جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة أمن الأجهزة المحمولة والأجهزة الشخصية

الإصدار: Version 2.0

رمز السياسة:DICT.I.06-42.CS. A. V2.0

جامعة الإمام عبد الرحمن 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 أمن الأجهزة المحمولة والأجهزة الشخصية	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
V1.0	د. بشار الذيب	2021/03/23	إنشاء
V1.1	د. سامر بني عواد	2022/02/20	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/18	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

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 لتطوير وإنشاء وتنظيم العمليات الأمنية المطلوبة لحماية الأصول المعلوماتية والتقنية وتحدد هذه الوثيقة سياسة أمن الأجهزة المحمولة والأجهزة الشخصية داخل الجامعة 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.

5. الهدف

تهدف هذه السياسة إلى تحديد متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل أخطار الأمن السيبراني الناتجة عن استخدام أجهزة الحاسب سواء المكتبية أو المحمولة، والأجهزة المحمولة (Mobile Devices)، والأجهزة الشخصية للعاملين (Bring Your Own Device "BYOD") داخل الجامعة، وحمايتها من التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي سرية المعلومات وسلامتها وتوافرها.

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 حماية البيانات والمعلومات المُخزّنة في أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) حسب تصنيفها باستخدام الضوابط الأمنية المناسبة لتقييد الوصول إلى هذه المعلومات، ومنع العاملين غير المصرّح لهم من الوصول إليها أو الاطلاع عليها.

2.1.7 يجب تحديث برمجيات أجهزة المستخدمين والأجهزة المحمولة، بما في ذلك أنظمة التشغيل والبرامج والتطبيقات، وتزويدها بأحدث حزم التحديثات والإصلاحات وذلك وفقاً لسياسة إدارة حزم التحديثات والإصلاحات.

3.1.7 يجب تطبيق ضوابط الإعدادات والتحصين (Configuration and Hardening) لأجهزة المستخدمين والأجهزة المحمولة وفقاً لسياسة الإعدادات والتحصين.

4.1.7 يجب عدم منح العاملين في الجامعة صلاحيات مهمة وحساسة (Privileged Access) على أجهزة المستخدمين والأجهزة المحمولة، ويجب منح الصلاحيات وفقاً لمبدأ الحد الأدنى من الصلاحيات والامتيازات.

5.1.7 يجب حذف أو إعادة تسمية حسابات المستخدم الافتراضية في أنظمة التشغيل والتطبيقات.

6.1.7 يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع أجهزة المستخدمين والأجهزة المحمولة.

7.1.7 يجب تزويد أجهزة المستخدمين والأجهزة المحمولة برسالة نصيّة (Banner) لإتاحة الاستخدام المصرّح به.

8.1.7 يجب السماح فقط بقائمة محددة من التطبيقات (Application Whitelisting) واستخدام أنظمة مراقبة البيانات وغيرها لمنع تسرّب البيانات.

9.1.7 يجب تشفير وسائط التخزين الخاصة بأجهزة المستخدمين والأجهزة المحمولة الهامة والحساسة والتي لها صلاحيات متقدمة وفقاً لمعيار التشفير المعتمد في الجامعة.

10.1.7 يجب منع استخدام وسائط التخزين الخارجية، ويجب الحصول على إذن مسبق من إدارة الأمن السيبراني لامتلاك صلاحية استخدام وسائط التخزين الخارجية.

11.1.7 يجب عدم السماح لأجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) المزوّدة ببرمجيات غير محدثة أو منتهية الصلاحية (بما في ذلك أنظمة التشغيل والبرامج والتطبيقات) بالاتصال بشبكة الجامعة لمنع التهديدات الأمنية الناشئة عن البرمجيات منتهية الصلاحية غير المحمية بحزم التحديثات والإصلاحات.

12.1.7 يجب أن تُمنَع أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) غير المزوّدة بأحدث برمجيات الحماية من الاتصال بشبكة الجامعة، لتجنب حدوث أخطار الأمن السيبراني التي تؤدي إلى الوصول غير المصرّح به أو دخول البرمجيات الضارة أو تسرّب البيانات. وتتضمّن برمجيات الحماية برامج إلزامية، مثل: برامج الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware)، وجدار الحماية للمستضيف (Host-Based Firewall)، وأنظمة الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Detection/Prevention).

13.1.7 يجب ضبط أجهزة المستخدمين والأجهزة المحمولة والأجهزة الشخصية (BYOD) بحيث يتم تأمين جميع الأجهزة المحمولة بعد مدة أقصاها (5 دقائق) خلال فترة عدم نشاط الجهاز.

