سياسة كلمة المرور

الإصدارة: ١. ١

رقم السياسة:

الرقابة على الوثيقة

معلومات عن الوثيقة

العنوان	التصنيف	الإصدارة	الحالة
سياسة كلمة المرور	سري	1.1	معتمدة

الإعداد والتحديث

الإصدار	إعداد	تاريخ الاصدار	التغييرات
1.0	د. زاهد – تقنية المعلومات والاتصالات بجامعة الإمام عبد الرحمن بن فيصل	01يناير 2013	مشروع
1.1	منيب أحمد- تقنية المعلومات والاتصالات بجامعة الإمام عبد الرحمن بن فيصل	17مايو 2017	تحديث

المراجعة والتحقق والاعتماد

الاسم	عنوان	تاريخ
لمياء عبد الله الجعفري	مدير الجودة	
الدكتور خالد العيسى	عميد تقنية المعلومات والاتصالات	

قائمة التوزيع

رقم النسخة	المستفيدون	الموقع

المحتويات

ملخص تنفيذي

كلمات المرور هي جانب مهم من جوانب تأمين الحاسب الآلي. فهي تمثّل الخط الأمامي لحماية حسابات المستخدمين. فقد تؤدي كلمة المرور المختارة بطريقة سيئة إلى إلحاق الضرر بشبكة الجامعة بالكامل. ولذلك فإنّ الغرض من وجود سياسة كلمة المرور هو ضمان وجود قدر أكبر من التأمين المتجانس لشبكة الجامعة والمعلومات التي تحتوي عليها. إن تنفيذ هذه السياسة سيوفر قدر أكبر من الحماية للمعلومات الشخصية والسرية المتعلقة بجميع أفراد الجامعة والوحدات التابعة لها. بالإضافة إلى ذلك، تضع هذه السياسة معيارًا لإنشاء كلمات مرور قوية والعمل على حمايتها والمدة التي يتم فيها تغيير هذه الكلمات.

المقدمة

تقوم جامعة الإمام عبد الرحمن بن فيصل بالتحقق الشديد من الوصول إلى مصادر المعلومات عبر الإنترنت، مثل البريد الإلكتروني والبيانات المؤسسية ومواقع الجامعة ومكتبة التعليم الإلكتروني والبيانات الأكاديمية والشخصية ومصادر الحوسبة السحابية وغيرها من الخدمات الحساسة. كلمات المرور هي "مفاتيح" المستخدم للوصول إلى نظم البيانات والمعلومات بالجامعة. والتساهل في هذه الكلمات قد يؤثّر بشكل مباشر على سرية أنظمة تقنية المعلومات وسلامتها وتوافرها كما قد يؤثر سلباً على معلومات الجامعة ومعلومات المستخدم على حدّ سواء. تضع هذه السياسة الحد الأدنى من المعايير لإنشاء كلمة (كلمات) المرور الخاصة بكل شخص في الجامعة ومعايير حماية هذه الكلمة أو الكلمات. فعلى جميع المستخدمين الذين يصلون إلى مصادر تقنية المعلومات بالجامعة الالتزام بالشروط الواردة في هذه السياسة عند إنشائهم لكلمات المرور الخاصة بهم وعند العمل لحماية هذه الكلمات.

الأهداف

فيما يلي أهداف السياسة:

١. منع الوصول غير المصرح به لأنظمة جامعة الإمام عبد الرحمن بن فيصل مما قد يؤدي إلى إساءة استخدام البيانات الشخصية أو المؤسسية.

٢. التأكد من استخدام مصادر تقنية المعلومات والاتصالات بطريقة صحيحة ودعم رسالة الجامعة وأهدافها وغاياتها.

٣. تشجيع المستخدمين على فهم حقوقهم ومسؤولياتهم فيما يتعلق بحماية كلمات المرور الخاصة بهم.

٤. حماية خصوصية وسلامة البيانات المخزنة على شبكة الجامعة.

الجهات المتأثرة بهذه السياسة

تنطبق هذه السياسة على جميع الأشخاص الذين لديهم حساب على أي نظام يتم الوصول إليه على شبكة الجامعة أو أنظمة الحاسب الآلي الخاصة بها أو هم مسؤولون عن ذلك الحساب.

بيان السياسة

إرشادات وبيانات الإجراءات

إرشادات عامة:

١. يجب تغيير كلمات المرور كل ٩٠ يومًا.
٢. يجب أن تفي جميع كلمات المرور بتعريف كلمة المرور القوية الموضحة أدناه في قسم إرشادات إنشاء كلمة مرور قوية.
٣. كل كلمة مرور تأتي عقب سابقتها مباشرة يجب أن تكون فريدة ، ولن يُسمح بإعادة استخدام كلمة المرور السابقة نفسها.
٤. تنتهي صلاحية أي كلمة مرور مؤقتة في الساعة ٢٣:٥٩:٥٩ من تاريخ الإصدار.
٥. سيتم قفل حساب المستخدم مؤقتًا لمدة ثلاث (٣) دقائق بعد ثلاث عمليات تسجيل دخول فاشلة متتالية:

أ- تأمين الحساب المدة: ١٥ دقيقة.
ب- حد تأمين الحساب: ٣
ت- إعادة تعيين عداد قفل الحساب: ٣٠ دقيقة.

