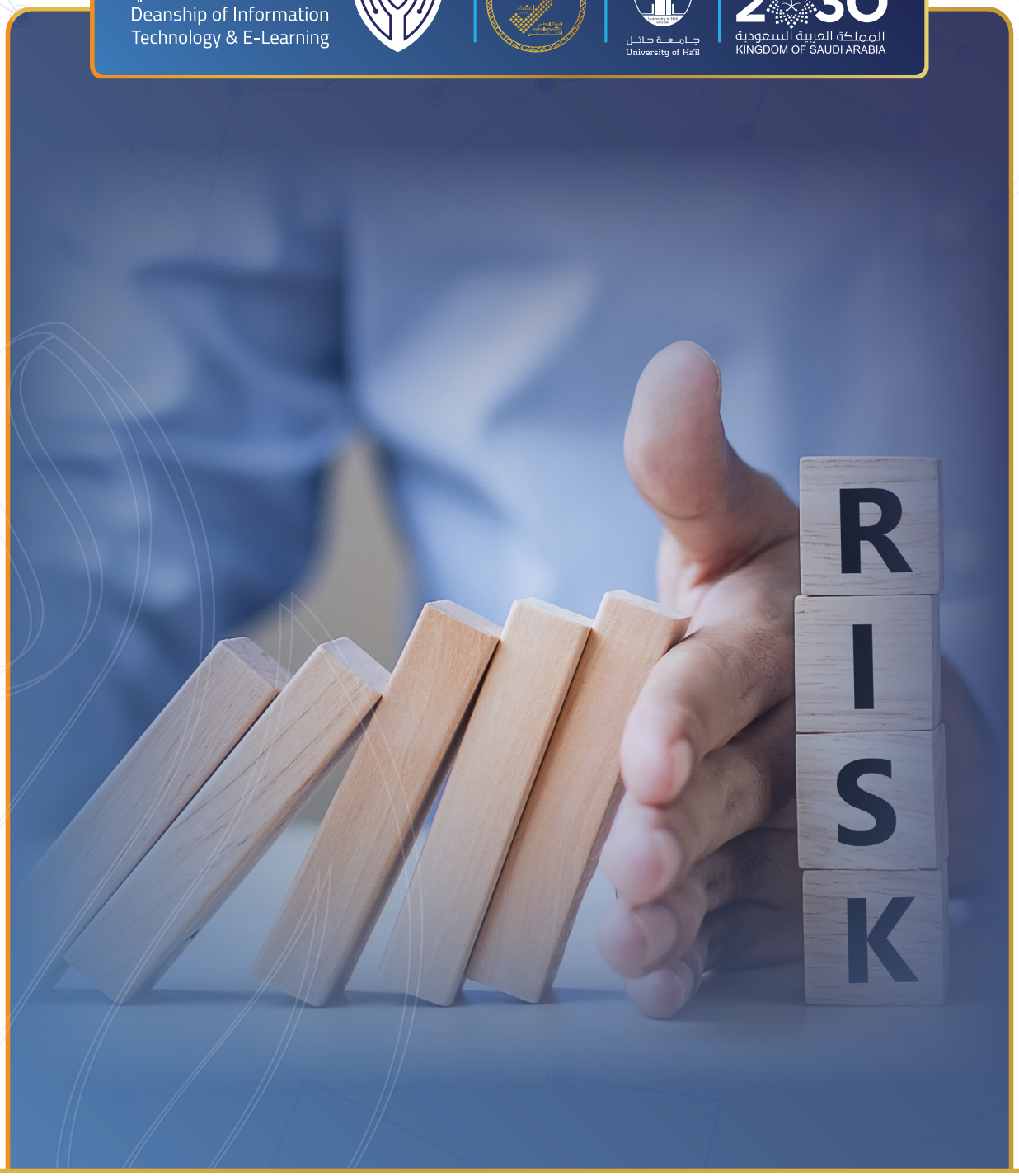
عمادة تقنية المعلومات
والتعليم الإلكتروني
Deanship of Information
Technology & E-Learning

معتمد
ACCREDITED

جامعة حائل
University of Ha'il

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA



سياسة إدارة المخاطر

بجامعة حائل

2023/2022م


بسم الله الرحمن الرحيم

سياسة إدارة المخاطر 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.

