ابتكار الأعمال الملهمة

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

سياسة أمن المعلومات

الإصدار: 2.0

رمز السياسة: DICT-QAP012

October 2020

All rights reserved for Deanship of ICT ®

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

المحتويات

معلومات ذات ملكية فكرية 3

الرقابة على الوثيقة 4

معلومات عن الوثيقة 4

الإعداد والتحديث 4

قائمة التوزيع 4

الاعتماد 4

المقدمة 5

نظرة عامة على السياسة 9

الغرض 9

النطاق 9

المصطلحات وتعريفها 10

التغيير والمراجعة والتحديث 10

الإنفاذ / الامتثال 11

الاستثناءات 11

الأدوار والمسؤوليات (مصفوفة المهام RACI) 12

الوثائق ذات الصلة 13

الملكية 14

بيانات السياسية 15

سياسات أمن المعلومات 15

مراجعة سياسات أمن المعلومات 17

All rights reserved for Deanship of ICT ©

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

معلومات ذات ملكية فكرية

هذه الوثيقة هي عبارة عن معلومات خاصة بعمادة الاتصالات وتقنية المعلومات في جامعة الإمام عبد الرحمن بن فيصل. وهي وثيقة موجهة للجهات المعنية فقط حيث لا يتم توزيعها أو الكشف عنها أو نشرها أو نسخها دون إذن كتابي من عمادة الاتصالات وتقنية المعلومات.

.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

الرقابة على الوثيقة

معلومات عن الوثيقة

عنوان	تصنيف	الإصدار	الحالة
سياسة أمن المعلومات	عام	2.0	معتمدة

الإعداد والتحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
0.1	علاء عليوه	9نوفمبر 2014	إعداد
0.2	نبيل البحبوح	1ديسمبر 2014	تحديث
0.3	أسامة العمري	27ديسمبر 2014	QA
1.0	نبيل البحبوح	31ديسمبر 2014	تحديث
1.1	منيب أحمد	27أبريل 2017	تحديث
1.2	لمياء عبد الله الجعفري	6 يونيو 2020	تحديث
2.0	د. يشار عبدالمهدي الذيب	28 سبتمبر 2020	تحديث

قائمة التوزيع

#	المستفيد
1	دائرة الشؤون القانونية
2	الموقع الالكتروني للجامعة
3	قسم ضمان الجودة بالعمادة

الاعتماد

الاسم	الصفة	التاريخ	التوقيع
د. خالد عدنان العيسى	عميد الاتصالات وتقنية المعلومات	8th October 2020	

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

المقدمة

تعتبر سرية أصول المعلومات وسلامتها وتوافرها ضرورية للحفاظ على الامتثال لأمن جامعة الإمام عبد الرحمن بن فيصل. يجب أن تقر عمادة تقينة المعلومات المعلومات والاتصالات بأهمية ضمان أمن المعلومات ضمن أصول المعلومات؛ وتلتزم بدعم أهداف ومبادئ أمن المعلومات .

الهدف النهائي لسياسة أمن المعلومات في جامعة الإمام عبد الرحمن بن فيصل هو ضمان ما يلي:

- الحفاظ على سرية المعلومات (على سبيل المثال، المعلومات الأكاديمية والإدارية والشخصية).
- سلامة المعلومات من خلال الحماية من التعديل غير المصرح به.
- توفر المعلومات للمستخدمين المصرح لهم، عند الاقتضاء.
- حماية المعلومات من الوصول غير المصرح به.
- تحقيق استراتيجية العمل.
- تقييم التهديدات الأمنية الحالية داخل البيئة.
- الوفاء بالمتطلبات التنظيمية والتشريعية.
- تحديد المسؤوليات والمساءلة عن أمن المعلومات.

