جامعة الأمير سطام بن عبدالعزيز
PRINCE SATTAM BIN ABDULAZIZ UNIVERSITY
إدارة الأمن السيبراني
Cybersecurity Department

سياسة إدارة كلمة المرور

مقيّد - داخلي

التاريخ : 2023-11-12

الإصدار: 3.1

المرجع: الهيئة الوطنية للأمن السيبراني

اعتماد الوثيقة

الدور	الاسم	التاريخ
المالك	مدير إدارة الأمن السيبراني	2022-01-02
المعمِّد	اللجنة الإشرافية للأمن السيبراني	2023-10-25

نسخ الوثيقة

النسخة	التاريخ	عُدلَ بواسطة		أسباب التعديل
1.0	2021-11-09	قسم الحوكمة والمخاطر والالتزام	أ.غادة العجلان	إنشاء الوثيقة
2.0	2022-02-21	قسم الحوكمة والمخاطر والالتزام	أ.نجود العسكر	تعديل مسمى إدارة أمن المعلومات إلى إدارة الأمن السيبراني
3.0	2023-03-04	قسم الحوكمة والمخاطر والالتزام	أ.نجود العسكر	تحديث الهوية
3.1	2023-11-12	قسم الحوكمة والمخاطر والالتزام	أ. ساره الجوير	1. تعديل مسمى عمادة تقنية المعلومات والتعليم عن بعد الى الإدارة العامة لتقنية المعلومات 2. التعديل بما يتناسب مع توصيات اللجنة الاشرافية للأمن السيبراني

قائمة المحتويات

الأهداف 3
نطاق العمل وقابلية التطبيق..... 3
بنود السياسة 3
الأدوار والمسؤوليات..... 7
الالتزام بالسياسة..... 7

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير لضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بكلمة المرور لحماية جامعة الأمير سطام بن عبدالعزيز من مخاطر الأمن السيبراني والتهديدات الداخلية والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٤-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

الهدف من هذه الوثيقة هو بيان السياسة الخاصة ببناء كلمة المرور للأنظمة والتطبيقات بالجامعة. مستخدمي هذه الوثيقة هم الموظفين وأعضاء هيئة التدريس ومن في حكمهم من المختصين.

بنود السياسة

إدارة كلمات المرور

تطبيق سياسة آمنة لكلمة المرور ذات معايير عالية لجميع الحسابات داخل جامعة الأمير سطام بن عبدالعزيز، ويتضمّن الجدول أدناه أمثلة على ضوابط كلمات المرور لكل مستخدم:

ضوابط كلمات المرور	جميع المستخدمين (All Users)	حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة (Privileged Users)	حسابات الخدمات (Service Account)
الحدّ الأدنى لعدد أحرف كلمة المرور	8 أحرف أو أرقام أو رموز	12 حرفاً أو رقماً أو رمزاً	12 حرفاً أو رقماً أو رمزاً
سجل كلمة المرور	تذكّر 2 كلمات مرور	تذكّر 3 كلمات مرور	تذكّر 5 كلمات مرور
الحد الأعلى لعمر كلمة المرور	365 يوماً	90 يوماً	180 يوماً

ضوابط كلمات المرور	جميع المستخدمين (All Users)	حسابات المستخدمين ذات الصلاحيات الهامة والحسّاسة (Privileged Users)	حسابات الخدمات (Service Account)
مدى تعقيد كلمة المرور	مُفعّل	مُفعّل	مُفعّل
مثال على تعقيد كلمة المرور	D_dyW5$_	R@rS%7qY#b!u	r?M4d5V=A1!s
مدة إغلاق الحساب	30 دقيقة أو حتى يقوم النظام بفك الإغلاق	30 دقيقة أو حتى يقوم النظام بفك الإغلاق	30 دقيقة أو حتى يقوم النظام بفك الإغلاق
حد إغلاق الحساب	5 محاولات غير صحيحة لتسجيل الدخول	3 محاولات غير صحيحة لتسجيل الدخول	لا توجد محاولات
إعادة ضبط عداد إغلاق الحساب بعد مرور فترة معينة	30 دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	30 دقيقة (يقوم المدير بفك إغلاق الحساب المغلق يدوياً)	لا يوجد
استخدام التحقق متعدد العناصر	مُفعل على الدخول من خارج المجال (Domain)	مُفعل على الدخول من خارج المجال (Domain)	غير مُفعل

1- معايير كلمات المرور

1-1 يجب إشعار المستخدمين قبل انتهاء صلاحية كلمة المرور لتذكيرهم بتغيير كلمة المرور قبل انتهاء الصلاحية.

