سياسة إدارة الأصول

الإصدارة ١ .١

رقم السياسة:

١. جدول المحتويات

٢. معلومات ذات ملكية فكرية

هذه الوثيقة هي عبارة عن معلومات خاصة بعمادة تقنية المعلومات والاتصالات في جامعة الإمام عبد الرحمن بن فيصل، وهي تعتبر سرية ولا يسمح بالاضطلاع عليها إلا للقراء للذين يحق لهم ذلك. كما لا يسمح بتوزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة تقنية المعلومات والاتصالات ..

٣. الرقابة على الوثيقة

معلومات عن الوثيقة

العنوان	التصنيف	الإصدارة	الحالة
سياسة إدارة الأصول	سري	١.١	معتمدة

تاريخ الإعداد

الإصدارة	المؤلف/ المؤلفون	تاريخ الاصدار	التغييرات
0.1	علاء عليوه	17نوفمبر 2014	إعداد
0.2	نبيل البحبوح	30نوفمبر 2014	مراجعة
0.3	أسامة العمري	23ديسمبر 2014	QA
١.0	نبيل البحبوح	31ديسمبر 2014	تحديث
١.١	منيب أحمد - تقنية المعلومات والاتصالات بجامعة الإمام عبد الرحمن بن فيصل	21أبريل 2017	تحديث

مراجعة والتحقق والموافقة

الاسم	العنوان	التاريخ
لمياء عبد الله الجعفري	مدير الجودة	
الدكتور خالد العيسى	عميد تقنية المعلومات والاتصالات	

قائمة التوزيع

عدد النسخ	المستفيدين	الموقع

٤. نظرة عامة على السياسة

يستعرض هذا الجزء بالتفصيل الغرض من هذه السياسة ونطاقها ومصطلحاتها وتعاريفها، وتغييرها، ومراجعتها وتحديثها، وإنفاذها والامتثال لها، والتنازل، والأدوار والمسؤوليات، والمستندات ذات الصلة والملكيّة.

٥. ٤. ١الغرض

الغرض من سياسة إدارة الأصول هو:

تحديد الأصول التنظيمية لجامعة الإمام عبد الرحمن بن فيصل وتحديد المسؤوليات المناسبة لحمايتها، وضمان تلقي المعلومات مستوى مناسب من الحماية وفقًا لأهميتها بالنسبة لجامعة الإمام عبد الرحمن بن فيصل، ومنع الكشف غير المصرح به للمعلومات المخزنة على الوسائط أو تعديلها أو إزالتها أو إتلافها.

٦. النطاق

تنطبق بيانات السياسة المكتوبة في هذه الوثيقة على جميع موارد جامعة الإمام عبد الرحمن بن فيصل بجميع مستويات حساسيتها؛ بما فيها:

- جميع الموظفين بدوام كامل وبدوام جزئي والموظفين المؤقتين الذين يعملون لدى الجامعة، أو يعملون لصالحها أو بالنيابة عنها.
- الطلاب الذين يدرسون في جامعة الإمام عبد الرحمن بن فيصل
- المقاولون والاستشاريون الذين يعملون لصالح جامعة الإمام عبد الرحمن بن فيصل أو نيابة عنها
- جميع الأفراد والجماعات الأخرى الذين تم منحهم إمكانية الوصول إلى أنظمة تقنية المعلومات والاتصالات في جامعة الإمام عبد الرحمن.

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

المصطلحات والتعريفات

يوفر الجدول ١ تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة

المصطلح	التعريف
المساءلة	مبدأ أمني يشير إلى وجوب تحديد هوية الأفراد وتحميلهم مسؤولية أفعالهم.
الأصل	معلومات ذات قيمة للمؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام المعلومات.
توفّر	الحالة التي في ظلها تحصل جهة مصرّح لها على أصل من الأصول أو خدمة من الخدمات وتستطيع استخدامها عند الطلب.
السرية	عدم إتاحة أصل من الأصول أو خدمة من الخدمات لأفراد أو كيانات أو عمليات غير مصرح بها.
الرقابة	وسيلة لإدارة المخاطر، بما في ذلك السياسات والإجراءات والإرشادات التي يمكن أن تكون ذات طبيعة إدارية أو تقنية أو إدارية أو قانونية.
الإرشاد	وصف لمتطلبات تحقيق الأهداف المحددة في السياسات وطريقة القيام بهذه المتطلبات.
حادث	الهشاشة والمهددات تؤديان معا إلى وقوع حادث. ويشار إلى حادث أمن المعلومات من خلال واحدة أو سلسلة من أحداث أمن

