ابتكار الأعمال الملهمة

جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

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

سياسة أمن العمليات

الإصدار: 2.0

رمز السياسة: DICT-QAP013

All rights reserved for Deanship of ICT ©

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

المحتويات

معلومات ذات ملكية فكريّة 3
الرقابة على الوثيقة 4
معلومات عن الوثيقة 4
الإعداد والتحديث 4
قائمة التوزيع 4
الإعتماد 4
نظرة عامة على السياسة 5
الغرض 5
النطاق 5
تعريف المصطلحات 6
التغيير، المراجعة والتحديث 7
الإنفاذ والامتثال 7
الاستثناءات 8
الأدوار والمسؤوليات (مصفوفة المهام) 8
الوثائق ذات الصلة 9
الملكية 10
بيانات السياسة 11
توثيق إجراءات التشغيل 11
إدارة التغيير 12
إدارة القدرات 13
الفصل بين بيئات التطوير وبيئات الاختبار والبيئات التشغيلية 13
ضوابط للحماية من البرامج الضارة 13
النسخ الاحتياطي للمعلومات 16
تسجيل الحوادث 17
حماية معلومات السجل 17
سجلات المسؤول والمشغل 18
مزامنة الساعات 18
تثبيت البرامج على أنظمة التشغيل 18
إدارة الثغرات الفنية 19
القيود المفروضة على تثبيت البرامج 20
ضوابط مراجعة نظم المعلومات 21

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

معلومات ذات ملكية فكريّة

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

العنوان	التصنيف	الإصدار	الحالة
سياسة أمن العمليات	عام	2.0	معتمدة

الإعداد والتحديث

الإصدار	الإعداد	تاريخ الاصدار	التغييرات
0.1	علاء عليوه	18 نوفمبر 2014	إعداد
0.2	نبيل البحبوح	1 ديسمبر 2014	تحديث
0.3	أسامة العمري	27 ديسمبر 2017	تحديث
1.0	نبيل البحبوح	31 ديسمبر 2018	تحديث
1.1	منيب أحمد	2 مايو 2019	تحديث
1.2	د. بشار عبدالمهدي الذيب	6 يونيو 2020	تحديث
2.0	د. سامر بني عواد	13 سبتمبر 2021	تحديث

قائمة التوزيع

الرقم	المستفيد
1	إدارة الشؤون القانونية
2	الموقع الالكتروني للجامعة
3	قسم ضمان الجودة بالعمادة

الإعتماد

الاسم	العنوان	التاريخ	التوقيع
د. خالد عدنان العيسى	عميد الاتصالات وتقنية المعلومات	15th April 2022	

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 وتعريف مصطلحاتها، وتغييرها، ومراجعتها وتحديثها، وإنفاذها/ والامتثال لها، والأدوار والمسؤوليات، واستثناءاتها، والوثائق ذات الصلة بالإضافة لملكية الوثيقة.

الغرض

الغرض الرئيسي من سياسة أمن العمليات هو:

ضمان التشغيل السليم والآمن لمر افق معالجة المعلومات، بالإضافة إلى ضمان الحماية من البرمجيات الخبيثة والفيروسات ومن فقدان البيانات بسبب أحصنة طروادة.

ومع ذلك، تضمن هذه السياسة سلامة النظم التشغيلية؛ وتمنع استغلال نقاط الضعف التقنية؛ وتقلل تأثير أنشطة التدقيق والمراجعة على النظم التشغيلية.

النطاق

تنطبق بيانات السياسة المكتوبة في هذه الوثيقة على جميع موارد وحدة المراجعة الداخلية على جميع مستويات الحساسية، 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 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 ©

تعريف المصطلحات

يقدم الجدول 1 تعريفات للمصطلحات الشائعة المستخدمة في هذه الوثيقة.

