جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة التحكم في الوصول

الإصدار: Version 2.0

رمز السياسة:DICT.I.06-33.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 التحكم في الوصول	مقيد	V2.0	فعال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الاصدار	التغييرات
V1.0	د. بشار الذيب	2021/01/02	إنشاء
V1.1	د. سامر بني عواد	2022/03/02	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/22	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 سياسة العمل عن بعد داخل الجامعة وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

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

5. الهدف

تهدف سياسة التحكم في الوصول الخاصة بالجامعة إلى إدارة وتقييد الوصول المنطقي والمادي للعاملين والأصول المعلوماتية والتقنية إلى مباني وأنظمة وشبكات البيانات الخاصة بالجامعة.

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 التحقق من هوية المستخدم ووثائق التفويض الخاصة بالجامعة والتحقق من صلاحيتها قبل منح المستخدم حق الوصول المنطقي أو المادي إلى موارد الجامعة.

2.1.7 يتم تحديد هوية المستخدم وتصاريح الوصول وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية والتنظيمية ذات العلاقة.

3.1.7 يجب أن يكون الوصول للبيانات والمعلومات في الجهة سواءً كان الوصول من عاملين أو أطراف خارجية بما يتوافق مع سياسات الجامعة.

2.7 إدارة هويات الدخول والصلاحيات

1.2.7 إدارة الصلاحيات

- يجب توثيق واعتماد إجراء لإدارة الوصول يوضح آلية منح صلاحيات الوصول للأصول المعلوماتية والتقنية وتعديلها وإلغائها في الجامعة، ومراقبة هذه الآلية والتأكد من تطبيقها.
- يجب إنشاء هويات المستخدمين (User Identities) وفقاً للمتطلبات التشريعية والتنظيمية الخاصة بالجامعة.
- يجب التحقق من هوية المستخدم (Authentication) والتحقق من صحتها قبل منح المستخدم صلاحية الوصول إلى الأصول المعلوماتية والتقنية.
- يجب توثيق واعتماد مصفوفة (Matrix) لإدارة تصاريح وصلاحيات المستخدمين (Authorization) بناءً على مبادئ التحكم بالدخول والصلاحيات التالية:
  - مبدأ الحاجة إلى المعرفة والاستخدام (Need-to-Know and Need-to-Use).
  - مبدأ فصل المهام (Segregation of Duties).
  - مبدأ الحد الأدنى من الصلاحيات والامتيازات (Least Privilege).
- يجب تطبيق ضوابط التحقّق والصلاحيات على جميع الأصول التقنية والمعلوماتية في الجامعة من خلال نظام مركزي آلي للتحكّم في الوصول، مثل بروتوكول النفاذ إلى الدليل البسيط (Lightweight Directory Access Protocol "LDAP").
- يجب منع استخدام الحسابات المشتركة (Generic User) للوصول إلى الأصول المعلوماتية والتقنية الخاصة بالجامعة.
- يجب ضبط إعدادات الأنظمة ليتم إغلاقها تلقائياً بعد فترة زمنية محدّدة (Session Timeout).
- يجب تعطيل حسابات المستخدمين غير المستخدمة خلال فترة زمنية محدّدة (يوصى ألا تتجاوز الفترة 90 يوماً).
- يجب ضبط إعدادات جميع أنظمة إدارة الهويات والوصول لإرسال السجلات إلى نظام تسجيل ومراقبة مركزي وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

- يجب عدم منح المستخدمين صلاحيات الوصول أو التعامل المباشر مع قواعد البيانات للأنظمة الحساسة، حيث يكون ذلك من خلال التطبيقات فقط، ويستثنى من ذلك مشرفي قواعد البيانات (Database Administrators).
- يجب على مديري التطبيقات وإدارة الأمن السيبراني التأكد من الفصل بين المهام ومبادئ الامتيازات الأقل عند منح امتيازات الوصول إلى مستخدمي الجامعة.
- يجب توثيق واعتماد إجراءات واضحة للتعامل مع حسابات الخدمات (Service Account) والتأكد من إدارتها بشكل آمن ما بين التطبيقات والأنظمة، وتعطيل الدخول البشري التفاعلي (Interactive Login) من خلالها.
- يجب أن تكون المصادقة متعددة العوامل (MFA) مطلوبة للوصول إلى:
  - جميع أصول معلومات الجامعة والشبكة عن بعد.
  - بريد الويب للوصول إلى خدمات البريد الإلكتروني للجامعة.
  - جميع تطبيقات الويب الخارجي.
  - حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة على الأصول التقنية والمعلوماتية.
  - الوصول إلى الأنظمة الحساسة والأنظمة المستخدمة لإدارة الأنظمة الحساسة ومتابعتها لجميع المستخدمين.
  - لكافة الحسابات السحابية للمستخدمين ذوي الصلاحيات الهامة والحساسة.
  - لعمليات الدخول لحسابات التواصل الاجتماعي.
- عند استخدام التحقّق من الهوية متعدد العناصر (Multi-Factor Authentication "MFA") فيجب أن تكون باستخدام طريقتين على الأقل من الطرق التالية:
  - المعرفة (شيء يعرفه المستخدم "مثل كلمة المرور").
  - الحيازة (شيء يملكه المستخدم فقط "مثل برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها "One-Time-Password").
  - الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل بصمة الإصبع").