	المعلومات غير المرغوب فيها أو غير المتوقعة التي تتميز بأن احتمال مساسها بعمليات الشغل وتهديد أمن المعلومات كبير.
أمن المعلومات	الحفاظ على سرية المعلومات وسلامتها وتوافرها. ويشمل أمن المعلومات استخدام خصائص أخرى تتعلق بها مثل الأصالة والمساءلة وعدم التنصل والموثوقية.
السلامة	الحفاظ على وتأكيد دقة وتناسق الأصول طوال دورة حياتها بأكملها.
وضع الديباجات	تثبيت ملصق فعلي أو إلكتروني يحدد فئة الأمان الخاصة بمستند أو ملف أو سلسلة سجلات من أجل تنبيه من يتعاملون معها إلى أنها تتطلب حماية على المستوى القابل للتطبيق.
صاحب	أي شخص أو مجموعة من الأشخاص تحددهم الإدارة لتحمّل مسؤولية الحفاظ على سرية الأصول وتوافرها وسلامتها. قد يتغير المالك أثناء دورة حياة الأصل.
سياسة	خطة عمل لتوجيه القرارات والإجراءات. وتتضمن عملية السياسة تحديد البدائل المختلفة مثل البرامج أو أولويات الإنفاق، واختيار البديل الملائم من بينها على أساس التأثير الذي سيحدثه.
خطر	مزيج من عواقب الحدث (بما في ذلك التغييرات في الظروف) واحتمال حدوثها.
نظام	جهاز أو نظام مترابط أو أنظمة فرعية من المعدات تُستخدم 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.
طرف ثالث	الشخص أو الجهة المعترف باستقلالها عن الأطراف المعنية، فيما يتعلق بالمسألة قيد النظر.

الجدول ١: المصطلحات والتعاريف

٧. التغيير والمراجعة والتحديث

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر المالك إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية. ولا تجرى تغييرات في هذه السياسة إلا من قبل ضابط أمن المعلومات على تعتمد هذه التغييرات من قبل الإدارة. يجب أن يظل سجل التغيير محدثًا ويتم تحديثه بمجرد إجراء أي تغيير.

٨. النفاذ / الامتثال

يعد الامتثال لهذه السياسة أمراً إلزاميًا ويجب مراجعته بشكل دوري من قبل ضابط أمن المعلومات. ويجب على جميع وحدات الجامعة (من عمادات، وإدارات، وكليات، وأقسام، ومراكز) ضمان مراقبة الامتثال المستمر لهذه السياسة في نطاق وحداتهم.

وفي حالة تجاهل أو انتهاك توجيهات أمن المعلومات، يمكن أن تتضرر بيئة الجامعة (فعلى سبيل المثال، تفقد الجامعة الثقة فيها وتفقد سمعتها أو يتعطل فيها، أو تحدث فيها مخالفات قانونية). وفي هذه الحالة يكون الأشخاص المخطئون مسؤولين عما حدث مما يؤدي إلى اتخاذ إجراءات تأديبية أو تصحيحية بحقهم (مثل الفصل من الخدمة) ويمكن أن يخضعوا لتحقيقات القانونية.

يجب ضمان خضوع الموظفين الذين يشتبه في انتهاكهم للأوامر الأمنية لمعاملة صحيحة وعادلة (مثل الإجراءات التأديبية). ويجب إبلاغ إدارة الموارد البشرية لمعالجة المخالفات المتعلقة بهذه السياسة، والتعامل مع ما يحدث لها من انتهاكات.

٩. الاستثناءات

يجب أن ينظر أمن المعلومات في الاستثناءات المتعلقة بهذه السياسة على أساس فردي. وللموافقة على استثناء متعلق بها، يجب أن يرفق مع طلب الاستثناء ظروف العمل التي اقتضت التقدم به مشفوعة بالمبررات المنطقية لذلك. ويتعيّن أن يوافق ضابط أمن المعلومات على الاستثناءات من شرط الامتثال للسياسة وأن تعتمد عمادة تقنية المعلومات والاتصالات هذه الموافقة. ويجب أن يشمل كل طلب استثناء المبررات والمزايا المنسوبة إلى الاستثناء.

تبلغ فترة التنازل عن السياسة أربعة أشهر كحد أقصى، ويجب إعادة تقييمها واعتمادها – إذا اقتضى الأمر - لمدة أقصاها ثلاثة فترات متتالية. ولن يتم تقديم أي تنازل لأكثر من ثلاث فترات متتالية.

١٠. الأدوار والمسؤوليات (مصفوفة راكي)

يوضح الجدول (٢) مصفوفة راكي (RACI) [١] التي تحدد من هو الشخص المسؤول ومن هو الشخص المساءل وماهي الجهة التي ينبغي استشارتها أو إبلاغها بكل مهمة هناك حاجة للقيام بها. هناك بعض الأدوار المشاركة في هذه السياسة على التوالي: عمادة تقنية المعلومات والاتصالات، موظف أمن المعلومات، إدارة الموارد البشرية / الوحدة الإدارية (الموارد البشرية أو الشخص المساءل)، المالك والمستخدم (الموظفون، أعضاء هيئة التدريس ، الطلاب ، المقاولون ، الاستشاريون والثالث حفلات).

الأدوار / المسؤوليات	تقنية المعلومات	المسؤول عن أمن المعلومات	مدير الإدارة	المالك	المستعمل
الحفاظ على وتحديث مخزون الأصول لأصول IAU.	R,A	C		C	
تطبيق الضوابط المناسبة لحماية سرية وسلامة وتوافر وصحة المعلومات الحساسة.	R,A	C			
تخصيص ملكية الأصول للأصول الجديدة في بيئة IAU.	R	C		C,I	
إدارة وتحديث أصول المعلومات من IAU.	R				
إجراء وإدارة أنشطة إدارة المخاطر (مثل تصنيف الأصول).	C,I	R,A		I	
تصنيف الأصول بناءً على سياسة وإجراءات إدارة الأصول.	R,A	C		R	I
تعيين قيمة للأصول.	R,C	R,C		R,A	I
الالتزام بسياسات وإجراءات أمن المعلومات المتعلقة بحماية المعلومات	C	C	C		R,A,I
الإبلاغ عن الحوادث الأمنية الفعلية أو المشتبه بها لعمادة تقنية المعلومات والاتصالات.	A,C	C			R
التأكد من أن الموظف المستقيل أو المنتهي يعيد جميع أصول IAU المهتمة قبل إكمال عملية الإنهاء.	C	C	R,A		

[١] تصف 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 (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.