يجب على جميع موظفي جامعة الإمام عبد الرحمن بن فيصل وأعضاء هيئة التدريس والطلاب والمقاولين والاستشاريين والأطراف الثالثة الالتزام بسياسة أمن المعلومات والسياسات الداعمة المناسبة. يلخص الجدول 1 بإيجاز كل السياسات التي تم تطويرها لدعم الموقف الأمني العام لأصول معلومات وحدة المراجعة الداخلية. تتبع هذه السياسات أفضل ممارسات الأمن وفقًا لمعيار الآيزو ISO / IEC 27001: 2013 وتعيين توصياتها (الملحق أ).

يجب أن تتضمن كل سياسة لأمن المعلومات عبارات تتناول الجوانب التالية:

- تعريف أمن المعلومات وأهدافه ومبادئه لتوجيه جميع الأنشطة المتعلقة بأمن المعلومات.
- الاستثناءات المتعلقة بجميع الأدوار والمسؤوليات ذات الصلة.
- عملية معالجة الاستثناءات من السياسة.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

الرقم	السياسة	الهدف أوالأهداف
1	تنظيم أمن المعلومات	وضع إطار إداري لتأسيس أمن المعلومات داخل جامعة الإمام عبد الرحمن بن فيصل ومراقبة تنفيذه وتشغيله. ضمان أمن العمل عن بعد واستخدام أجهزة الهاتف المحمولة.
2	أمن الموارد البشرية	التأكد من أن موظفي جامعة الإمام عبد الرحمن بن فيصل والمقاولين يفهمون مسؤولياتهم وأنهم مناسبون للأدوار المسندة إليهم. التأكد من أن العاملين بجامعة الإمام عبد الرحمن بن فيصل والمتعاقدين معها على دراية بمسؤولياتهم المتعلقة بأمن المعلومات والوفاء بها. حماية مصالح جامعة الإمام عبد الرحمن بن فيصل الأخرى عند تغيير العمل أو إنهاء الخدمة.
3	إدارة الأصول	تحديد الأصول الخاصة بجامعة الإمام عبد الرحمن بن فيصل وتحديد مسؤوليات الحماية المناسبة لها. التأكد من حصول المعلومات على مستوى مناسب من الحماية وفقًا لأهميتها بالنسبة لجامعة الإمام عبد الرحمن بن فيصل. منع الكشف غير المصرح به أو تعديل أو إزالة أو إتلاف المعلومات المخزنة على الوسائط.
4	التحكم في الدخول	الحد من الوصول إلى المعلومات ومرافق معالجتها. التأكد من وصول المستخدم المصرح به ومنع غيره من الوصول إلى الأنظمة والخدمات. جعل المستخدمين مسؤولين عن حماية المعلومات التي يتحقق بها منهم. منع الوصول غير المصرح به إلى الأنظمة والتطبيقات.
5	التشفير	ضمان الاستخدام السليم والفعال للتشفير حماية لسرية المعلومات و / أو صحتها و / أو سلامتها.
6	الأمن المادي والبيئي	منع الوصول المادي غير المصرح به إلى معلومات جامعة الإمام عبد الرحمن بن فيصل ومرافق معالجة هذه المعلومات ومنع إتلافها والتدخل فيها. منع فقدان أو تلف أو سرقة أو تسوية الأصول ووقف عمليات جامعة الإمام عبد الرحمن بن فيصل.
7	أمن العمليات	ضمان التشغيل الصحيح والآمن لمرافق معالجة المعلومات. التأكد من حماية المعلومات و مرافق معالجتها من البرامج الضارة. حماية البيانات من الفقدان. تسجيل الأحداث والتوصل الى الأدلة و البراهين المتعلقة بها.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