2.2.7 منح حق الوصول

- متطلبات حق الدخول لحسابات المستخدمين

- يتم التحكم في الوصول إلى شبكات المعلومات أو البيانات على أساس متطلبات العمل والأمن ويتم تحديد قواعد التحكم والوصول لكل نظام. كما يجب أن تأخذ هذه القواعد بعين الاعتبار:
  - متطلبات الأمان الخاصة بتطبيق (تطبيقات) الأعمال.
  - متطلبات عمل محددة للمستخدم كي يتمكن من الدخول إلى المعلومات أو لعملية التشغيل (مبدأ "الحاجة إلى معرفة").
  - يتم رفض جميع أنواع الدخول ما لم تتم الموافقة عليها بموجب أحكام هذه السياسة.
  - الالتزام القانوني و/أو التعاقدي بتقييد وحماية الدخول إلى نظم المعلومات.
  - يجب أن تتم الموافقة بشكل رسمي من قبل إدارة الأمن السيبراني على جميع أنواع الوصول إلى نظم المعلومات باستثناء الطلبات الأساسية التي يتم تحديدها بالاتفاق مع عمادة الاتصالات وتقنية المعلومات.
- يجب ألا يتم توفير الوصول للأطراف الخارجية إلى موارد الجامعة وأصول معلومات التشغيل إلا عندما يتم توقيع تعهد المحافظة على السرية واعتمادها من الجامعة.
- تمنح صلاحية الدخول بناءً على طلب المستخدم من خلال نموذج أو عن طريق النظام المعتمد يُحدّد فيه اسم النظام ونوع الطلب والصلاحية بعد الموافقة من قبل المدير المباشر ومالك النظام (System Owner) بناءً على مصفوفة تصاريح وصلاحيات المستخدمين.
- يجب منح المستخدم حق الوصول إلى الأصول المعلوماتية والتقنية الخاصة بالجامعة بما يتوافق مع الأدوار والمسؤوليات الخاصة به.
- يجب اتباع آلية موحدة لإنشاء هويات المستخدمين بطريقة تتيح تتبع النشاطات التي يتم أداؤها باستخدام "هوية المستخدم" (User ID) وربطها مع المستخدم، مثل كتابة <الحرف الأول من الاسم الأول> نقطة <الاسم الأخير>، أو رقم العامل المعرف مسبقاً لدى الإدارة العامة للموارد البشرية.
- تعطيل إمكانية تسجيل دخول المستخدم من أجهزة حاسبات متعدّدة في نفس الوقت (Concurrent Logins).
- متطلبات حق الوصول للحسابات الهامة والحسّاسة، بالإضافة إلى الضوابط المذكورة في قسم متطلبات حق الوصول لحسابات المستخدمين، يجب أن تُطبّق الضوابط المُوضّحة أدناه على كافة الحسابات ذات الصلاحيات الهامة والحسّاسة:

- تعيين حق وصول مستخدم فردي للمستخدمين الذين يطلبون الصلاحيات الهامة والحسّاسة (Administrator Privilege) ومنحهم هذا الحق بناءً على مهامهم الوظيفية، مع الأخذ بالاعتبار مبدأ فصل المهام.
- يجب تفعيل سجل كلمة المرور (Password History) لتتبع عدد كلمات المرور التي تم تغييرها.
- تغيير أسماء الحسابات الافتراضية، وخصوصاً الحسابات الحاصلة على صلاحيات مهمة وحسّاسة مثل "الحساب الرئيسي" (Root) وحساب "مدير النظام" (Admin) وحساب "مُعرّف النظام الفريد" (Sys id).
- منع استخدام الحسابات ذات الصلاحيات الهامة والحسّاسة في العمليات التشغيلية اليومية.

