ابتكار الأعمال الملهمة

سياسة أمن الاتصالات

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 وثيقة سرية وموجهة للجهات المعنية فقط حيث لا يتم توزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة تقنية المعلومات والاتصالات.

٣. الرقابة على الوثيقة

٣,١. معلومات عن الوثيقة

العنوان	التصنيف	الإصدارة	الحالة
سياسة أمن الاتصالات	سري	١.١	معتمدة

٣,٢. الإعداد والتحديث

الإصدارة	الإعداد	تاريخ الاصدار	التغييرات
0.1	علاء عليوه	18نوفمبر 2014	إعداد
0.2	نبيل البحبوح	1ديسمبر 2014	تحديث
0.3	أسامة العمري	23ديسمبر 2014	QA
1.0	نبيل البحبوح	31ديسمبر 2014	تحديث
١.١	منيب أحمد – تقنية المعلومات والاتصالات بجامعة الإمام عبد الرحمن بن فيصل	24أبريل 2017	تحديث

٣,٣. مراجعة والتحقق والاعتماد

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

٣,٤. قائمة التوزيع

عدد النسخ	المستلم	الموقع

٤. نظرة عامة على السياسة

يتناول هذا الجزء بالتفصيل الغرض من هذه السياسة ونطاقها وتعريف مصطلحاتها و، وتغييرها، ومراجعتها وتحديثها، وإنفاذها والامتثال لها والأدوار والمسؤوليات المتعلقة بها، والمستندات ذات الصلة وملكية السياسة.

٤,١. الغرض

الغرض الرئيسي من سياسة أمن الاتصالات هو:

ضمان حماية المعلومات في الشبكات والمرافق الداعمة لمعالجة المعلومات، والحفاظ على أمن المعلومات المنقولة داخل جامعة الإمام عبد الرحمن بن فيصل ومع أي جهة خارجية

٤,٢. النطاق

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

- جميع الموظفين بدوام كامل وبدوام جزئي والموظفين المؤقتين الذين يعملون لدى جامعة الإمام عبد الرحمن بن فيصل 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 حصلوا على حق الوصول إلى أنظمة المعلومات والاتصالات في جامعة الإمام عبد الرحمن بن فيصل.

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

٤,٣. تعريف المصطلحات

يقدم الجدول ١ تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة.

المصطلح	التعريف
المساءلة	مبدأ أمني يشير إلى ضرورة تحديد هوية الأفراد وتحميلهم مسؤولية أفعالهم.
الأصول	المعلومات التي ذات قيمة 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 قِبل جهة مصرح لها بذلك.
السرية	عدم توفير أو الكشف عن أصل من الأصول أو خدمة من الخدمات لأفراد أو كيانات أو عمليات غير مصرح بها.
الرقابة	وسيلة لإدارة المخاطر، وتشمل السياسات والإجراءات والإرشادات التي يمكن أن تكون ذات طبيعة إدارية أو تقنية أو إدارية أو قانونية.
الإرشاد	وصف يوضح ما يجب عمله لتحقيق الأهداف المحددة في السياسات الطريقة التي تحقق بها تلك الأهداف.
أمن المعلومات	الحفاظ على سرية المعلومات وسلامتها وتوفّرها. ويشمل أمن المعلومات وسائل أخرى مثل التحقّق والمساءلة وعدم التنصل والموثوقية.
السلامة	الحفاظ على الأصول والتأكّد من دقتها وتناسقها طوال دورة حياتها بأكملها.
المالك	أي شخص أو مجموعة من الأشخاص حددتهم الإدارة لتحمّل مسؤولية الحفاظ على سرية الأصول وتوفرها وسلامتها. قد 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 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.

الجدول ١: تعريف المصطلحات

٤,٤. التغيير والمراجعة والتحديث

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 محدثًا بحيث يخضع للتحديث بمجرد إجراء أي تغيير في السياسة.

٤,٥. الإنفاذ والامتثال

يعد الالتزام بهذه السياسة إلزاميًا ويجب مراجعته بشكل دوري من قبل ضابط أمن المعلومات. يجب على جميع وحدات جامعة الإمام عبد الرحمن بن فيصل (من عادات، وإدارات، وكليات، وأقسام ومراكز) ضمان مراقبة الامتثال المستمر في نطاقها.