المصطلح	التّعريف
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.
توفّر	الحالة التي يكون فيها الأصل أو الخدمة قابلة لأن تصلها جهة مصرّح لها بذلك وقابلة لأن تستخدمها أيضاً..
إدارة القدرات	عملية تحديد سعة النظام اللازمة لتقديم مستويات أداء محددة من خلال القياس والتحليل لحجم العمل الحالي والمتوقع.
السريّة	عدم توفّر الأصل أو الخدمة أو عدم كشف أيّ منهما لأفراد أو جهات 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 الأشياء المطلوب عملها وكيفية تحقيق الأهداف المحددة في السياسات.
الحادثة	حدوث حالة بعينها في النظام أو الخدمة أو الشبكة تشير إلى خرق محتمل لسياسة أمن المعلومات أو فشل إجراءات السلامة أو قد تكون الحالة ذات صلة بالأمن لكنها غير معروفة سابقًا.
أمن المعلومات	الحفاظ على سرية المعلومات وسلامتها وتوفّرها. وهو يشمل وسائل أخرى مثل التحقّق والمساءلة وعدم التنصل والموثوقية.
السلامة	الحفاظ على الأصول والتأكّد من دقتها وتناسقها طوال دورة حياتها بأكملها.
البرامج الضارة (الخبيثة)	برنامج مصمم لتعطيل تشغيل الحاسب الآلي أو جمع معلومات حساسة أو الوصول إلى أنظمة الحاسب الآلي الخاصة (على سبيل المثال، فيروس أو حصان طروادة).
المالك (الصاحب)	أي شخص أو مجموعة من الأشخاص تم تحديدهم من قِبل الإدارة لتحمل مسؤولية الحفاظ على سرية الأصول وتوافرها وسلامتها. وقد يتغير المالك أثناء دورة حياة الأصل.
اختبار الاختراق	طريقة لتقييم تأمين نظام الحاسب الآلي أو الشبكة عن طريق محاكاة هجوم من جهات خارجية ضارة (ليس لديها وسائل معتمدة للوصول إلى أنظمة الجامعة) وجهات داخلية خبيثة (لا تتمتع بمستوى معين من الوصول المصرح به). تتضمن هذه العملية تحليلًا نشطًا للنظام للتعرّف على أي ثغرة أمنية محتملة يمكن أن تنجم عن التكوين السيئ أو غير الصحيح للنظام، سواءً كانت عيوب معروفة أو غير معروفة في الأجهزة والبرمجيات أو نقاط ضعف تشغيلية في العملية أو التدابير التقنية المضادة. يتم تنفيذ هذا التحليل من موقع مهاجم محتمل ويمكن أن يتضمن هذه استغلالًا نشطًا لثغرات أمنية.
السياسة	خطة عمل يسترشد بها عند اتخاذ القرارات والإجراءات. وتشمل السياسة 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).
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 آلي والبرامج الثابتة والأجهزة.
التهديد	احتمال التسبب في حادثة غير مرغوب فيها تؤدّي إلى إلحاق ضرر بنظام من نظم الجامعة مثل الكشف عن معلومات

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

	حساسة أو أصول أو خدمات بطريقة غير مصرح بها أو تدميرها أو إزالتها أو تعديلها أو التسبب في انقطاعها أو إصابة عدد من الأشخاص. وقد يكون التهديد متعمدًا أو عرضيًا أو ناجم عن أصل طبيعي.
الثغرة	نقطة ضعف في الإجراءات أو العمليات أو الضوابط الأمنية يمكن استغلالها عن طريق التهديد بالوصول غير المصرح به إلى المعلومات أو تعطيل المعالجة الحرجة المتعلقة بها.
تقييم الثغرات	عملية تحديد نقاط الضعف وتحديد أولوياتها (أو ترتيبها) في نظام ما. والثغرة من منظور إدارة الكوارث تعني تقييم التهديدات الناجمة عن مخاطر محتملة على السكان والبنية التحتية.

الجدول 1: تعريف المصطلحات

التغيير، المراجعة والتحديث

يجب مراجعة هذه السياسة مرة واحدة كل عام ما لم يعتبر المالك إجراء مراجعة سابقة ضرورية لضمان استمرار السياسة الحالية. والجهة الوحيدة المخول لها إجراء تغييرات في هذه السياسة هو ضابط أمن المعلومات على أن تعتمد الإدارة هذه التغييرات. ويجب أن يظل سجل التغيير محدثًا بحيث يتم تحديثه بمجرد إجراء أي تغيير.

الإنفاذ والامتثال

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

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 التأكد من أنّ الموظفين الذين يشتبه في انتهاكهم للأوامر الأمنية تتم معاملتهم بطريقة صحيحة وعادلة (مثلا اتخاذ إجراءات تأديبية ضدهم). ويجب إبلاغ إدارة الموارد البشرية بالأمر والتعامل مع انتهاكات السياسة لمعالجتها.

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

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 الاتصالات وتقنية المعلومات. ويجب أن يشمل كل طلب استثناء المبررات والمزايا التي تنسب إليه.

