جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة الحماية من البرمجيات الضارة

الإصدار: Version 2.0

رمز السياسة: DICT.I.06-30.CS.A.V2.0

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

1. جدول المحتويات

2. 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.

3. الرقابة على الوثيقة

1.3 معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة الحماية من البرمجيات الضارة	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الإصدار	التغييرات
V1.0	د. بشار الذيب	2021/03/18	إنشاء
V1.1	د. سامر بني عواد	2022/02/09	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/30	مراجعة وتحديث

3.3 المراجعة والتدقيق

تاريخ المراجعة القادمة
2025/01/01

4.3 قائمة التوزيع

الرقم	المستفيد
1	جميع أقسام عمادة الاتصالات وتقنية المعلومات
2	الشؤون القانونية
3	الموقع الإلكتروني
4	

5.3 الاعتماد

الاسم	الوظيفة	رقم القرار	التاريخ
د. نهاد بنت عبد الله العمير	نائب الرئيس للتطوير والشراكة المجتمعية	61945	2024/03/06

4. المقدمة

حماية المعلومات والأصول المعلوماتية والتقنية أمر ضروري لنجاح الجامعة؛ ولهذه الغاية تقوم إدارة الأمن السيبراني بتطوير وإنشاء وتنظيم العمليات الأمنية المطلوبة لحماية الأصول المعلوماتية والتقنية وتحدد هذه الوثيقة المتطلبات الأمنية للحماية من البرمجيات الضارة بناءً على أفضل الممارسات العالمية والمتطلبات التشريعية والتنظيمية ذات العلاقة .

تدرج هذه السياسة في إطار سياسة الجامعة وتحت الصلاحيات الممنوحة من صاحب الصلاحية ابتداءً من تاريخ اعتمادها.

5. الهدف

تهدف هذه السياسة إلى وضع إجراءات ومتطلبات لتحديد وتقييم وتخفيف وتحييد هجمات البرمجيات الضارة ضد الجامعة، حيث تقوم إدارة الأمن السيبراني بتطوير عدد من الأدوات لحماية أصول الجامعة المعلوماتية والتقنية ليتم تنفيذها.

6. قابلية التطبيق ونطاق العمل

تنطبق أحكام هذه السياسة على جميع العاملين أو المكلفين الذين يعملون في الجامعة سواء بعقود دائمة أو مؤقتة وبشكل مباشر أو غير مباشر بما في ذلك الموردين والمقاولين الخارجيين وأي شخص لديه صلاحية الوصول الدائم أو المؤقت إلى بيانات الجامعة مهما كان مصدرها أو شكلها أو طبيعتها وإلى أنظمة وأجهزة وقواعد بيانات الجامعة.

7. السياسة

1.7 متطلبات السياسة العامة

1.1.7 يجب تثبيت برنامج مكافحة البرمجيات الضارة على جميع الخوادم وأجهزة الحاسب والأجهزة المحمولة المتصلة بالشبكة وإدارتها مركزياً بشكل آمن.

2.1.7 يجب تفعيل برامج مكافحة البرمجيات الضارة في جميع الأوقات.

3.1.7 يجب التأكد من أن تقنيات وآليات الحماية قادرة على اكتشاف جميع أنواع البرمجيات الضارة المعروفة وإزالتها، مثل الفيروسات(Virus) ، وأحصنة طروادة(Trojan Horse) ، والديدان(Worms) ، وبرمجيات التجسس (Spyware)، وبرمجيات الإعلانات المتسللة(Adware) ، ومجموعة الجذر(Root Kits) .

4.1.7 يجب اختيار تقنيات وآليات الحماية، يجب التأكد من ملاءمتها لأنظمة التشغيل الخاصة بالجامعة مثل أنظمة ويندوز (Windows)، وأنظمة يونكس (UNIX)، وأنظمة لينكس (Linux)، ونظام ماك (Mac)، وغيرها.

