جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

سياسة كلمة المرور

الإصدار: Version 2.0

رمز السياسة: DICT.I.06-15.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

All rights reserved for Deanship of ICT ©

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

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.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

3. الرقابة على الوثيقة

1.3 معلومات عن الوثيقة

العنوان	التصنيف	الإصدار	الحالة
سياسة كلمة المرور	مقيد	V2.0	فعّال

2.3 تاريخ الإعداد والتّحديث

الإصدار	المؤلفون	تاريخ الإصدار	التغييرات
V1.0	د. بشار الذيب	2021/03/05	إنشاء
V1.1	د. سامر بني عواد	2022/01/27	مراجعة وتحديث
V2.0	بهاء نوافله	2023/12/14	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

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

4. المقدمة

حماية الأصول المعلوماتية والتقنية أمر ضروري لنجاح الجامعة؛ ولهذه الغاية قام الجامعة بإنشاء إدارة الأمن السيبراني لتطوير وإنشاء وتنظيم العمليات المطلوبة لحماية الأصول المعلوماتية والتقنية وتحدد هذه الوثيقة سياسة كلمة المرور 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

تحدد هذه السياسة المعايير والإجراءات اللازمة لتوفير الضوابط الأمنية لكلمات المرور وإدارتها.

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 أن تحتوي كلمات مرور الحسابات العادية على ثمانية (8) خانات على الأقل من الأحرف والأرقام، واثنا عشر (12) خانة على الأقل للحسابات الهامة والحساسة (مثل حسابات المسؤول عن النظام).

2.1.7 يجب أن تكون كلمة المرور حساسة لحالة الأحرف، ويجب أن تحتوي في كلا الحالتين على الأحرف الصغيرة والكبيرة.

3.1.7 يجب أن تحتوي كلمة المرور على رمز واحد مميز على الأقل.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

4.1.7 يجب أن تُصمم الأنظمة بحيث تجبر المستخدمين على تغيير كلمة المرور الأولية المؤقتة للحسابات الحديثة عند تسجيل الدخول لأول مرة وأن تقوم بالاحتفاظ بسجل آخر خمس كلمات مرور للحساب لمنع إعادة استخدام كلمة المرور.

5.1.7 يجب إشعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية.

6.1.7 يجب ألّا تُعرض كلمات المرور على الشاشة عند إدخالها، كما يجب تخزين ملف التحقق من كلمة المرور المُخزَّن في نظام التطبيق بشكل مشفر.

7.1.7 يجب حماية كلمة المرور من قبل المستخدمين ويكون كل فرد مسؤولاً عن الأنشطة التي تم تنفيذها من خلال "هوية المستخدم" الخاصة بهم.

8.1.7 لا يسمح للمستخدمين ما يلي:

- استخدام نفس الطريقة لإرسال كلمات المرور لفتح الملفات أو الروابط التي تتطلب كلمة مرور، من ضمن وسائل المراسلات: البريد الإلكتروني، الرسائل الفورية والرسائل القصيرة وما إلى ذلك.
- مشاركة كلمة المرور مع العاملين الآخرين.
- الكشف عن كلمة المرور لأي شخص.
- كتابة كلمة المرور على ورق.
- حفظ كلمة المرور في ملفات غير محمية.
- تخزين كلمة المرور على شكل نص واضح.
- استخدام خاصية "تلميح (Hint)" لتذكر كلمة المرور.
- حفظ كلمة المرور تلقائياً.
- استخدم خاصية "تذكر كلمة المرور" في التطبيقات / الأنظمة.

9.1.7 لا يُستخدم "اسم المستخدم" في كلمة مرور.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

10.1.7 يجب ألّا يُستخدم الاسم الأول للمستخدم أو الاسم الأوسط أو اسم العائلة في كلمات المرور.

11.1.7 عند استخدام بروتوكول إدارة الشبكة البسيط (SNMP)، يجب تحديد سلاسل المجتمع (community strings) بخلاف الإعدادات الافتراضية القياسية "عام" و "خاص" و "نظام"، ويجب أن تكون مختلفة عن كلمات المرور المستخدمة لتسجيل الدخول بشكل تفاعلي، كما يجب استخدام التجزئة المفتاحية عند توفرها (على سبيل المثال، SNMP v3).

12.1.7 يجب استخدام الطرق والخوارزميات الآمنة لحفظ ومعالجة كلمات المرور مثل: استخدام دوال الاختزال (Hashing Functions).

13.1.7 يجب ألّا تستخدم كلمات المرور أي معلومات تخص الجامعة أو الموقع الجغرافي الخاص به.

14.1.7 يجب تغيير جميع كلمات المرور الافتراضية للحسابات ذات الصلاحيات الهامة مثل الحسابات الأساسية (Root) وحسابات المسؤول عن النظام (Administrator) بمجرد أن يصبح النظام فعّالاً.

15.1.7 يجب أن تُخصص الحسابات ذات الصلاحيات الهامة والحسّاسة لمسؤول واحد يكون مسؤولا عن كلمة المرور.

16.1.7 في حالة الشك في أن كلمة المرور الخاصة قد تم اختراقها، فيجب على المستخدم تغيير كلمة المرور على الفور وإخطار إدارة الأمن السيبراني عن الحادثة.

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 تعارضات تنشأ عن هذه السياسة.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

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 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.

10.1.8 تأمين وتمكين إعدادات أمن كلمة المرور لجميع أنظمة تقنية المعلومات في الجامعة.

11.1.8 مراجعة محاولات تسجيل الدخول الخاطئة وسجلات الصلاحيات الإدارية يومياً.

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

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

13.1.8 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.

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

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.06-26.CS.A. V2.0- سياسة المكتب النظيف والشاشة الخالية
- DICT.I.06-33.CS.A. V2.0- سياسة التحكم في الوصول
- DICT.I.06-71.CS.A.V2.0- معايير التشفير
- DICT.I.06-69.CS.A.V2.0- معايير كلمة المرور

All rights reserved for Deanship of ICT ©
جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©

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
استخدام معلومات التحقق السرية	2-1-2-2, 2-1-3-2	2-1-2-5	-	-	-	A.9.3.1	IA-5(1), IA-5(4), IA-2
نظام إدارة كلمات المرور	2-2-3-1	2-1-2-5	-	-	-	A.9.4.3	IA-6

----------نهاية الوثيقة----------

جميع الحقوق محفوظة لعمادة الاتصالات وتقنية المعلومات ©
All rights reserved for Deanship of ICT ©