جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة حماية الطابعات والماسحات الضوئية وآلات التصوير

الإصدار: Version 2.0

رمز السياسة:DICT.I.06-36.CS. A. V2.0

جدول المحتويات

1. 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.

2. الرقابة على الوثيقة

1.2 معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة حماية الطابعات والماسحات الضوئية وآلات التصوير	مقيد	V2.0	فعال

2.2 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
V1.0	د. بشار الذيب	2021/03/12	إنشاء
V1.1	د. سامر بني عواد	2022/02/14	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/25	مراجعة وتحديث

3.2 المراجعة والتدقيق

تاريخ المراجعة القادمة
2025/01/01

4.2 قائمة التوزيع

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

5.2 الاعتماد

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

3. 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 سياسة الأمن السيبراني لحماية الطابعات والماسحات الضوئية بالآلات التصوير لمكتب وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

4. الهدف

تحدد هذه السياسة المتطلبات والإجراءات اللازمة لحماية الطابعات والماسحات الضوئية وآلات التصوير، وتوفير التوجيه والمتطلبات الأمنية لجميع موظفي الجامعة والأطراف الخارجية بشأن مسؤولياتهم والتزاماتهم فيما يتعلق باستخدام أصول ومعلومات الجامعة اثناء استخدامهم للطابعات والماسحات الضوئية وآلات التصوير.

5. 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.

6. السياسة

1.6 متطلبات السياسة العامة

1.1.6 يجب على المستخدمين اثناء استخدام الطابعات والماسحات الضوئية وآلات التصوير وآلات تمزيق الورق المشتركة أو الخاصة أن يضمنوا آليات الحماية الكافية للأوراق والمطبوعات لتجنب الوصول غير المصرح به.

2.1.6 يجب أن الأخذ في عين الاعتبار أماكن الأصول التقنية مثل الطابعات وآلات النسخ والماسحات الضوئية حسب متطلبات الأمن المادي التي تم تحديدها في سياسة الأمن المادي والبيئي.

3.1.6 في حال وجود ذاكرة داخلية في الأصول التقنية مثل الطابعات والماسحات الضوئية فيجب أن يتم اتلاف الذاكرة الداخلية بما يتوافق مع متطلبات الجامعة والمتطلبات التشريعية التنظيمية ذات العلاقة قبل التخلص من الأصل.

4.1.6 يجب التأكد من إعدادات الطابعات والماسحات الضوئية وضبط إعداداتها وتحصينها بشكل آمن ومن هذه الإعدادات والتحصينات على سبيل المثال لا الحصر تعطيل الخدمات غير المستخدمة وتغيير كلمات المرور وتطبيق التحديثات وتعطيل خاصية التخزين المؤقت و/أو حذف الملفات المخزنة بشكل تلقائي.

5.1.6 يجب أن يتم إعداد الماسحات الضوئية بإرسال الملفات من خلال بريد إلكتروني تابع للجامعة وعدم تخزين الملفات المرسلة في صندوق البريد الإلكتروني.

6.1.6 يجب تفعيل خاصية التحقق من الهوية في الطابعات والماسحات الضوئية وآلات التصوير المركزية قبل عمليات الطباعة والتصوير والمسح الضوئي.

7.1.6 يجب مراقبة وتخزين سجلات الأحداث الأمنية وفق سياسة سجلات الأحداث ومراقبة الأمن السيبراني.

8.1.6 يجب تقديم التوعية اللازمة للمستخدمين بمخاطر الأمن السيبراني المترتبة على استخدام الطابعات والماسحات الضوئية وآلات التصوير.

9.1.6 يجب توفير التقنيات اللازمة للتخلص من المعلومات المصنفة المطبوعة فور الانتهاء منها (مثل آلة تمزيق الورق بتقنية (Cross-cut shredders) التي تعتمد على تقطيع الورق أفقياً وعمودياً في الوقت ذاته).

7. الأدوار والمسؤوليات

يجب على إدارة الأمن السيبراني:

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

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

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

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

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

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

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

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

يجب على عمادة الاتصالات وتقنية المعلومات:

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

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

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

11.1.7 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 أوعدم التزام بأي أحكام واردة في هذه السياسة الى مدير الأمن السيبراني.

8. ملكية السياسة

المسؤول عن هذه السياسة هو مدير الأمن السيبراني في الجامعة.

9. 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.

10. 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.

11. 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.06-32.CS.A. V2.0- سياسة الأمن المادي والبيئي
- DICT.I.06-10.CS.A. V2.0- سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- DICT.I.06-50.CS.A.V2.0- معايير الأمن المادي
- DICT.I.06-68.CS.A.V2.0- معايير إدارة سجلات الأحداث ومراقبة الأمن السيبراني

12. المراجع

اسم القسم	الضوابط الأساسية للأمن السيبراني	ضوابط الأمن السيبراني للأنظمة الحساسة	ضوابط الأمن السيبراني للعمل عن بعد	ضوابط الأمن السيبراني التواصل للجهات لحسابات الاجتماعي	ضوابط الأمن السيبراني للحوسبة السحابية	الآيزو 27001:2013	المعهد الوطني للمعايير والتقنية
متطلبات السياسة العامة	-	-	-	-	-	A.11.2.9	AC-1, AC-11, MP-1, MP-2, MP-4

----------نهاية الوثيقة----------