جميع الحقوق محفوظة لعمادة تقنية المعلومات والتعليم الإلكتروني.

الرقابة على الوثيقة

معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة إدارة المخاطر	عام	2.0	معتمدة

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

الاعـــــتماد

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.

الغـــرض:

الغرض الرئيسي من سياسة إدارة المخاطر هو:

تحديد مجالات ضعف أمن المعلومات والتهديدات داخل بيئة جامعة حائل وبدء العلاج المناسب لها.

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.

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 أمني يشير إلى ضرورة التعرف على الأفراد وتحميلهم مسؤولية أفعالهم.
الأصول	المعلومات التي تعتبر ذات قيمة للمؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام المعلومات.
المراجعة	فحص الحقائق لإبداء الرأي وقد يشتمل هذا الفحص على دليل اختباري يؤيد الرأي.
توفر	الحالة التي يكون فيها الأصل أو الخدمة قابلة لأن تصلها جهة مصرح لها بذلك وقابلة لأن تستخدمها أيضا.
السرية	حالة الأصل أو الخدمة القابلة للوصول وقابلة للاستخدام عند الطلب من قبل جهة معتمدة.
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. ويشمل أمن المعلومات وسائل أخرى مثل التحقق والمساءلة وعدم التنصل والموثوقية
السلامة	الحفاظ على الأصول والتأكد من دقتها وتناسقها طوال دورة حياتها بأكملها.
المالك	أي شخص أو مجموعة من الأشخاص حددتهم الإدارة لتحمل مسؤولية الحفاظ على سرية الأصول وتوفرها وسلامتها. وقد يتغير المالك أثناء دورة حياة الأصل.
السياسة	خطة عمل يسترشد بها عند اتخاذ القرارات والإجراءات. وتشتمل السياسة على 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).
تحليل المخاطر	استخدام المعلومات بطريقة منهجية لتحديد المصادر وتقدير المخاطر.
تقدير المخاطر	العملية الشاملة لتحليل المخاطر وتقويمها، حيث يعرف تحليل المخاطر بأنه الطريقة النظامية لتحديد مدى تعرض المنظمة الحالة عدم يقين وتقدير المخاطر الناشئة عن ذلك.
تقويم المخاطر	عملية مقارنة المخاطر المقدرة بمعايير مخاطرة موضوعة سلفا لتحديد حجم المخاطرة.
إدارة المخاطر	تنسيق الأنشطة الإدارة المنظمة والسيطرة عليها في حال وجود مخاطر. وهي عادة تشمل تقييم المخاطر ومعالجتها وقبولها ونقلها
معالجة المخاطر	عملية اختيار تدابير لتغيير المخاطر أو تعديلها أو تقليلها وتنفيذ تلك التدابير
الجهة الثالثة	الشخص أو الجهة المعترف بها على أنها مستقلة عن الأطراف المعنية، فيما يتعلق بالمسألة قيد النظر.
التهديد	احتمال التسبب في حادثة غير مرغوب فيها قد تؤدي إلى إلحاق الضرر بنظام من الأنظمة ومن أمثلة ذلك الكشف بطريقة غير مصرح بها عن معلومات حساسة أو أصول أو خدمات أو إتلافها أو إزالتها أو تعديلها أو قطعها أو احتمال التسبب في إصابة أشخاص. وقد يكون التهديد متعمدا أو عرضيا أو طبيعي الأصل.
الهشاشة	ضعف في الإجراءات الأمنية أو العمليات أو الضوابط أو أصول المعلومات النظام والتطبيق) حيث يمكن استغلال هذا الضعف عن طريق اللجوء إلى التهديد بالوصول غير المصرح به إلى المعلومات أو تعطيل المعالجة المهمة لها.
النظام	جهاز أو نظام مترابط أو أنظمة فرعية تتكون من أجهزة 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:

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر المالك إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية. يجب إجراء التغييرات في هذه السياسة بشكل حصري من قبل ضابط أمن المعلومات والموافقة عليها من قبل الإدارة. ويجب أن يظل سجل التغيير محدثا بحيث يتم تحديثه بمجرد إجراء أي تغيير..

