جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة الأمن المادي والبيئي

الإصدار: Version 2.0

رمز السياسة:DICT.I.06-32.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 الأمن المادي والبيئي	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
V1.0	د. بشار الذيب	2021/03/20	إنشاء
V1.1	د. سامر بني عواد	2022/02/09	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/21	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

تُعتبر حماية المعلومات وأصولها عنصراً أساسياً لنجاح الجامعة؛ وتحقيقاً لهذه الغاية تقوم إدارة الأمن السيبراني بإدارة العمليات الأمنية اللازمة لحماية أصول الجامعة المعلوماتية والتقنية. تحدد هذه الوثيقة سياسة الوصول المادي داخل الجامعة، كما تحدد الأمن المادي والبيئي بناءً على أفضل الممارسات والمتطلبات التشريعية ذات العلاقة.

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

5. الهدف

تهدف سياسة الأمن المادي والبيئي إلى تعزيز إجراءات حماية المنشأة وأصولها المعلوماتية والتقنية ضد أي تهديدات أو أخطار محتملة ووضع متطلبات الوصول المادي وضبطه ومراقبته.

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 نطاق الأمن المادي

1.1.7 يجب تطبيق المتطلبات الأمنية اللازمة لدخول مرافق الجامعة وتشمل التعرف على الأشخاص والتحقق من وجود التصريح اللازم للدخول.

2.1.7 توفير الوسائل المادية لتأمين المنشأة مثل الأسوار والسياج والبوابات الأمنية للحفاظ على سلامة المعلومات والبيانات ومنسوبي الجامعة.

3.1.7 يجب تجهيز نطاق الأمن المادي لكامل الجامعة بما في ذلك بوابة الدخول للمبنى الرئيسي بكاميرات المراقبة (CCTV) وذلك لمراقبة أي نشاط مشبوه أو تهديدات الخارجية (إن أمكن ذلك).

4.1.7 يجب حماية جميع بوابات الدخول/الخروج الرئيسة ضد الوصول غير المصرح به بآليات تحكم كالقضبان أو أجهزة الإنذار أو الأقفال المناسبة وغيرها، كما يجب قفل النوافذ والأبواب عند خلو أماكن العمل من العاملين.

5.1.7 توفير جهاز الفحص بالأشعة ضد المتفجرات والمعادن عند بوابات الدخول وتطبيق التعليمات الخاصة بفحص الحقائب.

2.7 ضوابط الدخول المادي

1.2.7 تُزود جميع بوابات الدخول والخروج الرئيسة للمبنى أو للجامعة بحراس أمن على مدار الساعة وطوال اليوم، وتكلف إدارة الأمن والسلامة بالمهام المناسبة وتبلغهم بها، ويجب تبليغ الاستقبال أو العاملين المختصين فورًا عن أي أنشطة مشبوهة أو أي وصول غير مصرح به من مصدر خارجي.

2.2.7 يجب تزويد جميع الأبواب والأسوار الخارجية بأجهزة المناسبة (كاميرات مراقبة، أقفال ذكية، ....) لتأمين نطاق الأمن الداخلي ومراقبتها واختبارها بشكل دوري.

3.2.7 يجب على جميع العاملين في الجامعة ارتداء بطاقة تعريف بالهوية (التصريح الأمني للدخول) في جميع الأوقات كما يجب أن تكون مرئية.

4.2.7 يجب على إدارة الأمن والسلامة توثيق جميع الأنشطة المتعلقة بإنشاء واتلاف بطاقات التعريف بالهوية (التصريح الأمني للدخول) في سجل خاص (Log Sheet).

5.2.7 لا يُسمح للذين لا يحملون بطاقة التعريف بالهوية (التصريح الأمني للدخول) بالدخول إلى أي مرفق من مرافق الجامعة الداخلية، الا بعد أخذ الموافقة من الإدارات المعنية.

6.2.7 يجب على إدارة الأمن السيبراني والمسؤولين عن أعمال الجامعة مراجعة القائمة الحالية لجميع العاملين الذين يمتلكون التصريح الأمني للدخول إلى المرافق بشكل دوري.