الأدوار / المسؤوليات	تقنية المعلومات	المسؤول عن أمن المعلومات	مدير الإدارة	المالك	المستعمل
إلغاء حقوق الوصول (المنطقية والمادية) للأصول عند إنهاء الموظف أو تغييره.	R,A	C	C		
تطبيق تدابير الأمان في حماية الوسائط القابلة للنقل والتخلص من المعلومات غير المستخدمة بطريقة آمنة.	R,A	C		R,I	

الجدول ٢: الأدوار والمسؤوليات المخصصة بناءً على مصفوفة *RACI*

الوثائق ذات الصلة

فيما يلي جميع السياسات والإجراءات ذات الصلة لهذه السياسة:

- سياسة أمن المعلومات
- سياسة التحكم في الوصول
- سياسة أمن العمليات
- سياسة أمن الاتصالات
- نظام اقتناء وتطوير وسياسة الصيانة
- سياسة إدارة حوادث أمن المعلومات
- سياسة الامتثال
- إجراءات تصنيف الأصول
- تغيير إجراءات الإدارة
- إجراءات إدارة المخاطر
- نظام اكتساب وتطوير وإجراءات الصيانة

١١. الملكية

هذه الوثيقة مملوكة وتحافظ عليها عمادة تقنية المعلومات والاتصالات بجامعة الإمام عبد الرحمن بن فيصل .

١٢. بيانات السياسية

تقدم الأجزاء الفرعية التالية بيانات السياسة في عشرة جوانب رئيسية هي:

- حصر الأصول
- ملكية الأصول
- الاستخدام المقبول للأصول
- عودة الأصول
- تصنيف المعلومات
- وصف المعلومات
- التعامل مع الأصول
- إدارة الوسائط القابلة للإزالة
- التخلص من وسائل الإعلام
- نقل الوسائط المادية

١٣. حصر الأصول

١. تحدد عمادة تقنية المعلومات والاتصالات عملية وإجراءات تسجيل وصيانة وتحديث القائمة التي تحصر فيها جميع أصول المعلومات (أي سجل الأصول) التي تملكها وتديرها الجامعة. ووفقًا لسياسة وإجراءات إدارة المخاطر فإنّ هذه القائمة تشمل تصنيفات لخمسة أنواع رئيسية هي: الأجهزة والبرامج والمعلومات والأفراد والخدمة.

٢. يجب أن تحتوي قائمة حصر الأصول على تحديد الأصول ووصفها وموقعها وتصنيفها وقيمتها وتسميتها ومالكها.

REF: [ISO/IEC 27001: A.8.1.1]

١٤. ملكية الأصول

١. تقوم عمادة تقنية المعلومات والاتصالات بتحديد مالك كل أصل من الأصول على أن يكون هذا المالك مسؤولاً عن تحديد تصنيفات الأصول؛ و حمايتها وإدارتها، ومعالجة الأصول الحرجة.

٢. لكل الأصول، يجب تحديد ما يلي:

الوظيفة	الوصف	المسؤوليات
مالك	مديرو الوحدات التنظيمية التي تتحمل المسؤولية الأساسية عن الأصول المرتبطة بسلطتها الوظيفية	▪ توزيع حقوق الوصول إلى الأصول التي كفلتها إدارة الجامعة. ▪ تصنيف الأصول. ▪ التأكد من وضع العلامات المناسبة فيما يتعلّق بالمعلومات الحسّاسة. ▪ التأكد من وجود ضوابط مناسبة لمعالجة سرية وسلامة وتوافر المعلومات. ▪ مراجعة تصنيف الأصول بشكل دوري. ▪ ضمان توفر المعلومات في جميع الأوقات والظروف. ▪ الإبلاغ عن ضوابط الأمن ومتطلبات الحماية لخادم المعلومات والمستخدم. ▪ تحديد ومراجعة قيود الوصول إلى المعلومات وتصنيفاتها بشكل دوري، مع مراعاة سياسات التحكم في الوصول المعمول بها. ▪ التحديد والمراجعة الدورية لجداول النسخ الاحتياطي، وجداول الاستعادة، ونتائج اختبار النسخ الاحتياطي والاستعادة وسلامة البيانات بعد الاستعادة.
وصي	المديرون والمسؤولون ومقدمو الخدمات، والمعينين بواسطة مالك المعلومات لإدارة أصول المعلومات أو معالجتها أو تخزينها	▪ حماية معلومات الجامعة لضمان سريتها وسلامتها وتوافرها. ▪ تطبيق سياسات أمن المعلومات وأفضل الممارسات على المعلومات. ▪ تحديد وتوثيق متطلبات الوصول المصرح به إلى المعلومات. ▪ أداء أنشطة النسخ الاحتياطي واختبار صحة البيانات بانتظام. ▪ كشف المخالفات الأمنية والتّعامل معها ▪ مراقبة الامتثال لسياسات أمن المعلومات وأفضل الممارسات. ▪ إبلاغ المالك عن أي انتهاكات أمنية مشتبه بها أو