أقصى مدة للاستثناء هي أربعة أشهر. 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 2 مصفوفة المهام[1] (RACI) التي تحدد من هو المساءل أو المسؤول أو الذي يجب أن يستشار أو يبلّغ بكل مهمة يجب تنفيذها.

هناك بعض الأدوار التي تشترك فيها عدة أطراف في هذه السياسة؛ وهي على التوالي: عمادة الاتصالات وتقنية المعلومات، موظف (ضابط) أمن المعلومات، مكتب إدارة المشاريع، المالك والمستخدم (ويشمل الموظف والمتعاقد).

الأدوار / المسؤوليات	تقنية المعلومات	ضابط أمن المعلومات	مكتب إدارة المشاريع	المالك	المستخدم
تحديد والحفاظ على متطلبات القدرات لجميع الأنشطة الجديدة والمستمرة لمشروع تقنية المعلومات.	R,A	C	R,I		
تحديد حقوق الوصول المطلوبة للمستخدمين للأصول.	R,C	C		R,A	I
أداء مراقبة النظام / التطبيق / شبكة الأمن.	R,A	C			
إدارة البنى التحتية الأمنية الحرجة (على سبيل المثال، البنية التحتية لمكافحة الفيروسات).	R,A	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	تقنية المعلومات	ضابط أمن المعلومات	مكتب إدارة المشاريع	المالك	المستخدم
تصميم وتنفيذ أمن الشبكات والنظام.	R,A	C		I	
تطبيق الضوابط المناسبة لحماية سرية وسلامة وتوافر وصحة المعلومات الحساسة.	R,A	C		I	
تنسيق الرد على الانتهاكات الفعلية أو المشتبه فيها في سرية أنظمة جامعة الإمام عبد الرحمن بن فيصل الحرجة أو سلامتها أو توفرها.	R,A	C		I	
تنفيذ التغييرات وتثبيت التصحيح على النظام / التطبيق / الشبكة وفقًا لإجراءات إدارة التغيير وإدارة التصحيح.	R,A	C		C,I	
الالتزام بسياسات وإجراءات أمن المعلومات المتعلقة بحماية المعلومات.	C	C			R,A,I
الإبلاغ عن الحوادث الأمنية الفعلية أو المشتبه بها لعمادة الاتصالات وتقنية المعلومات.	A,C	C		I	R

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

الوثائق ذات الصلة

فيما يلي جميع السياسات والإجراءات ذات الصلة بهذه 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 إدارة التغيير
- إجراءات إدارة التصحيح
- إجراءات إدارة الوصول المادي والمنطقي
- إجراءات الحصول على النظام وتطويره وصيانته

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

الملكية

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

All rights reserved for Deanship of ICT ©

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

بيانات السياسة

تقدم الأجزاء الفرعية التالية بيانات السياسة في أربعة عشر جانبًا رئيسيًا هي:

- توثيق إجراءات التشغيل
- إدارة التغيير
- إدارة القدرات
- فصل بيئات التطوير والاختبار والتشغيل
- ضوابط للحماية من البرامج الضارة
- النسخ الاحتياطي للمعلومات
- تسجيل الحوادث
- حماية معلومات السجل
- سجلات المسؤول الإداري والمشغل
- تزامن الساعة
- تثبيت البرامج على أنظمة التشغيل
- إدارة نقاط الضعف الفنية
- القيود المفروضة على تثبيت البرامج
- ضوابط تدقيق نظم المعلومات

توثيق إجراءات التشغيل

1. تبادر عمادة الاتصالات وتقنية المعلومات و مسؤول أمن المعلومات بإعداد العمليات والإجراءات والإرشادات والمعايير أو تشرف على إعدادها وفقًا للأنشطة التشغيلية لجامعة الإمام عبد الرحمن بن فيصل. قد يشمل توثيق إجراءات التشغيل على سبيل المثال لا الحصر ما يلي:

   i. إعادة تشغيل النظام واسترجاعه

   ii. تركيب النظام وتهيئته

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

iii. الدعم الإحتياطي

iv. صيانة الأجهزة

v. غرفة الخادم

vi. إدارة التعامل مع البريد

vii. الرقابة

2. عند تنفيذ البرامج المطورة حديثًا أو المحدّثة أو نقلها من بيئة اختبار إلى بيئة إنتاج يجب أن تتبع إجراءات توثيق صحيحة.