		ضمان سلامة النظم التشغيلية. منع استغلال الثغرات التقنية. تقليل تأثير أنشطة التدقيق على النظم التشغيلية.
8	أمن الاتصالات	ضمان حماية المعلومات في الشبكات ومرافق دعم المعلومات الخاصة بها. الحفاظ على أمن المعلومات المنقولة داخل جامعة الإمام عبد الرحمن بن فيصل والمرسلة إلى أي جهة خارجية.
9	اقتناء الأنظمة وتطويرها وصيانتها	التأكد من أن أمن المعلومات هو جزء لا يتجزأ من أنظمة المعلومات عبر دورة الحياة بأكملها. التأكد من أن أمن المعلومات تم تصميمه وتنفيذه خلال دورة حياة تطوير نظم المعلومات. ضمان حماية البيانات المستخدمة في إجراء الاختبارات.
10	العلاقات مع الموردين	ضمان حماية أصول جامعة الإمام عبد الرحمن بن فيصل التي يمكن للموردين الوصول إليها. الحفاظ على مستوى متفق عليه من أمن المعلومات وتقديم الخدمات بما يتماشى مع اتفاقيات التوريد.
11	إدارة حوادث أمن المعلومات	ضمان اتباع نهج ثابت وفعال لإدارة حوادث أمن المعلومات، بما في ذلك التواصل بشأن الأحداث الأمنية ونقاط الضعف.
12	جوانب أمن معلومات إدارة استمرارية العمل	التأكد من أن استمرارية أمن المعلومات مضمنة في أنظمة إدارة استمرارية العمل في جامعة الإمام عبد الرحمن بن فيصل. ضمان توافر مرافق معالجة المعلومات.
13	الامتثال	تجنب مخالفة الالتزامات القانونية أو التعاقدية المتعلقة بأمن المعلومات وأي متطلبات أمنية.
14	إدارة المخاطر	تحديد مجالات ضعف أمن المعلومات والتهديدات داخل بيئة جامعة الإمام عبد الرحمن بن فيصل وبدء العلاج المناسب.
15	الاستخدام المقبول	وضع مجموعة من القواعد التي تجعل المستخدمين يتقيدون بطرق استخدام خدمات الحاسب الآلي والشبكات والبريد الإلكتروني والإنترنت. التقليل من المخاطر المحتملة مثل هجمات الفيروسات، والتنازل عن أنظمة وخدمات الشبكة، والمشاكل القانونية.

الجدول 1: قائمة سياسات أمن المعلومات

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

يوضح الشكل (1) مجالات الأمن وجوانبها ذات الصلة وفقًا لمعيار الآيزو ISO / IEC 27001: 2013 الملحق أ.

هناك 14 نطاقاً لأربعة وثلاثين جانباً من الجوانب الأمنية (الأهداف)

أ .٥ - سياسات أمن المعلومات	• A.5.1-التوجيه الإداري لأمن المعلومات
A.6-تنظيم أمن المعلومات	• A.6.1-التنظيم الداخلي • A.6.2-أجهزة الهاتف المحمول والعمل عن بعد
A.7-أمن الموارد البشرية	• A.7.1- قبل التوظيف • A.7.2-أثناء التوظيف • A.7.3-إنهاء وتغيير الوظيفة
A.8- إدارة الأصول	• أ .٨,١ - المسؤولية عن الأصول • A.8.2 - تصنيف المعلومات • A.8التعامل مع الوسائط
A.9 - التحكم في الوصول	• A.9.1 - متطلبات العمل من التحكم في الوصول • A.9.2 - إدارة وصول المستخدم • A.9.3 - مسؤوليات المستخدم • A.9.4 - التحكم في الوصول إلى التطبيقات و A.10- التشفير
A.10.1 ضوابط التشفير	
A.11 - الأمن المادي والبيئي	• A.11.1 - المناطق الآمنة • A.11.2 - الأجهزة
A.12- أمن العمليات	• A.12.1 - الإجراءات والمسؤوليات التشغيلية • A.12.2 - الحماية من البرامج الضارة • A.12.3 - النسخ الاحتياطي • A.12.4 - التسجيل والمراقبة • A.12.5 - التحكم في البرامج التشغيلية • A.12.6 - إدارة الثغرات التقنية • A.12.7 - اعتبارات تدقيق نظم المعلومات
A.13 - أمن الاتصالات	• A.13.1 - إدارة أمان الشبكة • A.13.2 - نقل المعلومات
A.14 - اقتناء النظام والتطوير والصيانة	• A.14.1 - متطلبات الأمن لنظم المعلومات • A.14.2 - الأمن في عمليات التطوير والدعم • A.14.3 - بيانات الاختبار
A.15 - علاقات الموردين	• A.15.1 - أمن المعلومات في علاقات الموردين • A.15.2 - إدارة تقديم خدمات الموردين
A.16 - إدارة حوادث أمن المعلومات	• A.16.1 - إدارة حوادث أمن المعلومات والتحسينات
A.17 - جوانب أمن المعلومات لإدارة استمرارية الأعمال	• A.17.1 - استمرارية أمن المعلومات • A.17.2 - التكرار
A.18 - الامتثال	• أ. ١٨,١ الامتثال للمتطلبات القانونية والتعاقدية