14.1.7 يجب إدارة أجهزة المستخدمين والأجهزة المحمولة مركزياً من خلال خادم الدليل النشط (Active Directory) الخاص بنطاق الجامعة أو نظام إداري مركزي.

15.1.7 يجب ضبط إعدادات أجهزة المستخدمين والأجهزة المحمولة بإدارة الوحدات التنظيمية المناسبة (Domain Controller) لتطبيق السياسات الملائمة وتثبيت الإعدادات البرمجية اللازمة.

16.1.7 يجب تنفيذ سياسات النطاق المناسبة (Group Policy) في الجامعة وتطبيقها في جميع أجهزة المستخدمين والأجهزة المحمولة لضمان التزام الجامعة بالضوابط التنظيمية والأمنية.

17.1.7 تسمح الجامعة للعاملين فيها استخدام الأجهزة الشخصية (BYOD "Bring Your Own Device") داخل الجامعة أو الوصول إلى أصول معلوماتها أو معالجتها في حالة وجود متطلبات عملية وبعد تطبيق الضوابط اللازمة لذلك ومنها (استخدام أنظمة تشغيل وبرامج مرخصة).

18.1.7 يجب ضمان أن استخدام الأجهزة المحمولة الخاصة بالجامعة بناءً على ما تتطلبه مصلحة أعمال الجامعة ولا تكون لأغراض شخصية وتوعية العاملين بذلك.

19.1.7 يجب على الجامعة القيام بتحديد جميع أنواع ونماذج الأجهزة المقبولة المسموح باستخدامها داخل الجامعة.

20.1.7 يجب على الجامعة القيام بتحديد وحفظ ومراجعة جميع الأجهزة المحمولة المسجلة بشكل دوري.

21.1.7 يجب على الجامعة القيام باتخاذ التدابير اللازمة للحماية من الوصول غير المصرح به في حالة تم فقدان أو سرقة الأجهزة المحمولة.

22.1.7 يجب أن تتم تهيئة جميع الأجهزة المحمولة المتصلة بشبكات الجامعة بصورة آمنة، لكي تتوافق مع أدنى متطلبات الجامعة الأمنية.

23.1.7 يحق للعاملين المصرح لهم من قبل إدارة الأمن السيبراني في الجامعة الوصول إلى جميع البيانات المخزنة على أي جهاز ينتمي إلى الجامعة، ويشمل ذلك رسائل البريد الإلكتروني والمستندات وتسجيلات المكالمات الهاتفية والاتصالات المرسلة أو المخزنة على موارد الجامعة.

24.1.7 يمنع نسخ أي معلومات سرية أو تبادلها بأي شكل من الأشكال بما في ذلك على سبيل المثال لا الحصر، الأقراص المضغوطة أو وسائط التخزين الخارجية (USB) أو مرفقات البريد الإلكتروني وما إلى ذلك ما لم يكن مصرحاً بها لأغراض وعمليات الجامعة.

25.1.7 يجب عدم تصوير المرافق المؤمَّنة داخل الجامعة أو البيانات التابعة للجامعة باستخدام الكاميرات أو كاميرات الهواتف المحمولة دون الحصول على الموافقة اللازمة.

26.1.7 يجب عدم استخدام الأجهزة المحمولة من أجل التصوير، تسجيل مقاطع فيديو، تسجيل مقطع صوتية أو أي نوع من أنشطة التجسس أو التنصت.

27.1.7 يجب الإبلاغ عن فقدان أجهزة الحاسوب المحمولة والأجهزة الشخصية التابعة للجامعة والمساعدات الرقمية الشخصية على الفور إلى إدارة الأمن السيبراني.

28.1.7 يجب إدارة الأجهزة المحمولة والأجهزة الشخصية (BYOD) مركزياً باستخدام نظام إدارة الأجهزة المحمولة ("Mobile Device Management" MDM).

2.7 أمن أجهزة المستخدمين المكتبية والمحولة

1.2.7 يجب تخصيص أجهزة المستخدمين للفريق التقني ذي الصلاحيات الهامة، وأن تكون معزولة في شبكة خاصة لإدارة الأنظمة (Network Management) ولا ترتبط بأي شبكة أو خدمة أخرى.

2.2.7 يجب ضبط إعدادات أجهزة المستخدمين الهامة والحساسة والتي لها صلاحيات متقدمة لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني، مع عدم إمكانية إيقافه عن طريق المستخدم.

3.2.7 يجب على العاملين عدم تثبيت أنظمة جديدة على أجهزة الحاسب المكتبية أو المحمول من غير إذن مناسب من إدارة الأمن السيبراني في الجامعة.

4.2.7 يمنع استخدام برامج الألعاب على أنظمة الجامعة ولا يسمح بتثبيتها أو نقلها أو استخدامها داخل شبكة الجامعة.