7.2.7 يجب تقييد الوصول الى المناطق الهامة والحساسة) مثل غرف الاتصالات ومعالجة المعلومات)، وأن يقتصر الوصول على العاملين المصرح لهم فقط.

8.2.7 يجب تصنيف مرافق الجامعة استناداً على تصنيف المعلومات التي يتم تداولها ومعالجتها فيها.

9.2.7 لا يسمح بمنح عاملي الأطراف الخارجية صلاحية الوصول الى المناطق الهامة والحساسة إلا عند الضرورة ويجب العمل على اصدار تراخيص الدخول الأمني بالتنسيق مع الادارات ذات العلاقة كما يجب مرافقة الاطراف الخارجية من قبل الإدارة المستفيدة ومراقبتهم طوال فترة تواجدهم في الأماكن الهامة والحساسة.

10.2.7 يجب الاحتفاظ بسجلات الدخول إلى المناطق المؤمنة ومراجعتها بشكل دوري للكشف عن الحوادث الأمنية والاستجابة لها، ويجب تبليغ إدارة الأمن السيبراني وإدارة الأمن والسلامة فورًا عن أي أنشطة مشبوهة أو انتهاكات أمنية واضحة.

11.2.7 يجب تقييد الوصول لمناطق التحميل والتنزيل (Loading And Unloading Areas) الخاصة بمواقع الجامعة للعاملين المصرح لهم فقط.

12.2.7 يجب فحص جميع المواد الواردة للتأكد من خلوها من اي مواد خطرة أو تهديدات محتملة قبل نقلها من منطقة التحميل والتنزيل إلى مكان الاستخدام.

13.2.7 يجب تسجيل جميع المواد الصادرة والواردة وفقًا لسياسة إدارة الأصول عند دخولها إلى الموقع.

14.2.7 يجب تزويد المناطق المؤمنة كمركز معالجة البيانات وغرف المولدات ومصادر الطاقة الاحتياطية (UPS) وغرف وحدات معالجة الهواء، والمناطق التي يتم فيها معالجة المعلومات الهامة والحساسة بأنظمة التحقق من الهوية متعدد العناصر مثل بطاقات ضبط الدخول والسمات الحيوية "مثل بصمة الأصبع".

15.2.7 يجب أن يتم إلغاء صلاحية بطاقة الدخول بعد استقالة العامل أو إنهاء عقده أو نقله إلى جهة أخرى.

16.2.7 يُمنع على العاملين مشاركة بطاقات الدخول إلى المبنى مع الغير.

17.2.7 تمنح الاطراف الخارجية المسؤولة عن خدمات الدعم وصولًا مقيدًا إلى المناطق المؤمنة عند الحاجة فقط ويتم مراقبة هذا الوصول.

3.7 ضوابط دخول الزوار

1.3.7 يفضل أن يكون لجميع مواقع الجامعة نقاط تفتيش أمنية (إن أمكن ذلك) في منطقة الاستقبال مزودة بحراس الأمن، حيث لا يُسمح للزوار بالدخول إلا بعد تسجيلهم في سجل الزوار على أن يتم التحقق من تصريح الدخول، وغرض الزيارة قبل السماح لهم بالدخول إلى المرافق.

2.3.7 يجب على عاملي الاستقبال القيام بالاتصال واخذ موافقة الشخص الذي سيقابله الزائر قبل السماح له بالدخول.

3.3.7 يجب مرافقة جميع الزوار في المناطق المؤمنة داخل الجامعة حتى انتهاء الغرض من الزيارة، ويجب مرافقتهم حتى خروجهم من مرافق الجامعة.

4.3.7 يجب على جميع الزوار ارتداء بطاقة الزائر/ بطاقة الدخول في جميع الأوقات داخل المبنى، والابلاغ عن أي مخالفة في هذا الخصوص.

5.3.7 إيقاف جميع الزوار والأشخاص الذين لا يحملون بطاقة تعريف هوية واضحة.

6.3.7 يجب ألا يُسمح للزوار بالوصول إلى أجهزة الجامعة أو إلى أي من أصول معالجة المعلومات الأخرى دون إذن مسبق.