الشكل 1: مجالات الأمن وفقًا للمعيار ISO / IEC 27001: 2013 *(الملحق أ)*

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

نظرة عامة على السياسة

يستعرض هذا الجزء بالتفصيل الغرض من هذه السياسة ونطاقها ومصطلحاتها وتعريفاتها، وتغييرها، ومراجعتها وتحديثها، وإنفاذها/والامتثال لها ، والأدوار والمسؤوليات، والمستندات ذات الصلة والملكية.

الغرض

الغرض الرئيسي من سياسة أمن المعلومات هو:

رسم الاتجاه الذي تسلكه إدارة جامعة الإمام عبدالرحمن بن فيصل وما يرتبط بذلك الاتجاه من دعم لأمن المعلومات وفقًا لمتطلبات العمل والقوانين واللوائح ذات الصلة.

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 جامعة الإمام عبد الرحمن بن فيصل أو 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 بن فيصل.

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

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

المصطلحات وتعريفها

يقدم الجدول 2 تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة.

المصطلح	التعريف
المساءلة	مبدأ أمني يشير إلى القدرة على التعرف على الأفراد وتحميلهم مسؤولية أفعالهم.
الأصول	المعلومات التي لها قيمة لدى المؤسسة مثل النماذج والوسائط والشبكات والأجهزة والبرامج ونظام المعلومات.
توفر	فحص الحقائق لإبداء الرأي ويمكن أن يشمل اختبار الأدلة لدعم الرأي.
سرية	حالة الأصل أو الخدمة التي يمكن الوصول إليها وقابلة للاستخدام عند الطلب من قِبل جهة معتمدة.
مراقبة	وسيلة لإدارة المخاطر، بما في ذلك السياسات والإجراءات والمبادئ التوجيهية التي يمكن أن تكون ذات طبيعة إدارية عليا أو تقنية أو إدارية أو قانونية.
إرشاد	وصف يوضح ما يجب عمله وكيفية تحقيق الأهداف المحددة في السياسات.
أمن المعلومات	الحفاظ على سرية المعلومات وسلامتها وتوفرها. بالإضافة إلى ذلك، ويشمل ذلك أيضًا استخدام خصائص أخرى مثل التحقق والمساءلة وعدم التنصل والموثوقية.
السلامة	الحفاظ على الأصول وضمان دقتها وتناسقها طوال دورة حياتها.
صاحب	أي شخص أو مجموعة من الأشخاص تم تحديدهم من قِبل الإدارة لتحمل مسؤولية الحفاظ على سرية الأصول وتوفرها وسلامتها. قد يتغير الصاحب أثناء دورة حياة الأصل.
سياسات	خطة عمل لتوجيه القرارات والإجراءات. تتضمن عملية السياسة تحديد البدائل المختلفة مثل البرامج أو أولويات الإنفاق والاختيار من بينها على أساس التأثير الذي ستتركه.
خطر	مزيج من عواقب الحدث (بما في ذلك التغييرات في الظروف) واحتمال 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 2: المصطلحات والتعاريف

التغيير والمراجعة والتحديث

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر الصاحب إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية. ولا يجري تغييرات في هذه السياسة إلا ضابط أمن المعلومات ويجب أن تعتمد الإدارة هذه التغييرات و يجب أن يظل سجل التغيير محدثًا حيث يحدَّث بمجرد إجراء أي تغيير.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

الإنفاذ / الامتثال

يعد الالتزام بهذه السياسة إلزاميًا ويجب مراجعته بشكل دوري من قبل ضابط أمن المعلومات. يجب على جميع وحدات جامعة الإمام عبد الرحمن بن فيصل (العمادة، الإدارة ، الكلية ، القسم والمركز) ضمان مراقبة الامتثال المستمر في منطقتهم.