5.1.7 في حال تسبب تحديث تقنيات الحماية بضرر للأنظمة أو متطلبات الأعمال، يجب التأكد من أن تقنيات الحماية قابلة للاسترجاع إلى النسخة السابقة.

6.1.7 يجب تقييد صلاحيات تعطيل التثبيت أو إلغائه أو تغيير إعدادات تقنيات الحماية من البرمجيات الضارة ومنحها لمشرفي نظام الحماية فقط.

2.7 إعدادات تقنيات وآليات الحماية من البرمجيات الضارة

1.2.7 يجب ضبط إعدادات تقنيات الحماية وآلياتها وفقاً للمعايير التقنية الأمنية المعتمدة لدى الجامعة، مع الأخذ بالاعتبار إرشادات المورد وتوصياته.

2.2.7 لا يُسمح للأشخاص التابعين لأطراف خارجية بالاتصال بالشبكة التابعة للجامعة

3.2.7 يجب ضبط إعدادات تقنيات الحماية بالسماح لقائمة محددة فقط من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة.

4.2.7 يجب منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت المعروفة باستضافتها لبرمجيات ضارة وذلك باستخدام آلية تصفية محتوى الويب.

5.2.7 يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أصول الجامعة، وجميع تقنيات وآليات الحماية من البرمجيات الضارة.

6.2.7 يجب حماية الخوادم على جميع الأنظمة خاصة الحساسة عن طريق تقنيات حماية الأجهزة الطرفية المعتمدة لدى الجامعة (End-point Protection).

7.2.7 يجب ضبط برامج مكافحة البرمجيات الضارة على الخوادم/أجهزة المستخدمين لتحديث تعريفات الفيروسات الخاصة به تلقائياً. كما يجب ضبط الخوادم وأجهزة الحاسب لتنزيل تحديثات تعريف الفيروسات من خادم الإدارة المركزي باستخدام آلية العميل الرئيسي وفي حالة فشل خادم الإدارة المركزي؛ يجب ضبط جهاز العميل لتنزيل تحديثات تعريف الفيروسات مباشرةً من مصدر موثوق.

8.2.7 يجب أن يتم ضبط برامج مكافحة البرمجيات الضارة لفحص جميع الأصول القابلة للإزالة تلقائياً قبل الاستخدام.

9.2.7 يجب حماية برنامج مكافحة البرمجيات الضارة بكلمة مرور لمنع تغيير الإعدادات أو إغلاقه من قبل المستخدمين.

10.2.7 يجب إعداد تقارير دورية حول حالة الحماية من البرمجيات الضارة يوضح فيها عدد الأجهزة والخوادم المرتبطة بتقنيات الحماية وحالتها (مثل: محدثة، أو غير محدثة، أو غير متصلة، إلخ)، ورفعها إلى مدير الأمن السيبراني في الجامعة.

11.2.7 يجب أن يكون لجميع التطبيقات التي تدعم رفع الملفات أو نقلها تقنيات الحماية من البرمجيات الضارة.

12.2.7 يجب القيام بعمليات مسح دورية لأجهزة المستخدمين والخوادم والتأكد من سلامتها من البرمجيات الضارة.

يجب إضافة بند يتعلق بإجراء Quick scan

13.2.7 يجب ضبط إعدادات تقنيات الحماية من البرمجيات الضارة للقيام بعمليات التحقق من المحتوى المشبوه في مصادر معزولة مثل صندوق الفحص (Sandbox).

14.2.7 عندما يتم اكتشاف برمجيات ضارة في أصول الجامعة المعلوماتية والتقنية؛ تقوم إدارة الأمن السيبراني بفحص الخوادم/أجهزة الحاسب المصابة.

15.2.7 في حالة انتشار البرمجيات الضارة، تتخذ إدارة الأمن السيبراني تدابير فورية للحد من مدى الضرر.

16.2.7 يجب التحقق من البيانات الواردة إلى شبكة الجامعة، بما في ذلك البريد الإلكتروني والتأكد من خلوه من البرمجيات الضارة.