7.3.7 يجب تسجيل معلومات زوار الجامعة عند الاستقبال في "سجل الزوار" والاحتفاظ بمعلوماتهم ومراجعتها بشكل دوري، ويجب أن يحتوي السجل، على سبيل المثال لا الحصر، ما يلي:

- اسم الزائر
- هوية الزائر
- اسم الجهة التي يعمل بها الزائر
- الغرض من الزيارة
- اسم الشخص الذي سيقابله الزائر ورقم هاتفه
- وقت الدخول
- وقت المغادرة
- تاريخ الزيارة

4.7 تأمين مكاتب العمل

1.4.7 يجب تأمين جميع المناطق الهامة والحساسة بشكل دائم (مثل: مراكز البيانات، وغرف الخوادم، وغرف المولدات ومصادر الطاقة الاحتياطية، والغرف الكهربائية، وغرف وحدات معالجة الهواء وغرف الأرشفة والمناطق التي يتم فيها معالجة المعلومات الحساسة)، ولا يُسمح للزوار بالدخول إلى هذه المناطق مالم يتم الحصول على الموافقات اللازمة من صاحب الصلاحية.

2.4.7 من أجل تأمين المرافق والغرف والمكاتب، يجب أن تأخذ إدارة الأمن والسلامة في الاعتبار التدابير الأمنية التالية:

- إدراج لوائح الصحة والسلامة ذات الصلة.
- تحديد مواقع المناطق المؤمنة أو المرافق الرئيسية لتجنب وصول العامة إليها.
- يجب أن يكون لمباني ومرافق الجامعة تعريف رمزي يحدد الغرض منها، ويجب عدم وضع لافتات واضحة سواءً داخل المبنى أو خارجه تبيّن وجود أنشطة معالجة المعلومات في هذه المرافق.
- عدم السماح للعامة بالاطلاع على سجل ودليل الهواتف الداخلية التي تحدد مواقع مرافق معالجة المعلومات الحساسة.
- وضع لافتات تنص على "للعاملين المصرح لهم " أو "وصول مقيد" في جميع مداخل المناطق المؤمنة.
- تطبيق إجراءات وإرشادات السلامة والأمن المادي للعمل في المناطق المؤمنة الموثقة رسميًا والالتزام بها.
- إقفال مكاتب العاملين بعد ساعات الدوام أو عندما لا تكون قيد الاستعمال.
- تثبيت أجهزة إنذار الكشف عن التسلل في أماكنها المخصصة لتغطي الأبواب الخارجية والنوافذ التي يمكن الوصول إليها والمداخل الأخرى للمبنى.

5.7 الحماية من التهديدات البيئية والخارجية

1.5.7 يجب تحديد وتوثيق المستخدمين المصرح لهم الدخول لبيانات الجامعة من قبل مدراء التطبيق متى أمكن. كما يجب متابعة وتسجيل عملية منح/الغاء الصلاحيات.

2.5.7 يجب مراقبة مستويات درجة الحرارة والرطوبة داخل المناطق المؤمنة لتحديد الظروف التي قد تؤثر سلبًا على تشغيل المعدات ولاتخاذ الإجراءات التصحيحية.

3.5.7 يجب أن تكون المناطق المؤمنة التي يشغلها العاملين مجهزة بإضاءات الطوارئ التي تعمل تلقائياً عند انقطاع التيار الكهربائي للسماح بإخلاء العاملين في حالات الطوارئ.

4.5.7 يجب ألا يتم تخزين المواد الخطرة أو القابلة للاحتراق بالقرب من الأصول المعلوماتية والتقنية حيث إنها قد تشكل تهديدًا أو تجعل الأصول المعلوماتية والتقنية عرضة للخطر، ويجب تخزين وسائط النسخ الاحتياطي القابلة للإزالة في خزائن مضادة للاحتراق.

5.5.7 يجب على الجامعة أو الجهة المالكة للمبنى توفير أجهزة الكشف عن الحرائق وإخمادها وأجهزة التكييف وأجهزة التحكم في الرطوبة وأنظمة الحماية من العوامل البيئية الأخرى.