[ISO/IEC 27001: A.12.1.1]

إدارة التغيير

1. تقوم عمادة الاتصالات وتقنية المعلومات بالتعاون مع ضابط أمن المعلومات بإعداد إجراء إداري رسمي يحدد جميع الأدوار والمسؤوليات لضمان السيطرة الكافية على جميع التغييرات .

2. تشمل الإجراءات التفصيلية لإدارة التغيير والضوابط المناسبة لها ما يلي- على سبيل المثال لا الحصر:

i. وضع معايير القبول بالتنسيق مع مالك الأصول.

ii. قيام ضابط أمن المعلومات بتقييم المخاطر التي قد تنجم عن التغييرات الرئيسية الجديدة المقترحة.

iii. عدم استخدام التغييرات الطارئة على مرافق أو أنظمة أو تطبيقات تقنية المعلومات والاتصالات إلا في الظروف القاسية وبموافقة الإدارة.

iv. تطبيق إجراءات التحكم في المستندات دائمًا.

v. عدم تطبيق تصحيحات لمعالجة الأخطاء البرمجية إلا بعد التأكّد من أنها ضرورية على أن يتم ذلك بترخيص من الفريق الفني والإدارة والمورد.

vi. اختبار التطوير الذي يحدث في البرمجيات أو الأنظمة بدقة قبل نشر هذه البرمجيات والأنظمة المطورة في بيئة إنتاج جامعة الإمام عبد الرحمن بن فيصل.

Reference: [ISO/IEC 27001: A.12.1.2]

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

إدارة القدرات

1. يجب مراعاة متطلبات الأداء والسعة الجديدة للأنظمة في مرحلة التخطيط والتصميم. ومن أمثلة إدارة الطلب على السعة-على سبيل المثال لا الحصر- ما يلي:
   i. حذف البيانات القديمة (مساحة القرص).
   ii. إيقاف تشغيل التطبيقات أو النظم أو قواعد البيانات أو البيئات.
   iii. تقوية منطق التطبيق أو استفسارات قاعدة البيانات.
   iv. تقييد استخدام عرض النطاق الترددي في خدمات الأعمال غير الهامة التي تستهلك المزيد من الموارد (مثل بث الفيديو).
2. تقوم عمادة الاتصالات وتقنية المعلومات بالتعاون مع مكتب إدارة المشاريع بتحديد متطلبات القدرات المتعلقة بجميع الأنشطة الجديدة والمستمرة ويحتفظ بها.

[ISO/IEC 27001: A.12.1.3]

الفصل بين بيئات التطوير وبيئات الاختبار والبيئات التشغيلية

1. يجب تنفيذ الفصل بين بيئات الاختبار والإنتاج لتقليل فرص إساءة استخدام الأنظمة بإهمال أو بشكل متعمد.
2. عند الاقتضاء، لا تُستخدم بيانات حية لإجراء اختبارات على أي أصول، سواء في بيئة الإنتاج أو في بيئة الاختبار.
3. يجب أن تضمن عمادة الاتصالات وتقنية المعلومات تطبيق جميع التغييرات بدقة واختبارها في بيئة اختبار قبل التصريح بالتغيير في بيئة الإنتاج.

[ISO/IEC 27001: A.12.1.4]

ضوابط للحماية من البرامج الضارة

1. على عمادة الاتصالات وتقنية المعلومات ضمان بقاء البنية التحتية للكشف عن البرامج الضارة نشطة وغير معطلة ولا يمكن تعطيلها في أي نقطة دخول محتملة.

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

2. على عمادة الاتصالات وتقنية المعلومات تطبيق الضوابط المناسبة لمنع انتقال البرمجيات الضارة إلى المستخدمين المتصلين بالبنية التحتية الخاصة بشبكة جامعة الإمام عبد الرحمن بن فيصل.

3. يجب تحديد وتنفيذ مستوى مناسب من الضوابط لحماية سلامة البرامج والمعلومات؛ حيث قد تشمل هذه الضوابط على سبيل المثال لا الحصر ما يلي:

أ- ضوابط كشف ووقاية واسترداد للحماية من البرامج الضارة.

ب- إجراءات مناسبة لتوعية المستخدمين.