3.7 الوصول إلى الشبكة والخدمات

1.3.7 يجب على إدارة الأمن السيبراني ضمان أن يتم التحكم في الوصول إلى الشبكات والخدمات على أساس متطلبات العمل والأمن، وقواعد التحكم في الوصول المحددة لكل شبكة. يجب أن تأخذ هذه القواعد في الاعتبار ما يلي:

- متطلبات الأمان للشبكة أو خدمة (خدمات) الشبكة.
- متطلبات أعمال محددة للمستخدم ليتمكن من الوصول إلى الشبكة أو خدمة الشبكة (مبدأ "الحاجة").
- التزام قانوني و / أو تعاقدي لتقييد أو حماية الوصول إلى الأصول.

2.3.7 يجب أن تضمن عمادة الاتصالات وتقنية المعلومات ما يلي:

- أن يقتصر الوصول المنطقي للأجهزة والبرامج الشبكية على مسؤولي النظام في الجامعة.
- يقتصر الوصول إلى أجهزة الشبكة القابلة للبرمجة مثل أجهزة التوجيه ((Routers، المبدلات (Switches)، وجدران الحماية (Firewall)، على مسؤولي الشبكة في الجامعة.
- يقتصر استخدام أدوات تشخيص الشبكات والأمان على مسؤولي الشبكات فقط، ووفقًا لمسؤولياتهم الوظيفية.
- يقتصر الوصول إلى جميع إعدادات الشبكة والبيانات المتعلقة بالأمان (على سبيل المثال أرقام الطلب الهاتفي وعناوين IP) على الفريق المعني بإدارة الأمن السيبراني ومن عمادة الاتصالات وتقنية المعلومات.

4.7 الدخول عن بُعد إلى شبكات الجامعة

1.4.7 يجب منح صلاحية الدخول عن بعد للأصول المعلوماتية والتقنية بعد الحصول على إذن مسبق من إدارة الأمن السيبراني وتقييد الدخول باستخدام التحقق من الهوية متعدد العناصر (MFA).

2.4.7 يجب حفظ سجلات الأحداث المتعلقة بجميع جلسات الدخول عن بُعد الخاصة ومراقبتها حسب حساسية الأصول المعلوماتية والتقنية.

3.4.7 يجب منع الدخول عن بعد من خارج المملكة للأنظمة الحساسة، الا في حالات استثنائية بعد أخذ الموافقة بشكل رسمي من قبل إدارة الأمن السيبراني.

4.4.7 يجب توفير الوصول عن بعد على أساس الحاجة فقط ولأغراض عمل الجامعة فقط.

5.4.7 يجب أن يستخدم أي وصول عن بعد طرق التشفير اللازمة (مثل بروتوكول النقل الآمن وبروتوكول طبقة المنافذ الآمنة والشبكة الخاصة الافتراضية) لتأمين الاتصال عبر الشبكة .

6.4.7 يجب على مستخدمي الوصول عن بعد التأكد من أن جهاز الحاسوب أو محطة العمل الخاصة بهم والمملوكة من قبل الجامعة أو لهم، والتي تم توصيلها عن بعد بشبكة الجامعة:

- غير متصلة بأي شبكة أخرى في نفس الوقت.
- لديها أحدث برامج مكافحة الفيروسات ومكافحة التجسس وجدار الحماية الشخصية المثبتة.

7.4.7 تتحكم عمادة الاتصالات وتقنية المعلومات في جميع عمليات الوصول عن بُعد من خلال عدد محدود من نقاط التحكم في الوصول المُدارة.

8.4.7 يجب أن توافق إدارة الأمن السيبراني وعمادة الاتصالات وتقنية المعلومات وملاك الانظمة على جميع طلبات الوصول عن بعد.

9.4.7 يجب أن يتحمل مستخدم الوصول عن بعد المسؤولية عن العواقب إذا ما أسيء استخدام الوصول.

10.4.7 يجب على عمادة الاتصالات وتقنية المعلومات التأكد من تسجيل جميع أنشطة اتصال الوصول عن بعد بما في ذلك عنوان بروتوكول الإنترنت ومعرف تسجيل الدخول.

11.4.7 يجب مراقبة نشاط حساب الوصول عن بعد بواسطة عمادة الاتصالات وتقنية المعلومات.