6.5.7 يجب أن توفر إدارة الأمن والسلامة للعاملين التدريب الكافي لاستخدام معدات مكافحة الحرائق، ويجب إجراء تجربة إخلاء المبنى دورياً.

7.5.7 يجب أن يتم توفير وسائل إطفاء الحريق (طفاية الحريق، أغطية كتم النار، كرات الإطفاء الذاتي) في الجامعة بعدد كافي وتوزيع مناسب مما يضمن سهولة الوصول إليها.

8.5.7 يجب أن تكون أجهزة الكشف عن الدخان موجودة في كل طابق من طوابق مكاتب العاملين وداخل غرفة الخادم، والتي يجب أن تُطلِق الإنذار تلقائيًا بمجرد اكتشاف الدخان.

9.5.7 يجب أن تضمن إدارة الشؤون الأمن والسلامة فحص معدات السلامة من الحرائق بانتظام وفقًا لتعليمات الشركة المصنعة أو التنسيق مع مالك المبنى للقيام بذلك، كما يجب على مسؤول المعدات الحفاظ على مستند الصيانة.

10.5.7 يجب الأخذ في الاعتبار تدابير وقائية أخرى عند اللزوم للحماية من التهديدات كالفيضانات والزلازل والاضطرابات المدنية وغيرها من الكوارث الطبيعية أو البشرية.

11.5.7 يجب أن يُؤخذ في الاعتبار عند تحديد الضوابط البيئية لوائح ومعايير الصحة والسلامة ذات الصلة، وأن يُؤخذ في الحسبان التهديدات الأمنية التي تواجهها المباني المجاورة.

12.5.7 يجب ان تضمن إدارة الأمن والسلامة ما يلي:

- عدم وجود مرافق معالجة المعلومات في منطقة بيئية غير مستقرة.
- عدم وجود مرافق معالجة المعلومات بالقرب من أي مرافق مجاورة خطيرة (مثل المختبرات الكيميائية وغيرها).
- استيفاء الأجهزة المثبتة للكشف عن الحرائق ومكافحتها بالمتطلبات المحددة من الشركات المصنعة.
- تخزين المعدات البديلة والوسائط الاحتياطية على بعد مسافة آمنة من الموقع الرئيسي لتجنب التعرض لذات الكارثة التي تؤثر على الموقع الرئيسي.

6.7 أمن المعدات

1.6.7 يجب أن تتأكد عمادة الاتصالات وتقنية المعلومات من تطبيق ما يلي:

- يجب أن تكون جميع عناصر أنظمة الإنتاج في الجامعة بما في ذلك، على سبيل المثال لا الحصر، الخوادم وجدران الحماية، والموجهات وغيرها، موجودة داخل منطقة مؤمنة مثل مركز البيانات أو غرفة الخادم.
- يجب ان تُعامل جميع عناوين مواقع الأصول المعنية بمعالجة البيانات بشكل سري ولا يتم الإفصاح عنها للأشخاص غير المصرح لهم.

2.6.7 يجب وضع المعدات البديلة أو الأجهزة الاحتياطية في أماكن مؤمنة مغلقة، ويجب كذلك استخدام آليات القفل المتاحة لحماية هذه المصادر عندما تكون غير مستخدمة أثناء ساعات العمل أو خارجها.

3.6.7 يجب تثبيت مضادات الصواعق على جميع المباني التي تحتوي على مرافق معالجة المعلومات الحساسة ومرافق الاتصالات (إن أمكن ذلك).

4.6.7 يجب تحديد مقرات المعدات لتقليل الوصول غير اللازم إلى مناطق العمل.

5.6.7 يجب عزل المواد التي تتطلب حماية خاصة لتقليل المستوى العام للحماية اللازمة.

6.6.7 يجب حماية المعدات التي تعمل على معالجة المعلومات الحساسة لتقليل أخطار تسريب المعلومات.

7.6.7 يجب رصد الظروف البيئية لمعرفة الظروف التي قد تؤثر سلبًا على تشغيل أمن معالجة المعلومات.

8.6.7 يجب تعيين مرافق معالجة المعلومات للجامعة للحد من أخطار استعراض المعلومات من قبل أشخاص غير مصرح لهم أثناء استخدامها.