4. يجب أن تطبق برمجية مكافحة فيروسات مركزية- حيثما كان ذلك مناسبًا - على مختلف المستويات في البنية التحتية للشبكة والنظم (مثل الخوادم وأجهزة الحاسب المكتبية وأجهزة الحاسب الآلي المحمولة والبوابات في الشبكة المحيطة) في إطار منهج متدرّج للحد من دخول البرامج الضارة إلى بيئة جامعة الإمام عبد الرحمن بن فيصل على أن يؤخذ في الحسبان ما يلي:

i. يجب أن تظل ملفات التوقيع في برامج مكافحة الفيروسات محدثة باستمرار لتكون محمية من البرامج الضارة الجديدة التي تنشأ بانتظام.

ii. يجب توصيل خادم مكافحة الفيروسات المركزي في جميع الأوقات بخادم تحديث تعريف الفايروس الخاص بالبائع، على أن يجري تحديث ملفات توقيع الخوادم يوميًا؛ بمجرد توفر إصدارات البائع المعمول بها ومن ثمّ دفعها إلى جميع مستخدمي محطات العمل في جامعة الإمام عبد الرحمن بن فيصل.

iii. يجب أن تكون محطات العمل والأجهزة المفعلة على الشبكة والخوادم معدة لأن تصل للشبكة في هيئة تمكنها من الحصول على أحدث ملف للتوقيع بمجرد اتصالها بشبكة جامعة الإمام عبد الرحمن بن فيصل، سواء كان اتصالاً فعليًا أو عبر شبكة افتراضية خاصةVPN ().

iv. يجب إزالة جميع البرمجيات الضارة المكتشفة على أنظمة جامعة الإمام عبد الرحمن بن فيصل على الفور. ولا يُسمح للأنظمة التي عليها برمجيات ضارة لم تزل أو تعطّل أن تتصل بشبكة الجامعة.

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

v. يجب أن تعد برمجية مكافحة الفيروسات بحيث تزيل جميع البرامج الضارة التي تم اكتشافها على النظام تلقائيًا.

5. يحظر تمامًا تثبيت أي برمجية غير مصرح بها أو غير قانونية على أي نظام من أنظمة جامعة الإمام عبد الرحمن بن فيصل على أن يؤخذ في الاعتبار ما يلي:

i. لا يجوز استخدام جميع أقراص الذاكرة الخارجية (USB) أو الأقراص المضغوطة أو أقراص دي في دي (DVD) أو الوسائط القابلة للإزالة على أي جهاز حاسب آلي تابع لجامعة الإمام عبد الرحمن بن فيصل، ما لم تكن معتمدة من عمادة الاتصالات وتقنية المعلومات.

ii. يجب تهيئة جميع خوادم ومحطات عمل جامعة الإمام عبد الرحمن بن فيصل لمسح الوسائط الخارجية القابلة للإزالة بحثًا عن الفيروسات بمجرد توصيل هذه الأدوات بالأجهزة.

iii. يجب تنظيف الوسائط المصابة بالفيروسات قبل تركيبها لتكون وحدات تخزين للبيانات على خوادم ومحطات عمل جامعة الإمام عبد الرحمن بن فيصل.

iv. قبل توزيع أي برمجيات أو معلومات في شكل محوسب، على المستخدمين أولاً إخضاع هذه البرمجيات أو المعلومات للفحص المناسب، بما في ذلك المسح الشامل للتأكّد من عدم وجود أي فيروسات تهاجم الحاسب الآلي.

6. يجب أن يتفهم العاملون بجامعة الإمام عبد الرحمن بن فيصل مسؤوليتهم المتعلقة بإبلاغ عمادة الاتصالات وتقنية المعلومات بأي مشكلات ذات صلة بوجود شفرة ضارة (إن وجدت). كما يجب عليهم الإبلاغ عن أي سلوك غير طبيعي أو غير معتاد في النظام مثل:

i. معالجة بطيئة للتطبيقات.

ii. وجود نشاط مستمر أو مطول في الأقراص الثابتة أو الشبكة.

[ISO/IEC 27001: A.12.2.1]

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

النسخ الاحتياطي للمعلومات

1. يجب على عمادة الاتصالات وتقنية المعلومات بالتعاون مع مالكي (أصحاب) الأصول تحديد متطلبات النسخ الاحتياطي والاستعادة لجميع المعلومات والتطبيقات وأنظمة التشغيل وقواعد البيانات وإعدادات المستخدم وإعدادات الأجهزة بما يتماشى مع النصوص القانونية والتنظيمية وتوصيات الشركة الصانعة وخطورة المعلومات والعوامل الأخرى ذات الصلة.