الإنفاذ والامتثال:

يعد الالتزام بهذه السياسة إلزاميا ويجب مراجعته بشكل دوري من قبل ضابط أمن المعلومات. ويجب على جميع وحدات جامعة حائل (من العمادة، الإدارة، الكلية، القسم والمراكز) 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 توجهات الأمن ومخالفتها مما يؤدي إلى اتخاذ إجراءات تأديبية أو تصحيحية بحقهم (مثل الفصل من الخدمة) ويمكن أن يخضعوا لتحقيقات قانونية.

يجب ضمان معاملة صحيحة وعادلة للموظفين الذين يشتبه في انتهاكهم للأوامر الأمنية (مثل الإجراءات التأديبية). يجب إبلاغ إدارة الموارد البشرية والتعامل مع انتهاكات السياسة لمعالجة انتهاكات السياسة.

الاستثناءات:

يجب أن ينظر أمن المعلومات في الاستثناءات من هذه السياسة على أساس فردي. ويجب أن يشفع كل طلب استثناء من الامتثال لهذه السياسة بالمبررات المنطقية التي دعت لتقديمه على أن يوافق ضابط أمن المعلومات على هذا الاستثناء وتعتمده عمادة تقنية المعلومات والتعليم الالكتروني. ويجب أن يشمل كل طلب استثناء المبررات والمزايا التي تنسب إليه.

تبلغ فترة الاستثناء أربعة أشهر كحد أقصى. ويجوز تمديده لمدة أقصاها ثلاث فترات متتالية وذلك بعد إعادة تقييمه واعتماده. ولن يجدد أي استثناء لأكثر من ثلاث فترات متتالية.

الأدوار والمسؤوليات (مصفوفة المهام RACI):

يوضح الجدول مصفوفة المهام (RACI) التي تحدد من هو المساعل أو المسؤول أو الذي يتم استشارته أو إبلاغه بكل مهمة تحتاج إلى القيام بها. هناك بعض الأدوار المشاركة في هذه السياسة على التوالي: الإدارة، عمادة تقنية المعلومات والتعليم الالكتروني، موظف أمن المعلومات (ISO) والمالك.

المسؤوليات / الاسم	الإدارة	تقنية المعلومات	ضابط أمن المعلومات	المالك
إنفاذ سياسات أمن المعلومات داخل بيئة جامعة حائل لحماية الأصول الهامة.	R,A	C	C	C, I
مراجعة واعتماد تقارير تقييم المخاطر وخطة معالجة المخاطر وتقارير المراجعة.	R,A	C	C	C, I
مراجعة واعتماد معايير قبول المخاطر (المستوى المقبول للمخاطر) والمخاطر المتبقية.	R,A	C	C	C, I
إجراء وإدارة أنشطة إدارة المخاطر (على سبيل المثال، تحديد التهديدات ونقاط الضعف وتقييم BIA).	I	R	R,A	C
مراجعة والحفاظ على إجراءات إدارة المخاطر ومنهجيتها على أساس سنوي.		R	R,A	C
وضع خطة سنوية للتدقيق الداخلي لمراقبة تنفيذ إجراءات إدارة المخاطر.	I	R	R,A	C
إجراء تقييمات دورية للمخاطر تحدد نقاط الضعف الأمنية الحالية والمستقبلية، وتحديد مستوى المخاطر وتحديد أفضل الطرق لتقليل المخاطر إلى مستوى مقبول خطة معالجة المخاطر).	I	R	R,A	C
تطبيق الضوابط المناسبة لحماية سرية وسلامة وصحة المعلومات الحساسة		R,A	C	I
تطبيق الضوابط المناسبة لحماية النظم		R,A	C	I
تصنيف الأصول بناء على سياسة واجراءات إدارة الأصول.	I	C	C	R,A
تحديد قيمة للأصول	I	C	C	R,A