12.4.7 يجب أن يتم توفير الوصول عن بعد إلى أنظمة معلومات الجامعة عن طريق أطراف خارجية عندما يكون هناك مبرر قوي للتشغيل. إذا تم توفير الوصول عن بعد إلى أطراف خارجية إلى نظام / شبكة معلومات الجامعة، فيجب:

- أن يقتصر وصولهم على نظام / شبكة معلومات محددة فقط مطلوبة لأداء المسؤوليات الموكلة إليهم.
- يقوم مسؤول الشبكة والمراقبة بمراقبة سجلات الوصول الخاصة بهم وأنشطتهم.

5.7 إلغاء وتغيير حق الوصول

1.5.7 يجب على الإدارة العامة للموارد البشرية تبليغ عمادة الاتصالات وتقنية المعلومات لاتخاذ الإجراء اللازم عند انتقال المستخدم أو تغيير مهامه أو إنهاء/انتهاء العلاقة الوظيفية بين المستخدم والجامعة. وتقوم عمادة الاتصالات وتقنية المعلومات بإيقاف أو تعديل صلاحيات الدخول الخاصة بالمستخدم بناءً على مهامه الوظيفية الجديدة.

2.5.7 في حال تم إيقاف صلاحيات المستخدم، يمنع حذف سجلات الأحداث الخاصة بالمستخدم ويتم حفظها وفقاً لسياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني.

6.7 مراجعة هويات الدخول والصلاحيات

1.6.7 تقوم إدارة الأمن السيبراني بالتعاون مع مديري التطبيقات بمراجعة هويات الدخول (User IDs) والتحقق من صلاحية الوصول إلى الأصول المعلوماتية والتقنية وفقاً للمهام الوظيفية للمستخدم بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة هويات الدخول على الأنظمة الحساسة مرة واحدة كل ثلاثة أشهر على الأقل.

2.6.7 مراجعة الصلاحيات الخاصة (User Profile) بالأصول المعلوماتية والتقنية بناءً على مبادئ التحكم بالدخول والصلاحيات دورياً، ومراجعة الصلاحيات الخاصة بالأنظمة الحساسة مرة واحدة سنوياً على الأقل.

3.6.7 يجب مراجعة هويات الدخول والصلاحيات المستخدمة للعمل عن بعد، بحد أدنى مرة واحدة كل سنة.

4.6.7 عند اكتشاف أي سوء تصرف لحقوق الوصول المميزة، يجب على مديري التطبيقات تقييد هذه الامتيازات، وإخطار مسؤول النظام ذي الصلة باتخاذ مزيد من الإجراءات.

5.6.7 يجب الاحتفاظ بالسجلات الرسمية وتحديثها لجميع المستخدمين المسجلين في مصفوفة الصلاحيات لكل نظام / تطبيق.

7.7 التحكم في الوصول لخدمات الحوسبة السحابية

1.7.7 يجب إدارة هويات الدخول والصلاحيات لجميع الحسابات، التي لديها صلاحية الوصول إلى الخدمات السحابية، خلال دورة حياتها.

2.7.7 تجب مراعاة سرّية هوية المستخدم والحسابات والصلاحيات، بما في ذلك الطلب من المستخدمين حفظ خصوصيتها.

3.7.7 تجب الإدارة الآمنة للجلسات (Secure Session Management)، وتشمل موثوقية الجلسات (Authenticity)، وإقفالها (Lockout)، وإنهاء مهلتها (Timeout).

4.7.7 يجب عمل إجراءات لكشف محاولات الوصول غير المصرح به ومنعها مثل: (الحد الأقصى من محاولات عمليات الدخول غير الناجحة (Unsuccessful Login).

8.7 التحكم في الوصول لحسابات التواصل الاجتماعي

1.8.7 يجب استخدام حسابات التواصل الاجتماعي المخصصة للجامعة، وليس الأفراد.

2.8.7 يجب أن يكون التسجيل باستخدام معلومات رسمية (بريد إلكتروني رسمي خاص لوسائل التواصل الاجتماعي ورقم جوال رسمي)، وعدم استخدام معلومات شخصية.

3.8.7 يجب توثيق حسابات التواصل الاجتماعي والمحافظة على هوية متسقة في جميع حسابات التواصل الاجتماعي المستخدمة؛ لتسهيل معرفة الحسابات الرسمية، واكتشاف حسابات الاحتيال.