2. لتلبية ومعالجة متطلبات النسخ الاحتياطي؛ وإدارة بيئة احتياطية، يجب أن تؤخذ الأشياء التالية في الاعتبار:

   i. تقليل جهد الإدارة في التعامل مع أشرطة النسخ الاحتياطي للمعلومات.

   ii. دمج وسائط النسخ الاحتياطي والتخزين في موقع مركزي.

   iii. أن تكون برمجية النسخ الاحتياطي بسيطة بالقدر الذي يسهّل النسخ الاحتياطي واستعادة البيانات، بحيث يمكن تكليف مشغل النسخ الاحتياطي بأداء هذه المهام.

   iv. تثبيت حل مركزي للنسخ الاحتياطي لإدارة سياسة النسخ الاحتياطي للمعلومات وإعداد متطلباته وتشغيله.

3. على عمادة الاتصالات وتقنية المعلومات الاحتفاظ بسجلات النسخ الاحتياطي ومراجعتها وتحديثها (على سبيل المثال، نسخة احتياطية لشبكة سيمانتيك نت)

4. يجب تشفير النسخ الاحتياطي الذي يحتوي على معلومات حساسة حيثما كان ذلك ممكنا.

5. يجب الاحتفاظ بجميع وسائط التخزين الاحتياطية في مكان آمن ولا يسمح بالوصول إليها إلا للعاملين في جامعة الإمام عبد الرحمن بن فيصل المصرح لهم فقط.

[ISO/IEC 27001: A.12.3.1]

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

تسجيل الحوادث

1. يجب على ضابط (مسؤول) أمن المعلومات ضمان تنفيذ مستويات محددة وكافية لتسجيل الأحداث وصار ذلك ممكناً في أنظمة وتطبيقات وقواعد بيانات جامعة الإمام عبد الرحمن بن فيصل.

2. يجب على ضابط (مسؤول) أمن المعلومات التأكّد من أنّ الأحداث المتعلّقة بإنشاء حساب المستخدم وحذفه وإلغاء حقه في الوصول إلى معلومات الجامعة وخدماتها قد سجّلت بطريقة مفصلة لمدة ثلاث سنوات على الأقل.

3. يجب وضع إجراءات مفصلة لمراقبة استخدام مرافق تقنية المعلومات والاتصالات على أن تشمل هذه الإجراءات على سبيل المثال لا الحصر ما يلي:

   i. بيانات مفصلة عن الشخص الذي يراقب هذه الأنشطة وطبيعة المعلومات الإدارية المنتجة والجهة التي ستقدم لها هذه المعلومات.

   ii. الفترات التي يتكرر فيها رصد الأنشطة.

   iii. تفاصيل الإجراء الذي تم تنفيذه في حالة حدوث أي خرق أمني.

[ISO/IEC 27001: A.12.4.1]

حماية معلومات السجل

1. يجب أن تضمن عمادة الاتصالات وتقنية المعلومات أن الضوابط الحالية تهدف إلى حماية سجل المرفق من التعرض لتغييرات غير مصرح بها ومشاكل تشغيلية. وتشمل هذه الضوابط على سبيل المثال لا الحصر ما يلي:

   i. تعديلات على أنواع الرسائل المسجلة.

   ii. ملفات السجل التي يتم تحريرها أو حذفها.

   iii. السعة التخزينية لوسائط ملف السجل التي يتم تجاوزها، مما يؤدي إما إلى عدم تسجيل الأحداث أو الكتابة فوق الأحداث المسجلة السابقة.

[ISO/IEC 27001: A.12.4.2]

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

سجلات المسؤول والمشغل

1. على عمادة الاتصالات وتقنية المعلومات التأكد من مراجعة سجلات مسؤول النظام والمشغل بصورة دورية.
2. على عمادة الاتصالات وتقنية المعلومات التأكد من أن جميع مسؤولي النظام ومشغليه ليس لديهم إذن لتعديل أو إلغاء تنشيط سجلات أنشطتهم الخاصة.

[ISO/IEC 27001: A.12.4.3]

مزامنة الساعات

1. يجب أن تضمن عمادة الاتصالات وتقنية المعلومات أنّ تاريخ ووقت مسارات مراجعة وتدقيق جميع الأنظمة والخوادم ومكونات الشبكة قد كانت متزامنة (في وقت واحد) لتسهيل تتبع هوية المستخدم وأنشطته.
2. يجب مزامنة جميع الأنظمة والخوادم وساعات أجهزة الشبكة باستخدام بروتوكول وقت الشبكة (NTP) المقبول دولياً.