		فعلية، والتغرات الأمنية، والحوادث التي تعرض المعلومات للخطر. ▪ الحصول على موافقة مسبقة من المالك قبل تبادل المعلومات. ▪ أداء المهام الإدارية العادية.
مستخدم	الأفراد أو المجموعات أو المنظمات التي أذن لها المالك بالوصول إلى الأصول	▪ فهم تصنيفات أصول المعلومات، والالتزام بضوابط الأمان المحددة من قبل المالك والتي طبقها الوصي. ▪ الحفاظ على تصنيف الأصول ووضع الديباجات التي خصصها لها المالك. ▪ الاتصال بالمالك عندما تكون المعلومات غير مميزة أو التصنيف غير معروف. ▪ استخدام المعلومات فقط للأغراض المعتمدة من الجامعة. ▪ إبلاغ الوصي أو المالك بأي مخالفات أمنية فعلية أو مشتبه بها، والثغرات الأمنية، وحوادث المعلومات للخطر.

[ISO/IEC 27001: A.8.1.2]

١٥. الاستخدام المقبول للأصول

١. تحدد عمادة تقنية المعلومات والاتصالات "سياسة الاستخدام المقبول" التي توفر إرشادات لإدارة الأصول. ولا تفرض هذه السياسة قيوداً تتعارض مع ثقافة الانفتاح والثقة والنزاهة.

٢. تستخدم جميع أصول الجامعة لأغراض العمل على النحو المحدد في سياسة أمن المعلومات.

٣. على جميع موظفي جامعة الإمام عبد الرحمن بن فيصل:

ا. أن يقروا بالحاجة إلى حماية معلومات الجامعة؛ وأن ينفذوا أنشطتهم اليومية وفقًا لسياسة أمن المعلومات.

ب. لا يجوز المشاركة في أنشطة غير قانونية مثل الوصول غير المصرح به للأصول أو القرصنة أو إدخال أي ملوّثات ا أو فيروسات إلى الحاسب الآلي أو ارتكاب أعمال قد تؤدي إلى تعطيل استخدام الأصول.

٤. .تقوم عمادة تقنية المعلومات والاتصالات بمراقبة أو تسجيل أو تدقيق استخدام أي من معلوماتها وأنظمة الاتصالات السلكية واللاسلكية والمعدات الخاصة بها بشكل دوري. يجب الإبلاغ عن إساءة استخدام فعلية أو مشتبه بها لهذه الأنظمة إلى ممثل عمادة تقنية المعلومات والاتصالات المناسب في الوقت المناسب.

REF: [ISO/IEC 27001: A.8.1.3]

١٦. إعادة الأصول

١. تتأكّد إدارة الموارد البشرية وعمادة تقنية المعلومات والاتصالات والإدارات ذات الصلة من أنّ جميع العاملين في جامعة الإمام عبد الرحمن بن فيصل يقومون بإرجاع جميع الأصول التي بحوزتهم ولكنه مملوكة للجامعة (مثل ، أجهزة الحاسب المحمولة والمكتبية والطابعات وما إلى ذلك) عند إنهاء خدمتهم أو عقودهم أو الاتفاقيات المبرمة معهم وفقًا لإجراءات التخليص. قد يشمل ذلك، على سبيل المثال لا الحصر:

ا. عملية إرجاع رسمية لأصول الجامعة (على سبيل المثال، قوائم المراجعة مقابل الأصول المحصورة).

ب. عملية إعادة أو إتلاف رسمي لأي نوع من معلومات جامعة الإمام عبد الرحمن بن فيصل.

ج. مراعاة متطلبات الإزالة الآمنة للبرامج والمعلومات التي تخص جامعة الإمام عبد الرحمن بن فيصل عندما يستخدم الموظفون أجهزتهم الشخصية.

٢. خلال فترة إشعار الموظف بإنهاء خدمته، يجب أن تتحكم عمادة تقنية المعلومات والاتصالات في النسخ غير المصرح بها لأي معلومات متعلقة بجامعة الإمام عبد الرحمن بن فيصل ، مثل البرامج والمعلومات المتعلقة بالعمل والبيانات الحساسة.

REF: [ISO/IEC 27001: A.8.1.4]

١٧. تصنيف المعلومات

١. تحدد عمادة تقنية المعلومات والاتصالات تصنيفات المعلومات بناءً على حساسيتها وأهميتها وسريتها ومتطلبات خصوصيتها وقيمتها.

٢. تصنف جميع المعلومات التي يتم إنشاؤها بواسطة جامعة الإمام عبد الرحمن بن فيصل أو من أجلها سواء كانت ورقية أو إلكترونية أو على أي شكل آخر إلى أربعة مستويات هي معلومات سريّة للغاية، وأخرى سرية بالإضافة إلى معلومات داخلية وأخرى عامّة وفيما يلي تفاصيلها:

التصنيف	الوصف
1.سري للغاية	ينطبق هذا التصنيف على معلومات العمل الحساسة للغاية والمخصصة للاستخدام داخل جامعة الإمام عبد الرحمن بن فيصل وإفشاؤها غير المصرح به بتاتاً لما له من تأثير خطير على الأهداف الإستراتيجية طويلة المدى للجامعة أو يعرض بقاؤها للخطر. إنّ إفشاء هذه المعلومات يؤثر بشكل خطير وعكسي على الجامعة وأصحاب المصلحة فيها ولذا قد تطبق إجراءات قانونية عند كشف هذه المعلومات أو تبادلها بطريقة غير مصرح بها. يطلب الوصول إلى هذه البيانات بشكل فردي ومن يقوم بالتصريح بالوصول إليها هو مالك المعلومات المسؤول عن البيانات. وفي هذه الحالة مالك المعلومات هو الذي يقوم بتقييم المخاطر المحتملة قبل الموافقة على الوصول إليها. ومن أمثلة هذه المعلومات: المعلومات الصحية المحمية، المعلومات التي تعرف بالطالب، السجلات المالية للإدارة، المعلومات الخاصة التي تتعلق بالموظفين ، تفاصيل الائتمان والحسابات المصرفية ، بروتوكولات البحوث التعاقدية والاتصالات الإدارية.
2. سري	ينطبق هذا التصنيف على المعلومات الحساسة المعدة للاستخدام داخل جامعة الإمام عبد الرحمن بن فيصل والإفصاح عنها غير مصرح به لما له من تأثير كبير على المدى القصير على العمليات أو الأهداف التكتيكية. يحدد مالك المعلومات التدابير الأمنية اللازمة للحماية من الوصول أو التعديلات أو الكشف غير المصرح به. و من أمثلة هذه المعلومات: الملكية الفكرية المرخصة و / أو قيد التطوير، معلومات عن المشتريات، عقود البيع، تكوين النظام، سجلات النظام، تقارير المراجعة الداخلية، تقارير تقييم المخاطر، طلبات تقديم عروض وطلبات تقديم معلومات.
3. داخلي	ينطبق هذا التصنيف على جميع معلومات العمل التي تم إصدارها كتواصل داخلي أو دائري وله تصنيف أقل حساسية من "سري". يمكن اعتبار أي معلومات أخرى لم يتم تمييزها بشكل صريح "سرية أو عامة" على أنها "استخدام داخلي فقط". في حين أن الكشف غير المصرح به يتعارض مع السياسة، فقد يتسبب في إحراج بسيط أو إزعاج تشغيلي بسيط، وليس من المتوقع أن يؤثر هذا الأمر على نحو خطير أو سلبي على الجامعة وموظفيها وأصحاب المصلحة مثلما سيؤثر تسرب المعلومات السرية. يجب تطبيق مستوى معقول من التدابير الأمنية على المعلومات الداخلية. ومن أمثلة ذلك: المراسلات الروتينية، والنشرات الإخبارية للموظفين، والمذكرات الداخلية، والسياسات والإجراءات الداخلية ، والمواد والكتيبات التدريبية ، وتعاميم الموظفين الداخليين.

4. عام	ينطبق هذا التصنيف على جميع المعلومات الأخرى التي لا تتناسب بوضوح مع أي من التصنيفين أعلاه. بالإضافة إلى ذلك، تمت الموافقة عليها صراحةً من قبل إدارة الجامعة باعتبارها مناسبة للنشر العام. بحكم التعريف، لا يوجد شيء مثل الكشف غير المصرح به لهذه المعلومات، ويمكن نشره بحرية دون التسبب في أي ضرر محتمل لوحدة الرقابة الداخلية. مثال: الكتيبات والنشرات الجديدة والنشرات والمواقع الإلكترونية ودليل هاتف الموظفين والمواد التسويقية.

١. بالنسبة لجميع أنواع المعلومات الحالية، يكون المالك المعين مسؤولاً عن اختيار مستوى تصنيف المعلومات المناسب وفقًا لمتطلبات أعمال الجامعة.

٢. عند الجمع بين مختلف تصنيفات حساسية المعلومات، يتم تصنيف عملية جمع المعلومات الناتجة على أعلى مستوى مقيد بين المصادر.

٣. يجب على جميع موظفي الجامعة الالتزام بخطة تصنيف المعلومات المحددة.

٤. يعين مستوى تصنيف جميع المعلومات التي يتم صيانتها أو تخزينها أو إنتاجها من قبل الجامعة.

٥. يجب مراجعة تصنيف كل أصل معلومات مرة واحدة على الأقل في السنة.

٦. يتم تحديث نتائج تصنيف المعلومات وفقًا للتغييرات في قيمتها وحساسيتها وخطورتها خلال دورة حياتها.

REF: [ISO/IEC 27001: A.8.2.1]

١٨. ديباجات لوصف المعلومات

١. تقع على عاتق عمادة تقنية المعلومات والاتصالات مسؤولية وضع ديباجات تحدّد تصنيف الأصول التي تحتوي معلومات وأن تحتفظ بسجلات لهذه الأصول. ويجب أن تكون عملية وضع الديباجات متوافقة مع الممارسات المعتمدة في الجامعة.

٢. يجب الحفاظ على الأصول على أن يتم تداولها وتخزينها ونقلها (أو نشرها) وتدميرها وفقًا لإرشادات تصنيف المعلومات ومعالجتها المرتبطة بديباجة تصنيف الأصل.

٣. بالنسبة لجميع المستندات التي تحتوي على معلومات مصنفة على أنها "سرية للغاية"، يتعين على عمادة تقنية المعلومات والاتصالات:

ا. تخزينها في الأدراج المغلقة أو خزائن.

ب. حافظ على قفل أي مكتب يتم تخزين المستندات فيه عندما تكون غير مشغولة.

ج. لا تترك مفاتيحًا لخزانات التخزين في المكتب عندما يكون الشخص الذي لديه حق الوصول المصرح به إليها غير موجود.