5.2.7 يجب أن يخضع تقديم البرامج المجانية والتشاركية (سواء تم تحميلها من الإنترنت أو تم الحصول عليها من خلال أي وسائط أخرى) إلى الأصول التقنية والمعلوماتية في الجامعة لعملية تقييم وموافقة رسمية.

6.2.7 يجب حمل أجهزة الحاسب المحمولة في حقائب اليد لمنع الأضرار والوصول غير المصرح به عند السفر.

7.2.7 يجب منع وصول الأجهزة المحمولة للأنظمة المحمولة إلا لفترة مؤقتة وذلك بعد إجراء تقييم أخطار الأمن السيبراني والحصول على الموافقات من إدارة الأمن السيبراني.

8.2.7 يجب تشفير أقراص الأجهزة المحمولة التي تملك صلاحية الوصول للأنظمة الحساسة تشفيراً كاملاً.

9.2.7 يجب أن يكون جميع عاملي الجامعة على علم أن أجهزتهم المحمولة التابعة للجامعة جزء من شبكة الجامعة وأنهم يخضعون لنفس القواعد واللوائح التي تنطبق على الأصول المملوكة للجامعة.

10.2.7 يجب ضمان تأمين أجهزة المستخدمين مادياً داخل مباني الجامعة وتوعية العاملين بذلك.

3.7 أمن الأجهزة الشخصية (BYOD)

1.3.7 يجب فصل وتشفير البيانات والمعلومات الخاصة بالجامعة المخزنة على الأجهزة الشخصية للعاملين (BYOD).

2.3.7 يجب أن يكون وصول العاملين لأنظمة الجامعة للمصرح لهم فقط وفقاً لحاجة العمل فقط.

3.3.7 أمن جميع الأجهزة الشخصية المادي وأمن الوصول المنطقي لها (الحاسوب المحمول، أو جهاز لوحي، أو أجهزة الشبكة، أو أجهزة المساعد الرقمي الشخصي أو الهواتف الذكية أو وسائط التخزين الخارجية وغيرها) يقع ضمن مسؤوليات مالكها فقط. كما أن الجامعة غير مسؤوله عن أي تلف للبيانات أو كشف عن المعلومات الشخصية من أجهزة العاملين الشخصية عند اتصالهم بشبكة الجامعة أو عندما يكون الجهاز قد تم فقده/عزله داخل الجامعة.

4.7 متطلبات أخرى

1.4.7 يجب إجراء نسخ احتياطي دوري للبيانات المخزّنة على أجهزة المستخدمين والأجهزة المحمولة، وذلك وفقاً لسياسة إدارة النسخ الاحتياطي المعتمدة في الجامعة.

2.4.7 يجب حذَف بيانات الجامعة المُخزّنة على الأجهزة المحمولة والأجهزة الشخصية (BYOD) في الحالات التالية:

- فقدان الجهاز المحمول أو سرقته.
- انتهاء أو إنهاء العلاقة الوظيفية بين المستخدم والجامعة.
- إعادة استخدام الأجهزة المحمولة أو عند التخلص منها خصوصًا التي يتم استخدامها للدخول على الخدمات السحابية.

3.4.7 يجب توعية العاملين حول آلية استخدام الأجهزة ومسؤولياتهم تجاهها وفقاً لسياسة الاستخدام المقبول للأصول المعتمدة في الجامعة وإجراء جلسات توعية خاصة بالمستخدمين ذوي الصلاحيات الهامة والحساسة.

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 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.

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

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

يجب على عمادة الاتصالات وتقنية المعلومات:

9.1.8 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:

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

11.1.8 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.06-04.CS.A. V2.0- سياسة إدارة الأصول

- ❖ DICT.I.06-27.CS.A. V2.0- سياسة الاستخدام المقبول للأصول
- ❖ DICT.I.06-60.CS.A.V2.0- معايير تصنيف الأصول
- ❖ DICT.I.06-62.CS.A.V2.0- معايير إدارة الأصول

13. المراجع

اسم القسم	الضوابط الأساسية للأمن السيبراني	ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات	ضوابط الأمن السيبراني للأنظمة الحساسة	ضوابط الأمن السيبراني للحوسبة السحابية	ضوابط الأمن السيبراني للعمل عن بعد	الآيزو 27001:2013	المعهد الوطني للمعايير والتقنية (NTIS)
سياسة أمن الأجهزة المحمولة والأجهزة الشخصية BYOD	6-2	4-2	5-52-2	1-ش-5-2	5-2	A.6.2.1	AC-19, AC-7(2)

----------نهاية الوثيقة----------