[ISO/IEC 27001: A.12.4.4]

تثبيت البرامج على أنظمة التشغيل

1. يجب تنفيذ الإجراءات للتحكم في تثبيت البرمجيات على أنظمة جامعة الإمام عبد الرحمن بن فيصل، ولتقليل أخطار انقطاع الخدمات أو تلفها.
2. يجب تقوية تأمين جميع الأنظمة من خلال التكوين الآمن المتوافق مع معايير أفضل الممارسات الدولية .
3. يجب تطبيق الضوابط الأمنية الخاصة بنقطة النهاية لتقييد استخدام أجهزة النظام والأجهزة الطرفية.
4. على مسؤولي تقنية المعلومات والاتصالات (على سبيل المثال، مسؤول النظام، مسؤول التطبيق، مسؤول قاعدة البيانات ومشرف الشبكة) مراعاة ما يلي:

   i. أن يكونوا هم الجهة الوحيدة المعتمدة لإجراء تحديثات للبرمجيات والتطبيقات ومكتبات البرامج التشغيلية.

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

ii. التأكد من توثيق إجراءات التكوين الرسمية (formal configuration) والاحتفاظ بها.

5. أي قرار يقضي بتطوير أي مكون من مكونات تقنية المعلومات إلى إصدار جديد يجب أن يأخذ في الاعتبار متطلبات جامعة الإمام عبد الرحمن بن فيصل في مجال الأعمال والأمن.

6. يجب أن تكون إجراءات التشغيل الخاصة بأنظمة جامعة الإمام عبد الرحمن بن فيصل موثقة بشكل واضح وأن يتم الاحتفاظ بسجل للأنشطة بتفاصيلها وأنواعها ويجب أن يراقب سجل الأنشطة دوريًا وفقًا لسياسات وإجراءات الجامعة.

[ISO/IEC 27001: A.12.5.1]

إدارة الثغرات الفنية

1. على عمادة الاتصالات وتقنية المعلومات إجراء تقييم سنوي للثغرات الفنية و (أو) عند حدوث تغيير كبير لتحديد نقاط الضعف في تكوينات الأنظمة أو التعرف على التصحيحات التي تحتاجها تلك الأنظمة.

2. على الإدارة مراجعة تقارير تقييم الثغرات الفنية، وعلى مسؤول أمن المعلومات وضع خطة لمعالجة المخاطر التي يمكن أن تنتج عن هذه المخاطر وتحديد أولويات المعالجة.

3. يجب تحديد الأدوار والمسؤوليات المتعلّقة بإدارة الثغرات التقنية بوضوح.

4. يجب على ضابط أمن المعلومات ومسؤولي تقنية المعلومات والاتصالات القيام بما يلي:

i. اتخاذ خطوات استباقية لتحديد نقاط الضعف في تقنية الأنظمة وتقليلها قبل أن يتم استغلالها.

ii. تحديد الضوابط المناسبة لتخفيف المخاطر والتهديدات بعد إجراء تقييم للثغرات وعمل اختبار الاختراق.

iii. اتخاذ الخطوات اللازمة لتوفير أمن الأنظمة والبنية التحتية للشبكة .

5. لا يجوز تثبيت أي تصحيحات جديدة في بيئة إنتاج ما لم يتم اختبارها وتقييمها بشكل صحيح في بيئة اختبار بموافقة البائع.

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

6. يجب على الموظفين الذين يؤدون واجبات إدارة الثغرات الأمنية ضمان ما يلي :

i. يجب استخدام أدوات المسح الأمني على أساس محدد لتحديد الثغرات التي يمكن استغلالها من قبل أشخاص يقومون بمسح غير مصرح به باستخدام أدوات مماثلة، على ألا تؤثر أدوات المسح الأمني المستخدمة على أداء شبكة جامعة الإمام عبد الرحمن بن فيصل؛

ii. يجب استخدام أدوات متعددة بتقنيات مختلفة لتحديد أكبر قدر ممكن من الثغرات عند الاقتضاء.

iii. يجب إخطار مالك الأصول وأخذ موافقته على التأثيرات المحتملة لنشاط المسح على البيئة المستهدفة قبل بدء المسح.