٤. على عمادة تقنية المعلومات والاتصالات تحديد طريقة التعامل مع المعلومات وطريقة تخزينها؛ وأن تضع إجراءات لذلك من أجل حماية هذه المعلومات من أن تكشف بطريقة غير مصرح بها ومن أن يساء استخدامها.

٥. يجب أن تشتمل الديباجات الورقية الموضوعة على المستندات والأجهزة والوسائط القابلة للإزالة على التصنيفات الأمنية المناسبة وفقًا لسياسة إدارة الأصول.

٦. يجب ألا تسلّم الوسائط التي تحتوي على معلومات مصنفة على أنها "عالية السرية" إلى أي جهة خارجية أو طرف ثالث ما لم تأذن بذلك عمادة تقنية المعلومات والاتصالات بمبرر مناسب يتعلّق بالعمل. ويجب أن يوقع الطرف الثالث على اتفاقية يلتزم بموجبها بعدم كشف هذه المعلومات (وهذا في حالة تلف الوسيط وظهور حاجة لإعادته للطرف الثالث).

REF:[ISO/IEC 27001: A.8.2.2]

١٩. التعامل مع الأصول

١. يقوم ضابط أمن المعلومات وعمادة تقنية المعلومات والاتصالات بوضع وتحديد الإجراءات المناسبة للتعامل مع المعلومات ومعالجتها وتخزينها وإبلاغها بناءً على تصنيفها من أجل حماية هذه المعلومات من الكشف أو سوء الاستخدام غير المصرح بهما.

٢. يجب على الموظفين الذين يحتفظون بمعلومات حساسة تتعلق بجامعة الإمام عبد الرحمن بن فيصل اتباع سياسات التحكم في الوصول الأمني لضمان حماية هذه المعلومات من الوصول غير المصرح به

٣. يقتصر استخدام وسائط التخزين والأجهزة الطرفية عمل الجامعة فقط. (ومن هذه الوسائط على سبيل المثال، البيانات ا لرقمية ، ومنافذ USB ، وأقراص الفلاش ، إلخ) و يجب النظر في الآليات المركزية التي تتحكم وتحد من استخدام هذه الأجهزة.

٤. توضع وسائط التخزين المحمولة التي تحتوي معلومات حساسة غير مشفرة عن الجامعة في جهاز مغلق عند ما تكون غير مستخدمة.

٥. لا يمنح الوصول للمعلومات الحساسة أو القيمة المتعلقة بالجامعة إلا لأفراد محددين ، وليس مجموعات ، على أساس مبدأ الحاجة إلى المعرفة وبعد الحصول على إذن من إدارة الجامعة.

٦. يتم التعامل مع جميع المعلومات على أساس الطريقة التالية:

وصف	عام	داخلي	سري	سرية عالية
تعريف	المعلومات التي تتاح على نطاق واسع في رمي النشر العام، والنشرات، ومحتوى الويب وطرق التوزيع الأخرى والإفصاح أو التناوب أو التعديل لن تسبب أي خطر على الجامعة	معلومات التشغيل الروتينية أو اليومية التي لا تتطلب إجراءات خاصة للحماية من التعديل أو الكشف غير المصرح به للوصول ولكن هذا لا يتوفر على نطاق واسع للجمهور	المعلومات السرية أو الحساسة التي لن تعرض الجامعة بالضرورة لخسارة كبيرة، ولكن صاحب البيانات قد قرر اتخاذ تدابير أمنية ضرورية للحماية من الوصول أو التعديل أو الكشف غير المصرح به	المعلومات التي تتطلب أعلى مستوى من الحماية لأن الإفصاح من المحتمل أن يؤدي إلى تأثير إعلاني كبير على الجامعة (الإحراج، الخسارة المالية، إلخ ...)
مثال	الكتيبات والنشرات الجديدة والنشرات واتجاهات الهاتف الداخلية على الإنترنت والمواد التسويقية	المراسلات الروتينية، النشرات الإخبارية للموظفين، المذكرات الداخلية، السياسات والإجراءات الداخلية	الملكية الفكرية المرخصة و / أو التي قيد التطوير والسجلات ومعلومات الشراء وعقود البيع وتكوين النظام وسجلات النظام وتقرير المخاطر و RFP وRFI	معلومات تعريف الطالب الصحية المحمية (PHI) ، والبيانات المالية للإدارة ، والمعلومات الشخصية ، وتفاصيل الائتمان أو البنك ، وبروتوكولات أبحاث العقود
التداول				
البريد الإلكتروني الوارد من داخل الجامعة	لا معالجة خاصة المطلوبة	لا يوجد أي معالجة خاصة مطلوبة ولكن يجب اتخاذ احتياطات معقولة	لا يشجع استخدام البريد الإلكتروني لنقل المعلومات السرية، ولا يُسمح بإعادة التوجيه إلا بواسطة مالك البيانات	لا يشجع استخدام البريد الإلكتروني لنقل المعلومات السرية، ولا يُسمح بإعادة التوجيه إلا بواسطة مالك البيانات
البريد الإلكتروني من خارج الجامعة	لا معالجة خاصة المطلوبة	لا يوجد أي معالجة خاصة مطلوبة ولكن يجب اتخاذ احتياطات معقولة	استخدام البريد الإلكتروني يثبط بشدة النظر في استخدام التشفير ، يحظر	التشفير مطلوب