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 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 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 والاتصالات. ويجب أن يشمل كل طلب استثناء المبررات والمزايا التي تنسب إليه.

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

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

الأدوار والمسؤوليات (مصفوفة المهام RACI)

يوضح الجدول 2 مصفوفة المهام[1] (RACI) التي تحدد الشخص المسؤول والشخص المساءل والشخص الذي تتم استشارته أو إبلاغه بكل مهمة يجب تنفيذها. تشتمل هذه السياسة على أدوار تضطلع بها الأطراف التالية على التوالي: عميد تقنية المعلومات والاتصالات، مدير أمن المعلومات (ISM) ، عمادة تقنية المعلومات والاتصالات ، موظف أمن المعلومات (ISO) ، والإدارة القانونية ، إدارة الموارد البشرية / الوحدة الإدارية (HR / A) ، والمراجع الداخلي والخارجي، والمستخدم (الموظفون ، أعضاء هيئة التدريس ، الطلاب ، المقاولون ، الاستشاريون والأطراف الثالثة).

الأدوار / المسؤوليات	عميد تقنية المعلومات والاتصالات	مدير أمن المعلومات	تقنية المعلومات والتصالات	موظف أمن المعلومات	الإدارة القانونية	الموارد البشرية او الوحدة الإدارية	مراجع الحسابات	المستخدم
إنفاذ سياسات أمن المعلومات داخل بيئة جامعة الإمام عبد الرحمن بن فيصل لحماية أصول معلومات العمل الهامة.	R, A		C	C				I
دعم مبادرات أمن المعلومات والمشاريع والبرامج والأنشطة.	R, A		C	C				I
التأكد من أن سياسات أمن المعلومات متوافقة مع المتطلبات القانونية والتعاقدية الخاصة بجامعة الإمام عبد الرحمن بن فيصل.	I			C	R, A			I
تقديم المشورة القانونية المتخصصة اللازمة للوحدات والإدارات الأخرى لتقديم الخدمات بطريقة متوافقة تمامًا مع القوانين واللوائح السارية المفعول.			C	C	R, A			I
الموافقة على التعديلات الجديدة أو سياسات أمن المعلومات الحالية.	R, A		C	C				I
توزيع وثائق أمن المعلومات بحيث تتوفَّر نسخ لدى من يحتاجون إلى هذه المستندات أو يمكنهم تحديد موقع المستندات بسهولة عبر موقع إنترانت.	I		C	R, A		R, C		I

[1] تصف مصفوفة المهام (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.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

