مؤسسة كيو سن للسلام والتنمية الإعلامية
Q Sun Foundation for Peace and Media Development

سياسات الحوكمة

سياسة كلمات المرور

سياسات مؤسسة كيو سن للسلام والتنمية الإعلامية

الجهة
مؤسسة كيو سن

رمز الوثيقة
حـ ١٢

المحتويات

1. سياسة كلمة المرور
2. التعريف
3. الغرض
4. النطاق
5. المعايير العامة لكلمات المرور
6. إنشاء كلمات المرور
7. حماية كلمات المرور
8. الأدوار والمسؤوليات
9. الممارسات المخلة بالسياسة

التعريف والغرض والمعايير العامة

كلمة المرور هي أي كلمة سرية أو رمز يُستخدم كتدبير أمني لمنع الوصول غير المخوّل إلى البيانات والمعلومات. ويعرّف اسم المستخدم وكلمة المرور معًا هوية المستخدم في النظام.

١. التعريف

سياسة كلمة المرور مجموعة الإجراءات والقواعد المطبّقة لإنشاء كلمة المرور وتغييرها وحمايتها. ويُعد وضع قواعد جيدة لكلمات المرور الشخصية من أهم وسائل منع الوصول غير المخول إلى الأنظمة، بما فيها البيانات والمعلومات والخدمات وقواعد البيانات والمصادر.

٢. الغرض

إرساء معايير لإنشاء كلمات مرور قوية وحمايتها وتحديد الفترات الدورية لتغييرها، منعًا لخطر الوصول غير المخول إلى البيانات والمعلومات والخدمات والمصادر.

٣. النطاق

تطبق السياسة على جميع مستخدمي شبكة مؤسسة كيو سن وعلى مسؤولي تقنية المعلومات.

٤. السياسة

٤.١ المعايير العامة لكلمات المرور

1. تُغيّر كلمات المرور دوريًا لمنع غير المصرح لهم باستخدام الشبكة من تخمين كلمة مرور حساب معين واستخدامها للدخول عبر مصادقة الهوية. ويرسل النظام للمستخدمين تذكيرًا عند اقتراب موعد التغيير.
2. تُعد أول كلمة مرور عند إنشاء الحساب مؤقتة، ويجب تأمين إيصالها إلى المستخدم وتغييرها.
3. يُربط كل حساب، على مستوى المستخدم أو النظام، بمعرّف شخصي فريد لتمييزه، وتدل كلمة مرور فريدة على الحساب. وتُربط المصادقة بمعرّف الحساب الفردي.
4. تُشفّر جميع كلمات المرور المنتجة على مستوى النظام وتُدار من خلال قاعدة بيانات الإدارة المركزية لكلمات المرور، ويحظر تخزينها في ملفات حتى لو كانت مشفرة.
5. يُقفل الحساب إذا لم ينجح المستخدم في إدخال كلمة المرور الصحيحة خلال أربع محاولات. وبعد ٣٠ دقيقة من آخر محاولة تُتاح له أربع محاولات أخيرة. وإذا تجاوزها، يُقفل الحساب حتى يعيد مدير النظام تفعيله.
6. عند التغيير، لا يجوز استخدام أي من آخر ست كلمات مرور.
7. لا يقل طول كلمة المرور عن ثمانية محارف من الأبجدية المستخدمة.
8. تُعد جميع كلمات مرور المؤسسة بيانات حساسة.

إنشاء كلمات المرور وحمايتها

٤.٢ إنشاء كلمات المرور

1. استخدام الحروف الإنجليزية الكبيرة والصغيرة، من A إلى Z ومن a إلى z.
2. استخدام الأرقام من ٠ إلى ٩ والرموز الخاصة، مثل ! و@ و# و$ و% و^ و& و* والأقواس وعلامات الترقيم.
3. استخدام خليط من الحروف الصغيرة والكبيرة والرموز والأرقام.
4. لتذكّر كلمة المرور، يمكن ربطها بأغنية أو خطاب أو عنوان، وأخذ الحرفين الأول والثاني من كل كلمة.
5. لتسهيل إنشاء كلمة قوية، يمكن جعل الحرف الأول كبيرًا ووضع رمز في آخرها، مثل استبدال a بالرمز @ أو استخدام حرف بدل الرقم 0.
6. يُفضّل استخدام كلمات يتعمد المستخدم إدخال أخطاء إملائية فيها.
7. استخدام الخيال في إنشاء كلمة المرور الجيدة.
8. يُشعَر المستخدمون قبل انتهاء فترة كلمة المرور. وإذا انقضت دون تغييرها، يُمنع المستخدم من الوصول إلى موارد النظام حتى إشعار آخر من قسم تقنية المعلومات.