في حالة تجاهل أو انتهاك توجيهات أمن المعلومات، قد تتضرر بيئة جامعة الإمام عبد الرحمن بن فيصل (على سبيل المثال، يحدث فقدان للثقة في الجامعة وسمعتها، أو تتعطل عملياتها أو تحدث بها انتهاكات قانونية)، ويكون الأشخاص الذين تجاهلوا هذه التوجيهات 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 وعند التعامل مع هذه الانتهاكات.

٤,٦. 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 المخوّل لها الموافقة على هذا الطلب هي ضابط أمن المعلومات على أن تعتمد هذه الموافقة عمادة تقنية المعلومات والاتصالات. 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.

٤,٧. الأدوار والمسؤوليات (مصفوفة راكي)

يوضح الجدول ٢ مصفوفة راكي[1] (RACI) التي تحدد المساءل و المسؤول ومن تتم استشارته أو إبلاغه بكل مهمة هناك حاجة القيام بها. هناك بعض الأدوار المشاركة في هذه السياسة على التوالي: عمادة تقنية المعلومات والاتصالات، موظف أمن المعلومات (ISO) ، إدارة الموارد البشرية / الوحدة الإدارية (HR/ A) ، والإدارة القانونية ، الموظف المسؤول عن إدارة المشروع (PMO) ، المالك والمستخدم (الموظف و المتعاقد).

الأدوار / المسؤوليات	تقنية المعلومات والاتصالات	ضابط أمن المعلومات	الإدارة القانونية	الموارد البشرية/ الإدارة	الموظف المسؤول عن الإدارة	المالك	المستخدم
تحديد الاتفاقيات التي لا يجوز لموظفي جامعة الإمام عبد الرحمن بن فيصل والأطراف الثالثة أن يفصحوا عنها.	R, A	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 الألتقاط والمفاتيح وجدران الحماية).	R, A	C				I	

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

[1] تصف مصفوفة راكيRACI الخاصة بتحديد المسؤوليات المشاركة بأدوار مختلفة في إنجاز مهام العمل. إنها مفيدة بشكل خاص في توضيح الأدوار والمسؤوليات في العمليات التي تشترك في تنفيذها وظائف أوإدارات متعددة حيث يرمز الحرف(R) إلى المسؤول عن تنفيذ مهمة من المهام، وبينما يرمز الحرف (A) إلى المسؤول الذي يعتمد تنفيذ المهمة ؛ ويرمز الحرف(C) إلى المستشار الذي يقدم الآراء ويرمز الحرف (I) إلى المسؤول الذي يبلغ بآخر التطورات في تنفيذ المهمة.

٤,٨. 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

٤,٩. الملكية

هذه الوثيقة مملوكة لعمادة تقنية المعلومات والاتصالات بجامعة الإمام عبد الرحمن بن فيصل وهي التي تحافظ عليها .

٥. بيانات السياسة

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

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

ضوابط الشبكة

١. تحدد عمادة تقنية المعلومات والاتصالات وتنفيذ التدابير المضادة المناسبة من أجل:

أ- التحكم في سرية وسلامة المعلومات الحساسة التي تمر عبر الشبكات العامة.

ب- حماية الأنظمة والتطبيقات المتصلة بالشبكة.

ت- الحفاظ على توفر خدمات الشبكة واتصالها بأجهزة الحواسيب.

٢. لا يجوز لجميع موظفي جامعة الإمام عبد الرحمن بن فيصل وزوارها توصيل أي جهاز (على سبيل المثال أجهزة الحاسب الشخصية أو أجهزة الحاسب المحمول أو معدات الشبكات) بشبكة جامعة الإمام عبد الرحمن بن فيصل، دون الحصول على إذن وموافقة مناسبين من قسم تقنية ا لمعلومات المتعلقة بعمل جامعة الإمام عبد الرحمن بن فيصل.

٣. يجب على عمادة تقنية المعلومات والاتصالات السماح بكل حركة التقاط الشبكة المستندة إلى متطلبات الاتصالات المتعلقة بعمل جامعة الإمام عبد الرحمن بن فيصل.

٤. يجب على عمادة تقنية المعلومات والاتصالات تطبيق آليات تحكم مناسبة لالتقاط الشبكة لضبط تدفق المعلومات في مسارات الشبكة المعينة.