وصف	عام	داخلي	سري	سرية عالية
			البث إلى قائمة التوزيع. إعادة التوجيه مسموح بها فقط بواسطة مالك البيانات	
نقل البيانات (نقل الملفات ، الموقع الإلكتروني)	لا الاحتياطات الخاصة المطلوبة	ينصح التشفير ولكن ليس مطلوبا	التشفير مطلوب	التشفير مطلوب
طباعة البيانات وموقع الطابعة	لا قيود	يجب أن تكون الطابعة موجودة في منطقة لا يمكن لعامة الناس الوصول إليها	رصد المطلوبة وإزالة المواد المطبوعة على الفور	رصد المطلوب وإزالة المواد المطبوعة على الفور
النسخ الاحتياطي والاسترداد	يجب نسخها احتياطيًا شهريًا وبشكل تدريجي بناءً على التغييرات	يجب نسخها احتياطيًا شهريًا وبشكل تدريجي بناءً على متطلبات استرداد المعلومات من قبل صاحب البيانات والاحتياجات التشغيلية للشركة. يجب اختبار النسخ الاحتياطي لضمان الموثوقية.	يجب نسخ هذه المعلومات احتياطيًا شهريًا وبشكل تدريجي بناءً على متطلبات استرداد المعلومات من قبل صاحب البيانات والاحتياجات التشغيلية للشركة. يجب اختبار النسخ الاحتياطي لضمان الموثوقية.	يجب نسخها احتياطيًا شهريًا وبشكل تدريجي بناءً على متطلبات استرداد المعلومات من قبل صاحب البيانات والاحتياجات التشغيلية للشركة. يجب اختبار النسخ الاحتياطي لضمان الموثوقية. لا تقم بالكتابة فوق أحدث نسخة احتياطية.
التخزين				
المواد المطبوعة	لا توجد تحوطات خاصة مطلوبة.	احتياطات معقولة لمنع وصول غير الموظفين والعاملين في الجامعة	يجب أن يكون التخزين بطريقة آمنة في حالة عدم المراقبة. (منطقة آمنة، حاوية قابلة للقفل)	يجب أن يتم قفل المادة المخزّنة بطريقة آمنة عند عدم المراقبة (منطقة آمنة، حاوية قابلة للقفل).
الوثائق الالكترونية	يُسمح بالتخزين على جميع الأجهزة مع مراعاة التحكم في الوصول.	يُسمح بالتخزين على جميع الأجهزة ولكن مع مراعاة التحكم في الوصول.	التخزين على برامج التشغيل الآمنة أو قرص مشترك آمن فقط. يجب تخزين البيانات على خادم يمكن الوصول إليه داخليًا، ولا تخزن أي بيانات على خادم يمكن الوصول إليه مباشرة من الإنترنت.	التخزين على قرص آمن فقط. ويفضل حماية كلمة السر الخاصة بالوثيقة.
رسائل البريد الإلكتروني	لا توجد تحوطات خاصة مطلوبة.	احتياطات معقولة لمنع الوصول بواسطة إذن شخصي.	تخزين بطريقة آمنة، على سبيل المثال الوصول إلى كلمة المرور أو تصغيرها إلى تنسيق الطباعة، حذف النموذج الإلكتروني، وتخزينه وفقًا لطريقة تخزين مواد الطباعة.	تخزين بطريقة آمنة، على سبيل المثال، الوصول إلى كلمة المرور أو تصغيرها لتنسيق الطباعة، وحذف النموذج الإلكتروني، وتخزينه وفقًا لطريقة تخزين مواد الطباعة.
الأجهزة المحمولة	لا توجد تحوطات خاصة مطلوبة.	استخدام حاوية أو أجهزة قابلة للقفل	استخدام حاوية أو أجهزة قابلة للقفل	استخدام حاوية أو أجهزة قابلة للقفل
التخزين من قبل طرف ثالث	لا توجد تحوطات خاصة مطلوبة..	آمن مع مرفقات قابلة للقفل والتحكم في الوصول المطلوبة.	تأمين مع مرفقات قابلة للقفل والتحكم في الوصول المطلوبة.	تأمين مع مرفقات قابلة للقفل والتحكم في الوصول المطلوبة
تمييز المستند	لا قيود	للإستخدام الداخلي فقط	"سري"	"سري للغاية"
الأمن المادي				
محطة العمل	يجب استخدام شاشات حماية كلمة المرور عند عدم استخدامها. قم بالتسجيل عند عدم الاستخدام لفترة طويلة.	يجب استخدام شاشات حماية كلمة المرور عند عدم استخدامها. قم بالتسجيل عند عدم الاستخدام لفترة طويلة.	يجب استخدام شاشات حماية كلمة المرور عند عدم استخدامها. قم بالتسجيل عند عدم الاستخدام لفترة طويلة.	يجب استخدام شاشات حماية كلمة المرور عند عدم استخدامها. قم بالتسجيل عند عدم الاستخدام لفترة طويلة.
الخادم	غير مسموح به.	تأمين موقع المنطقة والوصول المحدود بناءً على مسؤوليات الوظيفة.	تأمين موقع المنطقة والوصول المحدود بناءً على مسؤوليات الوظيفة.	تأمين موقع المنطقة والوصول المحدود بناءً على مسؤوليات الوظيفة.
الطباعة	لا قيود.	جمع االمواد التي طبعت على الفور.	تقليل الطباعة وجمع المادة المطبوعة على الفور.	القيام بالطباعة عند الضرورة فقط ولا تترك الطابعة تترك بدون مراقبة.
مكتب الوصول	لا قيود.	لا قيود.	يجب تقييد الوصول إلى المناطق الحساسة باستخدام التحكم في الوصول.	يجب تقييد الوصول إلى المناطق الحساسة باستخدام التحكم في الوصول.