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 علاقات الموردين
- سياسة الامتثال.
- إجراءات إدارة المخاطر.
- إجراءات إدارة الأصول.
- منهجية إدارة المخاطر.

الملكية:

هذه الوثيقة مملوكة لعمادة تقنية المعلومات والتعليم الالكتروني بجامعة حائل وهي التي تحافظ عليها.

بيانات السياسة

تقدم الأجزاء الفرعية التالية بيانات السياسة في سبع جوانب رئيسة هي:

- الالتزام بإدارة المخاطر.
- متطلبات إدارة المخاطر.
- منهجية إدارة المخاطر.
- سجل المخاطر.
- تقييم المخاطر.
- معالجة المخاطر وقبولها.
- إدارة المخاطر.

الالتزام بإدارة المخاطر:

١. تتأكد الإدارة من تحديد المخاطر وإدارتها بطريقة فعالة وكفؤة وفي الوقت المناسب مع مراعاة تأثيرها على أعمال جامعة حائل.

٢. يجب تقييم المخاطر وإدارتها باعتبارها جزءا من جميع أنشطة جامعة حائل ذات الصلة (مثل وظائف الأعمال، والعمليات اليومية، واقتناء النظم، وتطويرها وتنفيذها، وتشغيل النظم وغيرها)، من خلال ضمان التنفيذ الفعال لسياسات واجراءات أمن المعلومات الخاصة بجامعة حائل.

متطلبات إدارة المخاطر:

١. يجب على مسؤول أمن المعلومات تحديد وتنفيذ إدارة المخاطر لضمان وجود حماية ذات تكلفة معقولة لجميع أنظمة جامعة حائل.

٢. تقوم إدارة المخاطر بتقييم التأثير المحتمل للأعمال، وتقييم التهديدات ونقاط الضعف واختيار الضوابط المناسبة لتلبية متطلبات أمن المعلومات الخاصة بالعمل بطريقة ذات تكلفة معقولة.

٣. يجب إكمال عملية إدارة المخاطر بطريقة منسقة تشمل جميع أصحاب المصلحة بما في ذلك أصحاب الأعمال ومالكي النظم والمحللين الأمنيين وغيرهم من خبراء الموضوعات

٤. تنفيذ إدارة المخاطر بطريقة مستقلة بحيث تتولى أمرها منظمات قائمة بذاتها ومفصولة عن تلك المسؤولة عن تشغيل أنظمة جامعة حائل.

٥. يجب إجراء عمليات تقييم مستقلة بواسطة موظفين مستقلين أو مقاولين أو بائعين بغرض تطبيق معايير تقييم دقيقة على الأصول حيثما اقتضى الأمر (مثل الإدارة المستقلة للمخاطر، ومراجعة الرموز بصورة مستقلة، واعتماد الاختبار الأمني المستقل، واختبار الاختراق بصورة مستقلة، ومسوحات الهشاشة).

منهجية إدارة المخاطر:

١. يجب على ضابط أمن المعلومات إعداد منهجية إدارة المخاطر والإشراف عليها وعلى سياساتها وإجراءاتها لحماية أنظمة جامعة حائل بشكل مستمر. ولابد أن تستند منهجية إدارة المخاطر وسياساتها وإجراءاتها إلى معايير وارشادات مقبولة دولية (مثل ISO/IEC 27001: 2013 و ISO/IEC 27005: 2011).