٥. تتأكّد عمادة تقنية المعلومات والاتصالات من وجود إدارة وإشراف فني محكم على هيكل محيط الأمن (مثل جدار الحماية) وهيئته الحالية حيث يجب تغطية ما يلي، على سبيل المثال لا الحصر:

i. *توثيق قواعد محيط الأمن ومراجعتها بشكل منتظم.*

ii. *توثيق تغييرات التكوين والحصول على موافقة الإدارة.*

iii. الحصول على موافقة الإدارة قبل تطبيق أي تغييرات على قواعد ضبط الأمن.

iv. العناية الكافية أثناء تطبيق التغييرات على قواعد محيط الأمن لضمان الحد الأدنى من التشويه لبيئة جامعة الإمام عبد الرحمن بن فيصل.

٦. يجب تقييد قدرة المستخدمين على الاتصال بالشبكة من خلال بواباتها التي تقوم بتصفية حركة المرور عن طريق جداول أو قواعد محددة مسبقًا. وتشمل هذه القيود على سبيل المثال لا الحصر الأشياء التالية:

i. المراسلة (مثل البريد الإلكتروني).

ii. نقل الملفات.

iii. الوصول التفاعلي.

iv. الوصول إلى التطبيقات

REF: [ISO/IEC 27001: A.9.1.1]

٥,١. أمن خدمات الشبكة

١. تحمي عمادة تقنية المعلومات والاتصالات البنية التحتية لشبكة جامعة الإمام عبد الرحمن بن فيصل من خلال تنفيذ تدابير وإجراءات 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 الآمن بخدمات الشبكة وفقًا لقواعد اتصال الشبكة والأمن مثل جدار الحماية و VPNو.IDS / IPS

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

REF: [ISO/IEC 27001: A.9.1.2]

٥,٢. فصل الشبكات

١. تقسم عمادة تقنية المعلومات والاتصالات شبكة جامعة الإمام عبد الرحمن بن فيصل إلى شرائح أو مناطق أو مجالات منطقية بناءً على المعايير التالية، على سبيل المثال لا الحصر:

أ. متطلبات الوصول (على سبيل المثال، الإدارة، الإدارة، 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، Trusted، Internet، DMZ.)

ه. خطوط العمل (مثل الخدمة والدعم).

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

REF:[ISO/IEC 27001: A.9.2.1]

٥,٣. 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 أو إتلافها بطريقة تتماشى مع سياسات جامعة الإمام عبد الرحمن بن فيصل التي تحكم وتحمي سرية هذه البيانات وسلامتها وتوفرها.

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

REF:[ISO/IEC 27001: A.9.2.2]

٥,٤. اتفاقيات نقل المعلومات

١. 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:

i. مسؤوليات الإدارة.

ii. التبادلات اليدوية والإلكترونية.

iii. حساسية المعلومات الهامة التي يتم تبادلها.

iv. متطلبات الحماية.

v. متطلبات الإخطار.

vi. معايير التغليف والنقل.

vii. تحديد ساعي لنقل المعلومات

viii. المسؤوليات والالتزامات.

ix. ملكية البيانات والبرامج.

x. مسؤوليات الحماية والتدابير.

xi. متطلبات التشفير.

REF:[ISO/IEC 27001: A.9.2.3]

٥,٥. المراسلة الإلكترونية

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

REF:[ISO/IEC 27001: A.9.2.4]

٥,٦. 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 والاتصالات 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:

i. تحديد المعلومات المراد حمايتها ومستويات الحساسية المطلوبة.

ii. تحديد المدة المتوقعة للالتزام.

iii. تحديد شروط إرجاع أو إتلاف المعلومات عند إنهاء الالتزام.

iv. تحديد المسؤوليات والمتطلبات المتعلقة بالتوقيع من أجل منع الكشف غير المصرح به للمعلومات.

v. نشر العقوبات المطبقة في حالة فشل المستخدم في احترام الالتزام.

٢. يجب أن تراعي التزامات السرية وعدم الإفصاح الشروط القانونية المعمول بها في جامعة الإمام عبد الرحمن بن فيصل من أجل تلبية متطلبات حماية أصول الجامعة.

REF: [ISO/IEC 27001: A.9.2.5]

---------- نهاية الوثيقة ----------