9.6.7 يجب عزل مرافق معالجة المعلومات التي تقوم بمعالجة البيانات السرية لتطبيق ضوابط إضافية عليها.

10.6.7 يجب منع دخول السوائل والمواد الخطرة للأماكن الحساسة التابعة للجامعة مثل (مراكز البيانات، مراكز التعافي، أماكن معالجة المعلومات، مراكز المراقبة وغرف اتصالات الشبكة) وغيرها.

11.6.7 يجب رصد جميع الظروف البيئية التي تؤثر على تشغيل مرافق معالجة المعلومات السرية (كالحرارة والرطوبة).

12.6.7 يجب اعتماد جميع الضوابط اللازمة للحد من أخطار أي تهديدات مادية محتملة.

7.7 المرافق الداعمة

1.7.7 يجب أن تتأكد إدارة الأمن والسلامة من تطبيق ما يلي:

- أن تكون جميع المرافق الداعمة، مثل الكهرباء، وإمدادات المياه، والتدفئة والتهوية وتكييف الهواء ملائمة للأنظمة التي تدعمها.
- إجراء فحص دوري للمرافق الداعمة للتأكد من أنها تعمل على النحو المطلوب، مع الاحتفاظ بالسجلات المناسبة.
- تسهيل مرافق معالجة المعلومات التي تدير عمليات الجامعة السرية من خلال مصادر الطاقة الاحتياطية لدعم تشغيلها المستمر.
- تسهيل مرافق معالجة المعلومات من خلال وضع مفاتيح إيقاف تشغيل التيار الكهربائي في الحالات الطارئة بالقرب من مخارج الطوارئ لتسهيل سرعة انخفاض الطاقة الكهربائية في حالة الطوارئ.

8.7 أمن الكابلات

1.8.7 يجب أن تضمن إدارة الأمن والسلامة بالتعاون مع عمادة الاتصالات وتقنية المعلومات ما يلي:

- أن تكون الإمدادات الكهربائية وأسلاك الاتصالات تحت الأرض قدر الإمكان، أو أن يتم حمايتها بشكل كاف بطرق بديلة.

- حماية كابلات الشبكة من الاعتراض غير المصرح به أو التلف، على سبيل المثال باستخدام أنابيب لحماية الكابلات أو عن طريق تجنب مسارات المناطق العامة.
- توسيم الكابلات والمعدات بشكل واضح للتعرف عليها بسهولة، وذلك للتقليل من أخطاء المعالجة، مثل إصلاح كابلات الشبكة الخاطئة من غير قصد.
- التحكم في الوصول المادي إلى خطوط نقل نظام المعلومات لمنع التنصت، أو التعديل أثناء النقل، أو التعطيل أو التلاعب.
- يجب على الجامعة، حيثما اقتضى الأمر ووفقًا للنهج القائم على المخاطر، استخدام الحماية الكهرومغناطيسية لحماية الكابلات.
- تقوم إدارة الأمن والسلامة بالتعاون مع عمادة الاتصالات وتقنية المعلومات بإجراء عمليات مسح تقنية وفحوصات دورية لضمان عدم ارتباط الأجهزة غير المصرح بها بالكابلات.
- حماية كابلات الاتصالات وشبكة البيانات من زراعة أجهزة التنصت (Wiretapping).
- في حال إن كانت متطلبات الكفاءة والتوافر عالية، يجب على الجامعة الاستفادة من كابلات الألياف البصرية لتحسين الموثوقية والحماية والكفاءة.
- عزل كابلات الطاقة الكهربائية بشكل كافي عن كابلات شبكة البيانات لتجنب تداخلها.
- عزل كابلات شبكة البيانات وحمايتها من الاعتراض غير المصرح به أو التلف عن طريق توجيه مساراتها عبر المناطق المحمية.
- إخفاء شبكة بيانات مرافق معالجة المعلومات وكابلات الطاقة الكهربائية.
- التحكم في الوصول إلى غرف ألواح توزيع الكابلات.