٦. سيتم تطبيق عملية "إعادة تعيين كلمة المرور" على المستخدمين الذين يسجلون الدخول لأول مرة.

خصائص كلمات المرور الضعيفة:

١. كلمة المرور تحتوي على أقل من ثمانية أحرف.
٢. كلمة المرور التي هي عبارة عن كلمة موجودة في القاموس (الإنجليزية أو الأجنبية).
٣. كلمة المرور التي هي عبارة عن كلمة شائعة الاستخدام مثل:

أ- اسم العائلة والحيوانات الأليفة والأصدقاء وزملاء العمل والشخصيات الخيالية، إلخ.

ب- مصطلحات الحاسوب والأسماء والأوامر وشركات المواقع والأجهزة والبرمجيات.
ت- أعياد الميلاد والمعلومات الشخصية الأخرى مثل العنوان وأرقام الهواتف.
ث- أنماط لكلمات أو أرقام مثل aaabbb ، ١١١٢٢٢، zyxwvts، ٤٦٥٤٣٢١، إلخ.
ج- أي مما ورد أعلاه مكتوب بطريقة معكوسة مثل fesuoy ، damha، الخ
ح- أي مما سبق يسبقه أو يتبعه رقم (على سبيل المثال، secret1، secret.١)

إرشادات إنشاء كلمة مرور قوية:

١. طولها ثمانية أحرف أبجدية رقمية على الأقل.
٢. لا تحتوي كلمات المرور على معرف المستخدم.
٣. لا تحتوي على أكثر من حرفين متطابقين في صف واحد ولا تتكون كلها من أرقام أو أحرف هجائية .
٤. تحتوي على ثلاثة على الأقل من فئات الأحرف الخمسة التالية:

أ- الأحرف الصغيرة
ب- الأحرف الكبيرة
ت- أعداد
ث- د. الأحرف "الخاصة" (مثل$ # @ ٪ {} ` \ = - ~ | + _ () * & ^ ":[]؛ '<> / إلخ)
ج- تحتوي على ثمانية أحرف أبجدية رقمية على الأقل.

مسؤوليات متعلقة ببيانات المستخدم

يتحمل المستخدمون مسؤولية المساعدة في حماية الشبكة وأنظمة الحاسب الآلي التي يستخدمونها. وتعد سلامة وسرية كلمة مرور الفرد عنصرا أساسيا في هذه المسؤولية. يتحمل كل شخص مسؤولية إنشاء كلمة مرور مقبولة وتأمينها وفقًا لهذه السياسة. قد يؤدي عدم الامتثال لهذه الضوابط إلى تعليق الحقوق في أنظمة الجامعة أو اتخاذ أي إجراء آخر على النحو المنصوص عليه في السياسة.

خاتمة

من خلال تطبيق سياسة الاستخدام المقبولة، نهدف إلى تحقيق النتائج التالية:

١. مجتمع جامعي مطّلع بشكل أفضل على الاستخدام المقبول وغير المقبول لمصادر تقنية المعلومات والاتصالات بالجامعة.
٢. مجتمع جامعي يكون مسؤولاً عن قيمة مصادر تقنية المعلومات والاتصالات الخاصة بالجامعة ومسؤولاً عن استخدام هذه المصادر.

انتهاك السياسة

يخضع أي شخص ينتهك هذه السياسة لأي من الإجراءات التالية أو جميعها:

- تعليق حساب الانترنت الجامعي أو الوصول إليه.
- إحالة القضية إلى الإدارة القانونية بالجامعة مشفوعة بالأدلة الداعمة لاتخاذ إجراء مناسب.
- يمكن إحالة القضية إلى هيئة الاتصالات وتقنية المعلومات بالمملكة العربية السعودية وهي الجهة التي قد تشرع في إجراء تحقيق جنائي وفقًا لأنظمة الجرائم الإلكترونية. يمكن الاطلاع على مزيد من المعلومات المتعلقة بهذه اللوائح على الرابط التالي:

  النسخة الإنجليزية:

  http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx

  النسخة العربية:

  http://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx

الملحق

تستخدم المصطلحات التالية في هذه الوثيقة.

الوصول - توصيل الجامعة أو الأجهزة الشخصية أو المملوكة لأطراف ثالثة بمرافق البنية التحتية لتقنية المعلومات والاتصالات عبر طريقة اتصال مباشر أو غير مباشر

مستخدم معتمد - فرد تم منحه حق الوصول إلى خدمات تقنية المعلومات والاتصالات بالجامعة

انتهاء الصلاحية - التاريخ الذي يلزم فيه تغيير كلمة المرور للوصول إلى أنظمة الجامعة وفقًا لمعايير كلمة المرور القوية.

مصادر المعلومات - الأصول والبنية التحتية التي تملكها الجامعة أو تسيطر عليها صراحة أو في عهدتها بما في ذلك على سبيل المثال لا الحصر البيانات والسجلات والخدمات الإلكترونية وخدمات الشبكة والبرمجيات وأجهزة الحاسب الآلي وأنظمة المعلومات.

المراجع

١. سياسة الاستخدام المقبول