٤.٣ حماية كلمات المرور

1. تُستخدم كلمات مرور مختلفة لحسابات المستخدم والأعمال. ويشمل ذلك حساب الإنترنت وحساب إدارة المؤسسة والبريد الإلكتروني والمنتديات وغيرها.
2. يحظر مشاركة كلمات مرور الحسابات الرئيسية مع أي شخص في المؤسسة، بمن في ذلك الموظفون والمديرون ومن يسألون عنها. ولا يُفعّل خيار تذكر كلمة المرور أو حفظها في التطبيقات أو المتصفحات.
3. يحظر تدوين كلمة المرور على الورق أو الاحتفاظ بها في المكتب أو في ملفات الحاسوب دون تشفيرها بإحدى طرق التشفير.
4. يوقف الحساب أو يُحذف عند مرور عشرة أيام على انتهاء كلمة مروره، مع مراعاة الحسابات قليلة الاستخدام.
5. عند الاشتباه في كلمة مرور أو حساب، أو عند وجود استفسار عن كلمة مرور حساب، يُبلّغ قسم تقنية المعلومات وتُغيّر كلمة المرور فورًا.
6. تُغيّر كلمات المرور الافتراضية، خصوصًا عند تثبيت البرامج أو التطبيقات.
7. استخدام كلمة مرور ضعيفة لمدة ٢١ يومًا يعرّض المستخدم للتحقيق والإجراءات التأديبية.
8. مخالفة أحكام الوثيقة بشأن كلمات المرور تُعرّض المستخدم للمساءلة والتحقيق والتأديب الملائم من لجنة تُشكّل بقرار من رئيس المؤسسة بناءً على اقتراح قسم تقنية المعلومات.

الأدوار والممارسات المخلة

٤.٤ الأدوار والمسؤوليات

٤.٤.١ قسم تقنية المعلومات

1. التأكد من قدرة موارد النظام على تنفيذ تعليمات السياسة.
2. تطبيق الإجراءات لأغراض الاختبار وإدارة السياسة.
3. تقديم التعليم والتوضيح اللازمين للمستخدمين بشأن السياسة.
4. التبليغ عن حالات الاشتباه أو انتهاك السياسة.
5. يفهم المستخدمون السياسة ويحمون كلمات مرورهم ويتواصلون مباشرة مع قسم تقنية المعلومات بشأن أي ملاحظات أو استفسارات أو شبهات.
6. يضمن مشرف النظام التزام جميع الموظفين بالتعليمات، ويرفع مباشرةً إلى قيادة المؤسسة أي انتهاك أو عدم تقيد بما ورد في السياسة.

٤.٤.٢ واضعو السياسة يزوّدون المستخدمين والمعنيين بتنفيذها بالتعليمات والنصائح، ويضعون أنظمة تدقيق لضمان الالتزام بها.

٤.٤.٣ مطورو الأنظمة يضمنون دعم أنظمتهم للإجراءات والتعليمات المحددة في هذه السياسة، ويتأكدون مما يلي.

1. قدرة الأنظمة على ربط المستخدم بمعرّف حسابه الفردي.
2. قدرة الأنظمة على ربط أدوار المستخدمين بحيث يمكنهم التحكم في وظائف أخرى دون الحاجة إلى معرفة كلمات المرور الأخرى.

٤.٥ الممارسات المخلة بالسياسة

1. تخصيص كلمة المرور باستخدام أنظمة التوليد العشوائية أو الأنظمة المشابهة لإنشاء كلمات المرور.
2. عدم تفعيل تغيير كلمة المرور أو الإفراط فيه، مثل جعل مدة التغيير أسبوعية أو شهرية.
3. الرغبة في مشاركة كلمة المرور.
4. اجتزاء إجراءات السياسة وتعليماتها وعدم الالتزام بمعاييرها القياسية.
5. الجمود في مراجعة السياسة وإعادة تقييمها أو الاكتفاء بها.