9.7 صيانة المعدات

1.9.7 يجب على عمادة الاتصالات وتقنية المعلومات أن تضمن ما يلي:

- صيانة جميع البنية التحتية لنظام المعلومات المستخدمة للإنتاج وفقًا لفترات ومواصفات الخدمات الموصي بها من قبل المورد، ولا يقوم بالإصلاحات وتقديم الخدمات إلا عاملون الصيانة المؤهلون والمصرح لهم بذلك.
- إجراء صيانة شاملة لكامل النظام بما في ذلك استبدال/ إصلاح الأجزاء والأنظمة التالفة بشكل منتظم.

- إنشاء خطة صيانة لجميع مكونات نظام المعلومات وإبلاغ أصحاب المصلحة.
- تطبيق الضوابط اللازمة قبل الصيانة لمنع تسرب معلومات الجامعة الحساسة.
- الاحتفاظ بسجلات الصيانة المناسبة ومراجعتها.
- إجراء صيانة المعدات من قبل العالمين المصرح لهم فقط.

10.7 أمن استخدام الأجهزة خارج الجامعة

1.10.7 بغض النظر عن الملكية، يجب أن يكون استخدام أي من أجهزة معالجة المعلومات خارج مباني الجامعة مصرح له.

2.10.7 يجب مراعاة تعليمات الشركة المصنعة لحماية الأجهزة عند وجودها خارج مباني الجامعة.

3.10.7 يجب أن تكون الأجهزة المصرح لها إخراجها من الجامعة مطابقة لمعايير الأجهزة الموجودة داخل الجامعة والمستخدمة للأغراض ذاتها.

4.10.7 يجب أن تحتفظ عمادة الاتصالات وتقنية المعلومات بسجلات دقيقة ومحدثة لجميع الأجهزة التي يتم نقلها خارج الجامعة.

5.10.7 يجب الحصول على تصريح من إدارة الأمن السيبراني لنقل الأجهزة أو المعلومات أو البرمجيات خارج الجامعة.

6.10.7 يجب تطبيق الضوابط بناء على المخاطر الأمنية المحددة، مع الأخذ في الاعتبار المخاطر المرتبطة بالعمل خارج مبنى الجامعة.

7.10.7 يجب على المسؤول عن الأصول التأكد من أنه يتم اتخاذ الإجراءات السليمة لوضع الأجهزة خارج الجامعة وفقًا لمتطلبات السلامة الخاصة بذلك الأصل.

8.10.7 يجب على المسؤولين عن الأصول ضمان استمرار استخدام الأجهزة الموضوعة خارج الجامعة في الامتثال للسياسات الأمنية المعتمدة في الجامعة.

9.10.7 يجب على العاملين الحفاظ على أمن الأجهزة المحمولة مثل أجهزة الحاسب المحمولة والأجهزة اللوحية وغيرها من خلال:

- عدم ترك الجهاز مفتوحًا أو قيد تسجيل الدخول أو قيد التشغيل عند عدم استخدام الجهاز.
- عدم ترك الجهاز والوسائط دون رقابة في المناطق العامة أو في أي مناطق أخرى غير آمنة.
- عدم ترك الجهاز في الجامعة أو منطقة العمل بعد نهاية أوقات الدوام الرسمية دون استخدام ضوابط أمنية (مثل الإقفال على الأجهزة في منطقة آمنة مخصصة).
- عدم استخدام شبكة الانترنت اللاسلكي (Wi-Fi) المفتوحة والغير موثوقة في الأماكن العامة.
- وضع أجهزة تقنية المعلومات المحمولة مثل الحواسيب والأجهزة المحمولة مع الأمتعة اليدوية أثناء السفر.
- إبلاغ إدارة الأمن السيبراني وعمادة الاتصالات وتقنية المعلومات على الفور عند فقدان الجهاز واتباع التوجيهات المقدمة من إدارة الأمن السيبراني.

11.7 إدارة الوسائط القابلة للإزالة والتعامل معها

1.11.7 يجب وضع الإجراءات المناسبة لضمان أمن الوسائط القابلة للإزالة وسرية المعلومات المخزنة فيها.