17.2.7 يجب على المستخدمين الإبلاغ عن حوادث البرمجيات الضارة إلى إدارة الأمن السيبراني.

18.2.7 يجب أن يمنع الجامعة استخدام البرامج والأدوات المساعدة غير المصرح بها وغير المرخصة على جميع الأصول المعلوماتية والتقنية الخاصة بالجامعة.

8. الأدوار والمسؤوليات

يجب على إدارة الأمن السيبراني:

1.1.8 على مدير الأمن السيبراني اعتماد السياسة من صاحب الصلاحية والعمل على تنفيذها.

2.1.8 على مدير الأمن السيبراني اعتماد المعايير والإجراءات والتوجيهات لضمان الالتزام الضروري بمتطلبات أمن عمليات الجامعة.

3.1.8 على مدير الأمن السيبراني ضمان التوافق بين هذه السياسة وأعمال الجامعة.

4.1.8 على مدير الأمن السيبراني حل أي متعارضات تنشأ عن هذه السياسة.

5.1.8 على مدير الأمن السيبراني توفير الموارد اللازمة لتحديد وشراء وتنفيذ الحلول التقنية وذلك لتنفيذ متطلبات السياسة حيثما أمكن.

6.1.8 على مدير الأمن السيبراني إنشاء آليات أو عمليات لمراقبة مكافحة البرمجيات الضارة لضمان المعالجة واستخدام برامج مكافحة البرمجيات الضارة على النحو الملائم والتأكد من اقتصار الأنشطة على العاملين الذين يحتاجون إلى البرنامج لأداء مهامهم المصرح بها.

7.1.8 على إدارة الأمن السيبراني تعميم سياسة الالتزام بالأمن السيبراني وحوكمة البيانات على جميع إدارات وعاملي ومستخدمي الجامعة المصرح لهم أو الذين سيصرح لهم الوصول إلى الأصول التقنية والمعلوماتية.

8.1.8 على إدارة الأمن السيبراني التنسيق مع الإدارات ذات العلاقة لمتابعة الالتزام والتنفيذ.

9.1.8 على إدارة الأمن السيبراني إنشاء خط أساس أمني يمكن من خلاله قياس النشاطات الضارة والمشبوهة.

10.1.8 على إدارة الأمن السيبراني كشف النشاطات غير المعتادة من عاملي الجامعة الملاحظات الإلكترونية وغيرها من المؤشرات، وبناءً على هذه الحالات المشبوهة، يجب تقييم أخطار السلوك الضار.

11.1.8 على إدارة الأمن السيبراني تحديد الإجراءات الواجب اتخاذها عند الاستجابة لتنبيهات الفيروسات في أجهزة الحاسب/الخوادم.

12.1.8 على إدارة الأمن السيبراني مراجعة السياسة بشكل دوري وفقًا للخطة الزمنية التي تم تحديدها.

يجب على عمادة الاتصالات وتقنية المعلومات:

13.1.8 الالتزام بهذه السياسة، وتنفيذ الضوابط المذكورة في هذه السياسة وكذلك الإبلاغ عن أي حادث أمني لإدارة الأمن السيبراني.

14.1.8 دعم مبادرات برنامج إدارة مكافحة البرمجيات الخبيثة في الجامعة بما في ذلك التحقيق في أمر المستخدمين المشتبه بهم أو الذين يعرضون معلومات الجامعة للخطر.

15.1.8 توفير الدعم اللازم لتوعية وتدريب المستخدمين داخل الجامعة.

يجب على الإدارة العليا ومدراء الإدارات ورؤساء الوحدات والمستشارين ما يلي:

16.1.8 التأكد من مشاركة هذه السياسة لجميع العاملين داخل الجامعة أو الملف.

17.1.8 إبلاغ إدارة الأمن السيبراني عن أي تجاوزات أو عدم التزام بهذه السياسة.