وصف	عام	داخلي	سري	سرية عالية
				يجب أن تبقى المعلومات السرية تحت القفل.
الأجهزة المحمولة	لا يجوز ترك الجهاز بدون مراقبة في أي وقت.	لا يجوز ترك الجهاز بدون مراقبة في أي وقت	لا يجوز ترك الجهاز بدون مراقبة فى أي وقت. النظر فى استخدام قفل والتحكم في الوصول.	يجب عدم ترك الجهاز بدون مراقبة فى أي وقت ويجب وضعه تحت القفل والتحكم في الوصول.
التحكم في الوصول	تحتوي على تغييرات من قبل الشخص المصرح له فقط.	التحكم في الوصول إلى كلمة المرور.	التحكم في الوصول إلى كلمة المرور تحتوي على تغييرات بناءً على بيانات صاحب العمل وحاجته.	كلمة المرور / البيومترية / المصادقة على التحكم في الوصول. تغيير المحتوى بناءً على مالك البيانات والحاجة إلى العمل.

REE: [ISO/IEC 27001: A.8.2.3]

٢٠. إدارة الوسائط القابلة للإزالة

١. يجب مراعاة متطلبات أمن المعلومات في إدارة المعلومات القابلة للنقل والوسائط التقنية ذات الصلة.

٢. يجب مراعاة ما يلي لإدارة الوسائط القابلة للإزالة:

ا. يجب تخزين جميع الوسائط وحفظها في بيئة آمنة ومأمّنة ووفقًا لمواصفات الشركة المصنعة وسياسات وإجراءات أمن المعلومات المعمول بها في جامعة الإمام عبد الرحمن بن فيصل.

ب. في حالة الوسائط التي تعد هناك حاجة لها، فإنّ محتويات هذه الوسائط المراد إزالتها يجب أن تكون غير قابلة للاسترداد.

ج. يجب السماح بمحركات تشغيل الوسائط القابلة للإزالة إذا اقتضت حاجة العمل ذلك.

د. يجب تخزين نسخ متعددة من المعلومات القيمة الخاصة بـ جامعة الإمام عبد الرحمن بن فيصل وحفظها في وسائط منفصلة لضمان توفرها في حالة تلف البيانات أو فقدها.

REF:[ISO/IEC 27001: A.8.3.1]

٢١. التخلص من والوسائط

١. يجب التصرف في جميع الوسائط الحساسة الخاصة بجامعة الإمام عبد الرحمن بن فيصل وفقًا لسياسة وإجراءات إدارة الأصول أو فترة الاحتفاظ بالوسائط أو انتهاء استخدامها. وبمجرد التخلص من الوسائط، يتم توثيق عملية التخلص وإبلاغ المالك بها.
٢. يجب الحصول على إذن المالك قبل إزالة جميع الوسائط أو التخلص منها.
٣. يجب تسجيل جميع الوسائط التي تم التخلص منها في سجل محدث خاص بهذا الأمر من أجل الحفاظ على سجل يرجع إليه عند التدقيق.
٤. يجب التخلص من جميع المعلومات الحساسة الخاصة الخاصة بالجامعة سواء كانت مستندات مطبوعة أو مخزنة في وعاء إلكتروني ولم تعد مطلوبة، بطريقة آمنة ، باستخدام المعدات والإجراءات المعتمدة لضمان عدم إمكانية استرداد هذه المعلومات. ويجب أن يتم التخلص باستخدام إحدى الطرق التالية، على سبيل المثال لا الحصر:
   ا. التمزيق.
   ب. إعادة التدوير.
   ج. الحرق (أي تحويله إلى ثاني أكسيد الكربون وبخار النفايات "الرماد" بالنار).
5. يجب الاحتفاظ بسجل للمعلومات الحساسة التي تم التخلص منها لمدة خمس سنوات على الأقل وفقًا للمتطلبات التنظيمية بجامعة الإمام عبد الرحمن بن فيصل ، ويجب أن يتضمن السجل كحد أدنى:
   ا. تاريخ التخلص منها.
   ب. اسم الشخص الذي قام بالتخلص.
   ج. اسم المالك.
   د. الحصول على موافقة المالك.
   ه. طريقة التخلص المتبعة.
٦. قبل إرسال وسائط التخزين إلى طرف ثالث ، يجب حذف أو إخفاء أو استبدال جميع المعلومات الحساسة المتعلقة بجامعة الإمام عبد الرحمن بن فيصل وفقًا للطرق المعتمدة من الجامعة.

REF:[ISO/IEC 27001: A.8.3.2]

٢٢. نقل الوسائط المادية

١. يجب استخدام تقنيات التشفير -حيثما أمكن - لحماية سرية وسلامة وصحة المعلومات الحساسة أثناء نقل الوسائط.

٢. يجب إرسال جميع المعلومات الحساسة الخاصة بـ جامعة الإمام عبد الرحمن بن فيصل في شكل ورقي بواسطة شركة بريد موثوق بها أو عن طريق البريد المسجل ويجب تتبعها دائمًا برقم فاتورة موازنة وطلب توقيع المستلم. ولا يجوز تسليم هذه المعلومات إلى الوسطاء.

REF: [ISO/IEC 27001: A.8.3.3]

---------- نهاية الوثيقة ----------