2.11.7 إذا لم تعد هناك حاجة إلى هذه المعلومات، فإنه يجب جعل محتويات الوسائط القابلة للإزالة والتي سيتم إزالتها من الأصل غير قابلة للاسترداد بالطرق التالية:

- يتم تقطيع/ إتلاف الأوراق والأقراص المدمجة وأقراص الفيديو الرقمية (DVD) بواسطة آلات التقطيع القادرة على إتلاف الأقراص المدمجة والأقراص المرنة.
- إتلاف الوسائط القابلة للإزالة)الأقراص الصلبة ووسائط التخزين الخارجية الممغنطة) من خلال عملية إزالة المغنطة.
- في حال عدم توفر جهاز تقطيع الورق أو إزالة المغنطة، فإنه يتم إتلاف الوسائط عن طريق كسرها أو حرقها أو إتلافها بطريقة لا يمكن استعادتها.
- يجب تخزين جميع وسائط التخزين الخارجية في بيئة آمنة.

- يجب تقييد استخدام أجهزة وسائط التخزين الخارجية وفي حال وجود استثناء ويجب أن تُرخص جميع الاستثناءات من قبل إدارة الأمن السيبراني، كما يجب توثيق جميع الأدلة وتخزينها.

12.7 التصرف الآمن في الأجهزة وإعادة الاستخدام

1.12.7 يجب أن لا يتم التصرف في الأجهزة أو أنظمة الحاسب التي تحتوي على وسائط تخزين أو لا يُعاد استخدامها إلا بعد التأكد من إزالة جميع البيانات السرية والبرمجيات المرخصة أو استبدالها بصورة آمنة.

2.12.7 في حالة استرجاع الأجهزة المخصصة للمستخدم (الحاسب المحمول أو الجامعي)، فإنه لا يتم النظر في إعادة استخدام هذه الأجهزة إلا بعد التهيئة المناسبة لأنظمة الحاسب (الأقراص الصلبة).

3.12.7 يجب أن يكون لأي طلب للتصرف في الأجهزة مبررًا مناسبًا، وأن يكون مصرحًا به من قبل المسؤولين عن الأصول أو رئيس الإدارة، وكذلك يجب الأخذ في الاعتبار متطلبات الأعمال التشغيلية والمتطلبات القانونية للجامعة.

4.12.7 يجب على عمادة الاتصالات وتقنية المعلومات التأكد من إزالة جميع البيانات السرية والبرمجيات المرخصة أو استبدالها بصورة آمنة قبل تقديم التوصية النهائية للتصرف في الأجهزة.

5.12.7 يجب على العاملين المكلفين بمسؤولية التصرف في المعدات والأجهزة والوسائط الاحتفاظ بسجلات كافية لكل مما يلي:

- طلب اتلاف الأجهزة.
- توصية إدارة الأمن السيبراني.
- سجلات أدلة التصرف الموقعة من قبل عاملين محددين من الإدارة.

6.12.7 يجب توعية منسوبي الجامعة حول أفضل الممارسات المتعلقة بالأمن المادي مثل سياسة الجامعة النظيف والشاشة الخالية وضمان التزامهم بها.

13.7 إزالة الأصول وضوابط نقل الوسائط المادية

1.13.7 يجب على إدارة الأمن والسلامة وضع ضوابط مناسبة للحماية من الوصول غير المصرح به أو سوء الاستخدام أو الإتلاف أثناء نقل هذه الوسائط إلى موقع خارج الجامعة.

2.13.7 لحماية أصول المعلومات أو الوسائط التي يتم نقلها بين المواقع، يتم تحديد الإرشادات التالية:

- يجب تحديد العاملين المعتمدين المسؤولين عن تحرك أي من الوسائط وتطبيقات البرمجيات من مكان داخل الجامعة إلى مكان خارجه.
- يجب الاحتفاظ بسجلات حركة الوسائط ويتعين على العاملين اتخاذ الإجراءات الكافية لضمان أمن الوسائط أثناء نقلها إلى موقع خارج الجامعة.
- عندما يتم أخذ نسخة ورقية من المعلومات السرية من مقر الجامعة، فإنه يجب عدم تركها دون رقابة في السيارة أو في غرفة الفندق أو في مطعم أو في أي مكان آخر.