iv. يجب مراقبة مصادر الطرف الثالث لمعلومات الثغرات الفنية للتأكد من ملاءمتها للأنظمة (على سبيل المثال، موقع البائعين، وتنبيهات الأمن، وتصحيحات النظام، وطرق المعالجة، وتحديثات الفيروسات).

v. إذا أصدر بائع تصحيحًا لإصلاح عنصر تحكم متعلق بالأمن، فيُعتبر إصدار التصحيح بمثابة إخطارًا ضمنيًا بالضعف وفي هذه الحالة يجب أن تُتخذ إجراءات تخفيف المخاطر.

vi. جميع الأجهزة المعتمدة الملحقة بشبكة جامعة الإمام عبد الرحمن بن فيصل وتشغيل أنظمة التشغيل التي بها ثغرات أمنية محددة تم تصحيحها لمعالجة الثغرات المعروفة وفقًا لتوصيات البائع.

vii. في حالة تعذر تصحيح أي جهاز أو نظام متصل بشبكة أو أنظمة جامعة الإمام عبد الرحمن بن فيصل، يتم تخفيف الثغرة الأمنية بواسطة تحكم أمني بديل مقبول.

[ISO/IEC 27001: A.12.6.1]

القيود المفروضة على تثبيت البرامج

1. يجب على عمادة الاتصالات وتقنية المعلومات تحديد وتنفيذ القواعد المناسبة للتحكم في تثبيت البرامج من قبل المستخدمين. يعتبر ما يلي:

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

i. نوع عمليات التثبيت المسموح بها للبرامج (على سبيل المثال، التصحيحات المحدثة والأمان للبرامج المعتمدة).

ii. نوع عمليات تثبيت البرمجيات المحظورة (على سبيل المثال، البرمجيات المخصصة لاستخدام الموظفين فقط).

[ISO/IEC 27001: A.12.6.2]

ضوابط مراجعة نظم المعلومات

1. يجب على عمادة الاتصالات وتقنية المعلومات اتخاذ الإجراءات التالية:

i. منع سوء الاستخدام المحتمل لأدوات مراجعة الأنظمة (على سبيل المثال، لاستخراج معلومات سرية دون إذن صحيح).

ii. التأكد من الحفاظ على سلامة النظم والبيانات المرتبطة بها.

iii. تجنب الانقطاعات المحتملة للأنظمة نتيجة لاستخدام هذه الأدوات.

2. يجب أن يكون استخدام أدوات مراجعة الأنظمة (مثل برمجية المراقبة وبرمجيات استخراج البيانات ومعالجتها والأدوات المساعدة) وفقاً للشرطين التاليين:

i. خضوع أدوات المراجعة للترخيص والقيود والضوابط وفقًا لإرشادات محددة.

ii. أن تكون أدوات المراجعة منفصلة عن الأنظمة التشغيلية ولا يحتفظ به في مكتبات الأشرطة أو مناطق المستخدمين، ما لم يتم توفير مستوى مناسب من الحماية الإضافية.

3. لا يجوز أن يقوم الأشخاص المسؤولون عن تنفيذ الضوابط والمحافظة عليها بأنشطة التدقيق.

4. يجب أن يتمتع للأشخاص الذين يقومون بأنشطة التدقيق وصول محدود (على سبيل المثال، حق الوصول إلى البرمجيات والبيانات لقراءتها فقط). ويقتصر الوصول بخلاف القراءة فقط على النسخ المعزولة من ملفات النظام ويجب محوه عند اكتمال أنشطة المراجعة

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

5. يجب مراقبة وتسجيل جميع عمليات الوصول أثناء أنشطة المراجعة لإنتاج مسار مرجعي. كما يجب توثيق جميع الإجراءات والمتطلبات والمسؤوليات.

6. إذا شاركت أطراف ثالثة في أداء أنشطة المراجعة (قد ينشأ خطر يتمثل في إساءة استخدام أدوات التدقيق من قبل هذه الأطراف الثالثة، والمعلومات التي يتم الوصول إليها من قبل هذه الجهات الخارجية)، فيجب أن تؤخذ ضوابط تقييم المخاطر وتقييد الوصول المادي في الحسبان لمعالجة هذا الخطر وأي تبعات تنجم عنه ، مثل القيام بتغيير فوري لكلمات المرور التي تم الكشف عنها للمراجعين.

[ISO/IEC 27001: A.12.7.1]

---------- نهاية الوثيقة ----------

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