يجب على العاملين في الجامعة الالتزام بأحكام هذه السياسة والإبلاغ عن أي حادث أمني أو عدم التزام بأي أحكام واردة في هذه السياسة الى مدير الأمن السيبراني.

9. ملكية السياسة

المسؤول عن هذه السياسة هو مدير الأمن السيبراني في الجامعة.

10. تغييرات السياسة

يجب مراجعة السياسة سنويًا على الأقل أو عند حدوث تغييرات في المتطلبات التشريعية والتنظيمية، وتوثيق التغييرات واعتمادها من قبل صاحب الصلاحية في الجامعة.

11. الالتزام

يجب على جميع العاملين في الجامعة والأطراف (الخارجية/المتعاقد معهم) الالتزام بأحكام هذه السياسة، ويجب على مدير الأمن السيبراني في الجامعة ضمان المراقبة المستمرة للالتزام، ورفع التقارير اللازمة بهذا الشأن لصاحب الصلاحية بشكل دوري.

يجب اتخاذ الإجراءات اللازمة لضمان الالتزام بأحكام هذه السياسة، وذلك من خلال قيام إدارة الأمن السيبراني أو الإدارات ذات العلاقة بمراجعة دورية، واتخاذ إجراءات تصحيحية من قبل صاحب الصلاحية في الجامعة وفقاً للتوصيات المقدمة من قبل مدير الأمن السيبراني حيال أي انتهاك لأي من أحكام هذه السياسة، على أن تكون الإجراءات التأديبية متناسبة مع خطورة الحادثة وفقًا لما يسفر عنه التحقيق بهذا الخصوص، وتتضمن الإجراءات التأديبية على سبيل المثال لا الحصر الآتي:

- سحب صلاحية الوصول إلى البيانات وأصول تقنية المعلومات وأنظمة الجامعة المتصلة بها.
- توجيه إنذار خطي، أو إنهاء خدمة العامل أو حسب ما يراه الجامعة من إجراءات مناسبة.

يستوجب عدم الالتزام بأي من أحكام هذه السياسة -دون الحصول على استثناء مسبق من إدارة الأمن السيبراني - اتخاذ الإجراءات المناسبة وفقًا للسياسات واللوائح المعمول بها في الجامعة، أو حسبما يكون مناسبًا، ووفقًا للشروط التعاقدية مع أي أشخاص أو جهات متعاقد معهم.

12. السياسات والمعايير والإجراءات ذات العلاقة

- DICT.I.06-01.CS.A. V2.0- السياسة العامة للأمن السيبراني وحوكمة البيانات
- DICT.I.06-02.CS.A. V2.0- سياسة الالتزام بالأمن السيبراني وحوكمة البيانات
- DICT.I.06-29.CS.A. V2.0- سياسة التشفير
- DICT.I.06-09.CS.A. V2.0- سياسة إدارة حوادث الأمن السيبراني
- DICT.I.06-10.CS.A. V2.0- سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- DICT.I.06-71.CS.A.V2.0- معايير التشفير
- DICT.I.06-67.CS.A.V2.0- معايير إدارة حوادث الأمن السيبراني
- DICT.I.06-68.CS.A.V2.0- معايير إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- DICT.I.04-37.CS.A.V2.0- إجراءات الحماية من البرمجيات الضارة

13. المراجع

اسم القسم	الضوابط الأساسية للأمن السيبراني	ضوابط الأمن السيبراني للأنظمة الحساسة	ضوابط الأمن السيبراني للعمل عن بعد	ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات	ضوابط الأمن السيبراني للحوسبة السحابية	الآيزو 27001:2013	المعهد الوطني للمعايير والتقنية
الحماية من البرمجيات الضارة						A12.2.1 ,A12.2	
حماية تطبيقات الويب	2-15-1	-	-	-	-	A.6.2.2	-
حماية الأنظمة وأجهزة معالجة المعلومات	2-3-3	2-3-1	-	-	-	-	-

----------نهاية الوثيقة----------