14.7 التعامل مع المعاملات التي ترد خارج وقت الدوام الرسمي

1.14.7 يجب التأكد من ان المعاملات موجهة للجامعة وأنها مصنفة وعليها رقم الصادر وتاريخه ومراعاة ألا يكون التاريخ قديم.

2.14.7 يجب التأكد من أن تكون المعاملة مظرفة ومختتمة وأنها بحالة جيدة.

3.14.7 يجب التوقيع بوضوح في سجل استلام المعاملات وادراج وقت وتاريخ استلام المعاملة.

4.14.7 على عاملي الاستقبال بعد استلام المعاملات، تسليمها مباشرة لمكتب المدير ويكون ذلك في بيان مستقل ويدرج فيه وقت التسليم.

5.14.7 إذا لم يتواجد أحد في مكتب المدير يتم التحفظ على المعاملات في الخزنة الخاصة بذلك ثم الاتصال برئيس الجامعة لأخذ التوجيه، وتسجيل ذلك في خانة الاجراء المتخذ على المعاملة.

8. الأدوار والمسؤوليات

تكون صلاحية الاعتماد لضوابط واجراءات اصدار البطاقات وتعليمات مكتب الاستقبال والتعامل مع الزوار والمعاملات من صلاحيات رئيس الجامعة.

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 هذه السياسة على جميع إدارات والعاملين 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 مدير الأمن والسلامة:

9.1.8 أن تكون لديه الصلاحية والمسؤولية الأساسية عن الأمن المادي والبيئي، وعن التوعية والتدريب وإجراء التقييمات.

10.1.8 تقديم توصية لدعم تحديد الحلول التقنية وتأمينها ونشرها لتنفيذ متطلبات سياسة الأمن المادي والبيئي قدر الإمكان.

11.1.8 توجيه العاملين في الجامعة حول التنفيذ والالتزام بهذه السياسة.

12.1.8 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:

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

14.1.8 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 أوعدم 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.06-21.CS.A. V2.0- سياسة تصنيف البيانات
- ❖ DICT.I.06-26.CS.A. V2.0- سياسة المكتب النظيف والشاشة الخالية
- ❖ 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 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
نطاق الأمن المادي	3-14-2	-	-	-	-	A.11.1.1	PE-3, PE-4, PE-5
ضبط الدخول المادي	3-14-2	-	-	-	-	A.11.1.2	MA-5, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
دخول الزوار	3-14-2	-	-	-	-	A.11.1.2	MA-5, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
المرافق والغرف والمكاتب المؤمنة	3-14-2	-	-	-	-	A.11.1.3	PE-3, PE-4, PE-5
الحماية من التهديدات البيئية والخارجية	3-14-2	-	-	-	-	A.11.1.4	CP-2, CP-6, CP-7, PE-1, PE-9, PE-13, PE-15, PE-18, PE-19

العمل في أماكن آمنة						A.11.1.5	
أمن المعدات - تثبيت المعدات وحمايتها	3-14-2	-	-	-	-	A.11.2.1, A.11.2.6	PE-13, PE-14, PE-15, PE-18, PE-19
المرافق الداعمة	3-14-2	-	-	-	-	A.11.2.2	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14
أمن الكابلات	3-14-2	-	-	-	-	A.11.2.3	PE-4, PE-9
صيانة المعدات	3-14-2	-	-	-	-	A.11.2.4	MA-2, MA-3, MA-4, MA-5, MA-6
أمن استخدام الأجهزة خارج الجامعة	3-14-2	-	-	-	-	A.11.2.6	AC-19, AC-20, MP-5, PE-17
التصرف الآمن في الأجهزة وإعادة الاستخدام	3-14-2	-	-	-	-	A.11.2.7	MP-6
عدم ترك الاجهزة دون رقابة						A.11.2.8	
إدارة الوسائط القابلة للإزالة	3-14-2	-	-	-	-	A.8.3.1	MA-2, MP-5, PE-16
إزالة الأصول وضوابط نقل الوسائط المادية	-	-	-	-	-	A.8.3.3, A.11.2.5	MA-2, MP-5, PE-16

----------نهاية الوثيقة----------