2-1 يجب ضبط إعدادات كافة الأصول المعلوماتية والتقنية لطلب تغيير كلمة المرور المؤقتة عند تسجيل المستخدم الدخول لأول مرة.

3-1 يجب تغيير جميع كلمات المرور الافتراضية لجميع الأصول المعلوماتية والتقنية قبل تثبيتها في بيئة الإنتاج.

4-1 يجب تغيير كلمات مرور السلاسل النصية (Community String) الافتراضية (مثل: «Public» و«Private» و«System») الخاصة ببروتوكول إدارة الشبكة البسيط (SNMP)، ويجب أن تكون مختلفة عن كلمات المرور المستخدمة لتسجيل الدخول في الأصول التقنية المعنية.

2- حماية كلمات المرور

1-2 يجب تشفير جميع كلمات المرور للأصول المعلوماتية والتقنية الخاصة بجامعة الأمير سطام بن عبدالعزيز بصيغة غير قابلة للقراءة أثناء إدخالها ونقلها وتخزينها وذلك وفقاً لسياسة التشفير.

2-2 يجب إخفاء (Mask) كلمة المرور عند إدخالها على الشاشة.

3-2 يجب تعطيل خاصية "تذكّر كلمة المرور" (Remember Password) على الأنظمة والتطبيقات الخاصة بجامعة الأمير سطام بن عبدالعزيز.

4-2 منع استخدام الكلمات المعروفة (Dictionary) في كلمة المرور كما هي.

5-2 يجب تسليم كلمة المرور الخاصة بالمستخدم بطريقة آمنة وموثوقة.

6-2 إذا طلب المستخدم إعادة تعيين كلمة المرور عن طريق الهاتف أو الإنترنت أو أي وسيلة أخرى، فلا بد من التحقّق من هوية المستخدم قبل إعادة تعيين كلمة المرور.

7-2 يجب حماية كلمات المرور الخاصة بحسابات الخدمة والحسابات ذات الصلاحيات الهامة والحسّاسة وتخزينها بشكل آمن في موقع مناسب (داخل مغلف مختوم في خزنة) أو استخدام التقنيات الخاصة بحفظ وإدارة الصلاحيات الهامة والحسّاسة (Privilege Access Management Solution).

3- يحظر على الموظف القيام بما يلي:

1-3 إدخال كلمة المرور في رسائل البريد الإلكتروني.

2-3 توزيع كلمة المرور إلى موظفين آخرين.

3-3 تخويل موظف آخر بإنشاء كلمة المرور عوضا عنه .

4-3 التقاط أو تخمين كلمات المرور، ومفاتيح فك التشفير، أو أي آلية أخرى من آليات التحكم في الوصول، مما يتيح الوصول دون إذن.

5-3 الإفصاح عن كلمة المرور عبر الهاتف إلى أي شخص.

6-3 الكشف عن كلمة المرور للآخرين بما في ذلك مشرفي تقنية المعلومات والمدير المباشر.

7-3 الحديث عن كلمة المرور أمام الآخرين.

8-3 قول أي تلميحات حول كلمة المرور على سبيل المثال (اسم العائلة).

9-3 الكشف عن كلمة المرور من خلال الاستبيانات أو النماذج الأمنية .

10-3 مشاركة كلمة المرور مع المقربين.

1-10-3 الكشف خلال الإجازة، عن كلمة المرور لأحد زملاء العمل .

2-10-3 كتابة كلمة المرور على ورقة .

3-10-3 تكوين أنظمة للسماح بتسجيل دخول المستخدم دون كلمة مرور.

4- تخزين كلمة المرور: يجب تخزين كلمة المرور بطريقة آمنة تضمن عدم كشفها، باتباع التالي:

1-4 يجب التعامل مع جميع كلمات المرور في الجامعة على أنها بيانات سرية.

2-4 لا يحتفظ بكلمات المرور كنص عادي يمكن قراءته، وإنما يتم حفظ كلمات السر على شكل نص مشفر لا يمكن فكه أو استخدامه من الشخص المخول.

3-4 يجب ألا يتم تخزين كلمات المرور على أنظمة الحاسوب في شكل غير محمي.