4.8.7 يجب استخدام كلمة مرور آمنة وخاصة لكل حسابات التواصل الاجتماعي، وتغير كلمة المرور بشكل دوري، وعدم إعادة استخدام كلمة مرور تم استخدامها من قبل.

5.8.7 يجب تفعيل وتحديث الأسئلة الأمنية وتوثيقها في مكان آمن.

6.8.7 تجب إدارة صلاحيات المستخدمين لحسابات التواصل الاجتماعي بناءً على احتياجات العمل، مع مراعاة حساسية الحسابات ومستوى الصلاحيات، ونوعية الأجهزة والأنظمة المستخدمة.

7.8.7 يجب حصر صلاحيات مقدمي خدمة إدارة حسابات التواصل الاجتماعي أو المراقبة الآلية لحسابات التواصل الاجتماعي أو حماية هوية الجهة من الانتحال.

8.8.7 يجب حصر إمكانية الدخول لحسابات التواصل الاجتماعي للجهة من أجهزة محددة.

9.8.7 يجب مراجعة هويات الدخول والصلاحيات المستخدمة لحسابات التواصل الاجتماعي للجهة، بحد أدنى مرة واحدة كل سنة.

9.7 التحكم في الوصول إلى الشفرة المصدرية

1.9.7 يجب على مديري التطبيقات التأكد من أن جميع الشفرات المصدرية (Source Code) يتم تجميعها مركزيًا وبطريقة محكومة في مكتبة البرامج.

2.9.7 يجب على مدير التطبيقات تجنب الكشف غير الضروري عن معلومات تهيئة النظام التي قد تكون مفيدة للمهاجمين، من خلال:

- منع، حقل الخادم في عناوين بروتوكول نقل النص الفائق (HTTP) التي تحدد العلامة التجارية لنسخة خادم الويب والإصدار.
- التأكد من عدم فهرسة أدلة الملفات الموجودة على خادم الويب لأن ذلك يمكن أن يكشف عن وجود ملفات لا تهدف إلى أن تكون متاحة للجمهور.
- التأكد من أنه لا يمكن عرض شفرة المصدر الخاصة بالبرامج التنفيذية والبرامج النصية من جانب الخادم عبر متصفح الويب.

3.9.7 بالنسبة إلى التطبيقات الويب، يتعين على مديري التطبيقات وإدارة الأمن السيبراني مراجعة مصدر لغة ترميز النص التشعبي وجافا سكريبت وغيرها من لغات البرمجة النصية من جانب العميل لضمان عدم احتوائها على معلومات غير ضرورية، مثل:

- أسماء المطورين (يمكن استخدامها في الهندسة الاجتماعية).
- خاصية التعطيل.
- تفاصيل حول الاختصاصات والمعايير.
- أدوات الطرف الخارجي قيد الاستخدام، والتي قد تحتوي على ثغرات معروفة.
- مراجعة رسائل الخطأ التي تم إرجاعها بواسطة تطبيق الويب للتأكد من أنها لا تكشف عن معلومات غير مرغوب فيها.

4.9.7 تضمن إدارة الأمن السيبراني ومديري التطبيقات عدم تمكن عاملي عمادة الاتصالات وتقنية المعلومات من الوصول إلى رموز مصدر البرنامج أو القدرة على تعديل سلوك البرامج عن طريق تغيير معلمات التكوين الخاصة بهم.

5.9.7 يجب الاحتفاظ بسجلات دقيقة وحديثة لمكتبات مصدر البرامج.

10.7 إدارة معلومات المصادقة للمستخدمين

1.10.7 يجب على مديري التطبيقات التأكد من:

- تحديد الهوية والمصادقة من خلال كلمات المرور قبل السماح للمستخدم بالوصول إليها لجميع أنظمة المعلومات في الجامعة.
- مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء الخدمة المهنية لهم بالجهة.
- بالنسبة لجميع حالات النقل، تتم مراجعة جميع امتيازات الوصول الحالية للمستخدم وفقًا لمتطلبات الوظيفة المعتمدة، وبناءً على المراجعة، يتم تعديل امتيازات الوصول أو إبطالها وفقًا لذلك.

11.7 تقييد الوصول إلى المعلومات

1.11.7 يجب على مديري التطبيقات ضمان ما يلي:

- أن يعمل التطبيق الهام والحساس الذي يعالج بيانات حساسة على نظام تشغيل مخصص.
- تقييد وصول المستخدمين وعاملي الدعم إلى معلومات النظام الحساسة ووظائف نظام التطبيق.
- يتم ممارسة العزل المادي و/أو المنطقي للأنظمة الحساسة.