٢. يجب على إدارة جامعة حائل القيام بما يلي:

أ. تحديد نطاق تقييم المخاطر التي تتعرض لها الأصول.

ب. التأكد من وجود تدابير مناسبة لإدارة المخاطر والمبادرات الاستراتيجية، ومواءمتها مع أهداف الجامعة.

ج. دعم تدابير إدارة المخاطر واستراتيجيتها بهيكل تنظيمي مناسب؛ والتأكد من أن المسؤوليات المرتبطة بإدارة المخاطر محددة بوضوح وتبلغ إلى جميع المستويات.

د. التأكد من أن المخاطر يبلغ عنها من خلال هيكل تقارير واضح وقوي.

ه. دمج أنشطة إدارة المخاطر الجارية مع أنشطة إدارة المخاطر الأخرى في أعمال جامعة حائل.

٣. تشمل منهجية إدارة المخاطر الجوانب التالية:

أ. تحديد وتصنيف الأصول

ب. تحديد قيمة الأصول.

ج. تحديد وتقييم التهديدات العملية على البنية التحتية لجامعة حائل وبيئتها.

د. تحديد وتقييم مدى تعرض الأصول للتهديدات المحددة.

ه. تحديد الخطر (أي العواقب المتوقعة الناجمة عن أنواع محددة من الهجمات على أصول محددة).

و. تحديد طرق للحد من هذه المخاطر ومعالجتها.

ز. وضع أولويات تدابير الحد من المخاطر بناء على خطة استراتيجية.

سجل المخاطر:

١. يقوم ضابط أمن المعلومات بالتنسيق مع موظفي عمادة تقنية المعلومات والتعليم الإلكتروني بإنشاء سجل للمخاطر والاحتفاظ به لتسجيل كل خطر تم تحديده في إطار عملية تقييم المخاطر. قد يتضمن هذا السجل، على سبيل المثال لا الحصر ما يلي:

أ. وصف للمخاطر (أسبابها وآثارها بالتفصيل).

ب. تقييم كامل للمخاطر.

ج. تصنيف كامل للمخاطر.

د. الخطوط العريضة لعناصر التحكم الموجودة.

ه. تقييم لعواقب المخاطر.

و. تصنيف المخاطر المتبقية.

ز. توصية حول كيفية إدارة المخاطر بشكل أكثر فاعلية.

ح. قائمة بالإجراءات العلاجية مدرجة خطة بهذا الأمر (تذكر فيها الإجراءات والقائمين على أمر تنفيذها، والقيد الزمني للتنفيذ).

ط. تقرير عن التقدم المحرز في إدارة المخاطر.

تقييم المخاطر:

١. يجب إجراء تقييم للمخاطر بالنسبة للأنظمة الجديدة وعمليات الاستحواذ والعقود والمشاريع الجديدة والعقود الحالية وتغييرات العقود لضمان تحديد أي مخاطر أو فرص لاحقة وتحليلها والإبلاغ عنها إلى المستوى الإداري المناسب وفقا للهيكل التنظيمي لوحدة المراجعة الداخلية.

٢. يجب أن يعالج تقييم المخاطر المحتملة على الفوائد التجارية المتوقعة للوحدة والامتثال للمتطلبات القانونية ذات الصلة:

أ. فهم التقييم التصنيفي الأمني للأنظمة.

ب. تحديد نقاط الضعف ذات الصلة الموجودة داخل النظم ومرافق معالجة المعلومات.

ج. تحديد التهديدات الماثلة أمام معلومات جامعة حائل وأنظمتها ومرافق معالجة المعلومات الخاصة بها.

د. تحديد الضوابط الأمنية المطلوبة للأنظمة (بناء على نوع النظام وطريقة تصنيفه أمنية). تؤخذ هذه الضوابط من سياسات أمن المعلومات الخاصة بجامعة حائل ومن معايير النظام المحددة وغيرها من أفضل الممارسات ذات الصلة.