4-4 كلمات المرور للأنظمة (جذر النظام/مسؤول النظام Root/Administrator) يجب أن تخزن باستعمال برمجيات حفظ كلمات المرور بطريقة مشفرة.

5-4 يجب ضمان عدم تفعيل خاصية حفظ كلمة المرور في المتصفح وإدخال البيانات في كل مرة من جديد.

5- **الحفاظ على سرية كلمات المرور:** يجب الحرص على المحافظة على كلمة المرور، باتباع التالي:

5-1 يجب عدم مشاركة أو كشف كلمة المرور مع أي شخص لأي سبب من الأسباب.

5-2 يجب عدم إفشاء كلمة المرور وعدم كتابتها بطريقة صريحة مما يجعلها عرضة للاطلاع أو حتى التلميح عن تركيبتها، إلا في حالةِ الضرورةِ القصوى ويجب تغييرها بعد الكشف عنها.

5-3 يمنع إرسال كلمة المرور عبر البريد الإلكتروني أو من خلال أي وسيلة عبر الأنترنت.

5-4 يجب تغيير كلمات المرور إذا ظهر أي مؤشر على احتمال اختراق للنظام أو لكلمة المرور.

5-5 يجب تغيير كلمات المرور المستخدمة للحسابات المشتركة على الفور في حالة اختراقها أو عندما يغادر مالكها الجامعة.

5-6 لا يجب استخدام نفس كلمة المرور لحسابات المسؤولين المتعددة.

5-7 يجب على المستخدمين قدر الإمكان عدم استخدام كلمة المرور نفسها لحسابات مختلفة في الجامعة.

5-8 يجب على المستخدمين عدم استعمال ذات كلمة المرور للحسابات والأجهزة داخل الجامعة والحسابات والأجهزة الأخرى خارجها.

5-9 يجب على المستخدم في حالة أن يشتبه أو يلاحظ وجود مشكلة أمنية أو أن كلمة المرور الخاصة به قد تعرضت للاختراق الإبلاغ عن الحادث عبر البريد الإلكتروني (IR@psau.edu.sa) وتغيير جميع كلمات المرور.

5-10 يجب أن يُطلب من المستخدمين التوقيع على بيان للحفاظ على سرية كلمات المرور الشخصية؛ يمكن تضمين هذا البيان في شروط التوظيف.

5-11 يجب أن يكون المستخدم على علم ودراية أنه المسؤول الوحيد عن حماية كلمة السر/المرور الخاصة به.

6- **كلمات المرور الأولى (المؤقتة):** يجب تغيير كلمات المرور الأولية للمستخدمين وفرض مدة انتهاء لصلاحيتها لإجبار المستخدم على تغييرها.

6-1 على المستخدم تغيير كلمة المرور الأولية التي يستلمها من الجهة المختصة في أول استخدام له وقبل انتهاء وقت صلاحيتها؛ وذلك لضمان عدم تسريب كلمة السر لمستخدمين آخرين.

6-2 يجب إعطاء كلمات المرور المؤقتة للمستخدمين بطريقة آمنة؛ ينبغي تجنب نقلها على ورقة مكشوفة (نص عادي) أو عن طريق أطراف ثالثة أو رسائل البريد الإلكتروني غير المحمية (النص الواضح) .

6-3 وضع إجراءات للتحقق من هوية المستخدم قبل تقديم كلمة مرور جديدة أو بديلة أو مؤقتة.

6-4 يجب على المستخدمين الإقرار باستلام كلمات المرور المؤقتة.

6-5 يتطلب فحص كلمات المرور الجديدة في قوائم كلمات المرور شائعة الاستخدام أو المخترقة.

الأدوار والمسؤوليات

1. **راعي ومالك وثيقة السياسة:** مدير إدارة الأمن السيبراني.
2. **مراجعة السياسة وتحديثها:** إدارة الأمن السيبراني.
3. **تنفيذ السياسة وتطبيقها:** الإدارة العامة لتقنية المعلومات وإدارة الأمن السيبراني وعمادة الموارد البشرية.

الالتزام بالسياسة

1- يجب على مدير إدارة الأمن السيبراني ضمان التزام جامعة الأمير سطام بن عبدالعزيز بهذه السياسة دورياً.

2- يجب على جميع العاملين في جامعة الأمير سطام بن عبدالعزيز الالتزام بهذه السياسة.

3- قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة، إلى إجراء تأديبي؛ حسب الإجراءات المتبعة في جامعة الأمير سطام بن عبدالعزيز.