2.11.7 فيما عدا مشرفي قواعد البيانات (Database Administrators)، يمنع الوصول أو التعامل المباشر لأي مستخدم مع قواعد البيانات؛ ويتم ذلك من خلال التطبيقات فقط، وبناءً على الصلاحيات المخوّل بها؛ مع مراعاة تطبيق حلول أمنية تحد، أو تمنع من اطلاع مشرفي قواعد البيانات على البيانات المصنفة (Classified Data).

12.7 إجراءات تسجيل الدخول الآمن

1.12.7 يجب أن يحدد النظام عدد محاولات تسجيل الدخول غير الناجحة المسموح بها؛ وتعتبر التالية:

- تسجيل كل من المحاولات الناجحة وغير الناجحة.
- فرض تأخير زمني قبل السماح بمزيد من محاولات تسجيل الدخول أو رفض أي محاولات أخرى دون تفويض محدد.
- يقوم مديري التطبيقات بمراجعة جميع محاولات التسجيل غير الناجحة بشكل دوري.
- يجب تكوين التنبيهات على نظام (SIEM) لإخطار فريق العمليات الأمنية بأي نشاط أو حادث مشبوه.

13.7 نظام كلمة المرور

1.13.7 يجب على مسؤولي النظام (التطبيق، قاعدة البيانات، أنظمة التشغيل، الشبكات، إلخ) التأكد من تخزين أسماء المستخدمين وكلمات المرور الخاصة بأنظمة المعلومات بأمان (تشفيرها)، والتعامل معها وتوزيعها.

2.13.7 يجب أن يكون مسؤولي النظام (التطبيق، قاعدة البيانات، أنظمة التشغيل، الشبكة، إلخ) مسؤولين عن تغيير جميع أسماء المستخدمين وكلمات المرور الافتراضية للنظام، في الوقت الذي يتم فيه الحصول على هذه الأنظمة.

3.13.7 يجب على المستخدم تغيير كلمات المرور على الفور إذا كان هناك أي اشتباه في اختراق كلمة المرور؛ وسيتم الإبلاغ عن ذلك على الفور إلى عمادة الاتصالات وتقنية المعلومات وإدارة الأمن السيبراني.

8. الأدواروالمسؤوليات

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 المقبولة لاستخدام الأصول حيثما أمكن.

6.1.8 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.

7.1.8 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 الملفات 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.06-21.CS.A. V2.0- سياسة تصنيف البيانات
- DICT.I.06-10.CS.A. V2.0- سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- DICT.I.06-22.CS.A. V2.0- سياسة اقتناء النظام وتطويره وصيانته
- DICT.I.06-15.CS.A. V2.0- سياسة كلمة المرور
- DICT.I.06-14.CS.A. V2.0- سياسة حماية تطبيقات الويب
- DICT.I.06-49.CS.A.V2.0- معايير إدارة هويات الدخول والصلاحيات
- DICT.I.06-60.CS.A.V2.0- معايير تصنيف الأصول
- DICT.I.06-69.CS.A.V2.0- معايير كلمة المرور
- DICT.I.06-68.CS.A.V2.0- معايير إدارة سجلات الأحداث ومراقبة الأمن السيبراني
- DICT.I.06-73.CS.A.V2.0- معايير حماية تطبيقات الويب
- DICT.I.04-36.CS.A.V2.0- إجراءات اقتناء النظام وتطويره وصيانته

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	ضوابط الأمن السيبراني للحوسبة السحابية	الآيزو 27001:2013	المعهد الوطني للمعايير والتقنية
ضبط الوصول إلى نظام العمليات	3-2-2	1-2-2 2-2-2	1-2-2	1-2-2 2-2-2	٢-٢-ش-١	A.11.5.1, A.11.5.2, A.11.5.3	AC-2, AC-7, AC-8, AC-9, IA-2, IA-5, IA-6, IA-8
استخدام معلومات المصادقة السرية	3-2-2	1-2-2 2-2-2	1-2-2	1-2-2 2-2-2	٢-٢-ش-١	A.9.3.1	IA-5(1), IA-5(4), IA-2
الوصول إلى الشبكة	3-2-2	1-2-2 2-2-2	2-2-2	1-2-2 2-2-2	٢-٢-ش-١	A.11.4.1	AC-1, AC-6, AC-17, AC-18, AC-20, CM-7, SC-1, SC-7

----------نهاية الوثيقة----------