الأدوار / المسؤوليات	عميد تقنية المعلومات والاتصالات	مدير أمن المعلومات	تقنية المعلومات والتصالات	موظف أمن المعلومات	الإدارة القانونية	الموارد البشرية او الوحدة الإدارية	مراجع الحسابات	المستخدم
توصيل هذه السياسة إلى جميع موظفي جامعة الإمام عبد الرحمن بن فيصل الجدد وأعضاء هيئة التدريس والطلاب والعقود والاستشاريين والأطراف الثالثة لضمان فهمهم للمتطلبات والمسؤوليات تجاه سياسات أمن المعلومات.			C	C		R, A		I
تحديد سياسات أمن المعلومات والحفاظ عليها.	I		C	R, A, C				
إعداد وتحديث أدلة أمن المعلومات بشكل دوري واللازمة لتعزيز أمن المعلومات في جامعة الإمام عبد الرحمن بن فيصل.	I		C	R, A, C		I		I
الالتزام بسياسات أمن المعلومات والمبادئ التوجيهية والإجراءات المتعلقة بحماية المعلومات.			C	C		C		R, A,I
الإبلاغ عن الحوادث الأمنية الفعلية أو المشتبه بها لعمادة تقنية المعلومات والاتصالات.	I		A, C	C				R
إدارة جميع أنشطة تدقيق أمن المعلومات.		C, I	I	C, I			R,A	
تطوير خطة التدقيق السنوية.		C, I	I	C, I			R,A	
الإبلاغ عن نتائج التدقيق إلى مدير أمن المعلومات.		C, I	I	C, I			R,A	
ضمان الامتثال لممارسات وسياسات وإجراءات أمن المعلومات		C, I	I	C, I			R,A	
مراقبة الامتثال لسياسات وإجراءات وإرشادات ومعايير أمن المعلومات إلى جانب المعايير الخارجية المختارة.		C, I	I	C, I			R,A	

الجدول 2: الأدوار والمسؤوليات المخصصة بناءً على مصفوفة المهام (RACI)

الوثائق ذات الصلة

فيما يلي جميع السياسات والإجراءات ذات الصلة لهذه السياسة:

- تنظيم سياسة أمن المعلومات
- سياسة أمن الموارد البشرية
- سياسة إدارة الأصول
- سياسة التحكم في الوصول
- سياسة التشفير

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

- سياسة الأمن المادي والبيئي
- سياسة أمن العمليات
- سياسة أمن الاتصالات
- سياسة اقتناءالنظام وتطويره وصيانته
- سياسة علاقات الموردين
- سياسة إدارة حوادث أمن المعلومات
- سياسة جوانب أمن المعلومات الخاصة باستمرارية العمل
- سياسة الامتثال
- سياسة إدارة المخاطر
- سياسة الاستخدام المقبول
- إجراءات تصنيف الأصول
- إجراءات تغيير الإدارة
- إجراءات إدارة التصحيح
- إجراءات إدارة المخاطر
- إجراءات التعامل مع حوادث أمن المعلومات
- إجراءات التحكم في الوصول المادي والمنطقي
- إجراءات أمن الموارد البشرية
- إجراءات النسخ الاحتياطي والاستعادة
- إجراءات الحصول على النظام وتطويره وصيانته

الملكية

هذه الوثيقة مملوكة وتحافظ عليها عمادة الاتصالات وتقنية المعلومات بجامعة الإمام عبد الرحمن بن فيصل.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

بيانات السياسية

تقدم الأجزاء الفرعية التالية بيانات السياسة في جانبين رئيسيين:

- سياسات أمن المعلومات
- مراجعة سياسات أمن المعلومات

سياسات أمن المعلومات

1. تحدد الإدارة إطارًا جيدًا لإنشاء أمن المعلومات والحفاظ عليه وفقًا لمتطلبات عمل جامعة الإمام عبد الرحمن بن فيصل.
2. يجب على الإدارة أن تقر بأهمية ضمان أمن المعلومات داخل أصول جامعة الإمام عبد الرحمن بن فيصل وأن تلتزم بدعم غايات ومبادئ أمن المعلومات.
3. يجب أن تدرك الإدارة مسؤولياتها تجاه دعم أهداف أمن المعلومات داخل بيئة جامعة الإمام عبد الرحمن بن فيصل.
4. يجب على الإدارة أن تحدد اتجاه أمن المعلومات وتدعم تنفيذ متطلباته في كل بيئة جامعة الإمام عبد الرحمن بن فيصل.
5. تلتزم الإدارة بالحفاظ على أمن جميع المعلومات التي داخل أصول جامعة الإمام عبد الرحمن بن فيصل. وتكلف هذه الأصول بضمان أمن المعلومات ومراعاة الجوانب القانونية في ذلك.
6. يجب أن تعتمد طريقة جامعة الإمام عبد الرحمن بن فيصل في إدارة أمن المعلومات على المعايير الدولية {على سبيل المثال مواصفة الآيزو، (ISO / IEC 27001: 2013) } وأفضل الممارسات المقبولة عالميًا لضمان الجوانب التالية:

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

a. عدم الوصول إلى المعلومات (على سبيل المثال، المعلومات الأكاديمية والإدارية والشخصية) إلا عن طريق الأفراد المصرح لهم، والذين لديهم إذن وصول مناسب ومعتمد.

b. جميع المعلومات السرية محمية بشكل جيد وفق الضوابط اللازمة.

c. لا يحدث تغيير و / أو تحديث للمعلومات إلا بواسطة الأشخاص المصرح لهم الذين يتمتعون بصلاحية صحيحة ومعتمدة.

d. توفَّر المعلومات دائمًا لجميع الأفراد الذين لديهم تصريح صحيح ومعتمد للوصول إلى هذه المعلومات.

e. تحمَّل جميع الأفراد الذين منحوا شكلاً من أشكال الوصول إلى المعلومات مسؤولية كاملة عن الاستخدام الصحيح لهذه المعلومات.

7. تلتزم إدارة جامعة الإمام عبد الرحمن بن فيصل والعاملين فيها بسياسات وممارسات أمن المعلومات الخاصة بالجامعة؛ كما تمتثل الإدارة والعاملين معاً لسياسات وإجراءات أمن المعلومات ذات الصلة.

8. يجب على عمادة تقنية المعلومات والاتصالات تحديد وتطوير مجموعة من سياسات أمن المعلومات على مستويين:

a. مستوى رفيع حيث توضع "سياسة أمن المعلومات" التي تحدد طريقة جامعة الإمام عبد الرحمن بن فيصل في إدارة أهداف أمن المعلومات الخاصة بها؛ وتعتمدها إدارة الجامعة.

b. مستوى منخفض حيث توضع سياسات خاصة بموضوع من المواضيع لدعم تنفيذ الضوابط الأمنية داخل بيئة جامعة الإمام عبد الرحمن بن فيصل. ومن أمثلة هذه المواضيع ما يلي:

- التحكم في الوصول المادي والمنطقي
- الأمن البيئي
- أمن الشبكات والاتصالات
- ضوابط التشفير

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

- معلومات النسخ الاحتياطي والاسترداد
- استمرارية الأعمال
- تبادل المعلومات
- إدارة التهديدات الخارجية
- أمن سطح المكتب والحاسب الشخصي المحمول
- خصوصية البيانات وحمايتها
- إدارة أمن الموردين

REF: [ISO/IEC 27001: A.5.1.1]

مراجعة سياسات أمن المعلومات

1. يجب على موظف أمن المعلومات الحفاظ على جميع سياسات وإجراءات أمن المعلومات ومراجعتها وتحديثها سنوياً.
2. يجب على موظف أمن المعلومات قياس فعالية الضوابط المطبقة سنويًا لتجنب الحوادث الأمنية وتقليل الآثار الناتجة عنها من خلال عملية محددة جيدًا لقياس مدى نضج أمن الأصول آخذاً في الاعتبار ما يلي:
   a. التغذية الراجعة من المستخدمين المعنيين وردود أفعالهم.
   b. تقارير الحوادث الأمنية.
   c. مراجعة المستشارين المستقلين والإدارة.
   d. اتجاهات التهديدات ونقاط ضعفها.
   e. التشاور مع إدارة الموارد البشرية / الوحدة الإدارية والإدارة القانونية وإشراكهم في الأمر.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

3. يجب على مسؤول أمن المعلومات التأكد من أن سياسات أمن المعلومات الداخلية والإجراءات ذات الصلة موثقة جيدًا بما يتماشى مع المعايير الدولية ذات الصلة مثل مواصفة الآيزو 27001 ISO / IEC 27001: (2013) والمتطلبات القانونية والتنظيمية.

REF: [ISO/IEC 27001: A.5.1.2]

---------- نهاية الوثيقة----------

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©