ه. تقييم حالة عناصر التحكم هذه من خلال المناقشات مع أصحاب المصلحة المعنيين أو إجراء تقنيات اختبار الأمان المناسبة.

معالجة المخاطر وقبولها:

١. تعتبر معالجة المخاطر عملية مستمرة تقلل من المخاطر من خلال تنفيذ التدابير الأمنية الفعالة من حيث التكلفة. يجب أن تأخذ عملية معالجة المخاطر في الاعتبار ما يلي:
   أ. اختيار الضوابط المناسبة التي تقلل من التعرض للخطر.
   ب. تعيين ترتيب للأولويات لتنفيذ التدابير المضادة المناسبة.
   ج. إسناد المسؤولية عن تنفيذ التدابير المضادة المناسبة.
   د. تنفيذ وتوثيق التدابير المضادة المناسبة.

٢. يجب على الإدارة تحديد معايير قبول المخاطر، التي يقررونها، والمستوى المقبول للمخاطرة، والمخاطر الحالية والمخاطر المتبقية، وتقر بوجود بعض المخاطر حتى بعد تطبيق الضوابط.

٣. إذا كان مستوى المخاطر المتبقية غير مقبول، فيجب تطبيق ضوابط إضافية لخفضها المستوى مقبول.

٤. يجب مراعاة ما يلي بعد تنفيذ إجراء معالجة المخاطر
   أ. مراجعة أي ملاحظات تم تحديدها نتيجة لعلاج المخاطر من حيث فعاليتها وتأثيرها على جامعة حائل.
   ب. تحديد الأفراد أو العمليات أو الإجراءات أو المبادرات العلاجية المناسبة المتعلقة بالتقنية، وتبليغها للجهة الإدارية ذات الصلة في الجامعة، واعتمادها وتنفيذها على نحو فعال.

الاهتمام بإدارة المخاطر ومراجعتها:

١. يجب وضع خطة مراجعة داخلية سنوية لرصد تنفيذ إجراءات إدارة المخاطر. وفي إطار برنامجها السنوي للمراجعة تقوم وحدة المراجعة الداخلية بتقييم ما يلي:
   أ. مدى تنفيذ وفعالية الضوابط التي أوصى بها تقييم وعلاج المخاطر.
   ب. وجود خطة لعلاج المخاطر في كل وظيفة تخضع للمراجعة
   ج. دمج خطة معالجة المخاطر بشكل مناسب مع وثائق التخطيط الأخرى، وهي محدثة وتراجع بشكل منتظم.

٢. يجب أن ترفع المراجعة الداخلية تقارير عن قضايا إدارة المخاطر إلى الإدارة والأطراف المعنية الأخرى وذلك في إطار التقارير العادية التي تعد بعد أي عملية مراجعة.

٣. يقوم موظف أمن المعلومات بالتعاون مع موظفي عمادة تقنية المعلومات والتعليم الإلكتروني - من خلال مجموعة من الأليات - بمراجعة إجراءات ومنهجية إدارة المخاطر سنوية والحفاظ عليها. وقد تشمل الآليات، على سبيل المثال لا الحصر ما يلي:
   أ. ملاحظات الموظفين.
   ب. المسوحات المستهدفة.
   ج. المقابلات مع المديرين بخصوص التخطيط لإدارة المخاطر.
   د. تقييم طبيعة الاستفسارات وعدد مرات تكرارها.

٤. يجب إعادة تقييم وتحديث جميع المخاطر على النحو التالي:
   أ. في كل سنة على الأقل بعد آخر تقييم المخاطر.
   ب. بعد الحصول على نتائج مهمة إثر المراجعة.
   ج. كلما خضع الأصل لتحسينات أو تعديلات كبيرة.
   د. بعد وقوع حادث ينتهك سياسات أمن المعلومات الخاصة بجامعة حائل ويعرض سلامة.
   ه. أصولها أو توفر هذه الأصول أو سريتها للخطر.

RISK