مرجعية الوثيقة

	الوصف			
عنوان الوثيقة:	سياسة معايير كلمة المرور			
النسخة:	١,٠			
التصنيف:	◉ عامة	○ سرية	○ سرية عالية	○ سرية للغاية
الحالة:	معتمده	**النوع :**	وثيقة	
تاريخ الإصدار:	٢٠١٥/٠٦/٢٥			
تاريخ المراجعة:	٢٠١٥/٠٦/٢٥			

النسخة رقم	التاريخ	إعداد ومراجعة	الملاحظات
١,٠	٢٠١٥/٠٦/٢٥	الإدارة العامة لتقنية المعلومات (قسم أمن المعلومات)	النسخة الأولى من الوثيقة

الموظف المختص

النسخة رقم	التاريخ	المختص	الملاحظات
١,٠	٢٠١٥/٠٦/٢٥	محمد الشهري	تم المراجعة

الإعتماد

النسخة رقم	التاريخ	المعتمد/ المعتمدين	الملاحظات
١,٠	٢٠١٥/٠٧/٠٨	رئيس لجنة التعاملات الإلكترونية معالي مدير جامعة الملك خالد	

جدول المحتويات

١. تعريف هيكلة السياسة

تشتمل وثيقة السياسة على العناصر التالية:

- **الهدف:** وصف مختصر لأغراض وأهداف السياسة.
- **نطاق العمل:** تحدد الإدارات والجهات المختلفة الداخلية والخارجية وكذلك الأشخاص الذين تنطبق عليهم هذه السياسة.
- **الإمتثال والتنفيذ:** تحدد تبعات ونتائج أية مخالفة لهذه الساسة.
- **السياسات:** يشتمل هذا القسم على وصف لجزئية القيود/الضوابط المتعلقة بالسياسة المحددة.

٢. الهدف

الغرض من هذه السياسة هو توفير الحد الأدنى من المعايير الأمنية لكلمة المرور ليتم تنفيذها على أنظمة الكمبيوتر، وأجهزة الشبكة، وأنظمة المعلومات لدى جامعة الملك خالد.

٣. نطاق العمل

تطبق هذه السياسة على جميع الموظفين، والموردين، وشركاء العمل، والموظفين المتعاقدين، والوحدات الوظيفية لدى جامعة الملك خالد سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم؛ الذين لديهم حساب (أو أي شكل من أشكال الوصول التي تطلب اسم المستخدم وكلمة السر) على أي نظام يتبع لجامعة الملك خالد.

٤. الإمتثال و التنفيذ

في حالة مخالفة أي موظف أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لدى جامعة الملك خالد لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر- نظام العمل والعمال، ونظام مكافحة الجرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٥. **السياسات** :

- **معايير كلمة المرور**

يجب أن تكون كلمة المرور قوية؛ وهي كلمة من طول كافي لردع أي محاولة للتخمين، ويسهل تذكرها، ويصعب معرفتها من قبل الآخرين مع العلم أن كلمة المرور هي كل مايقف بين أهم بيانات الجامعة والمستخدمين الغير مصرح لهم.

موارد تقنية المعلومات لدى الجامعة يجب تهيئتها وإعدادها للإمتثال للحد الأدنى لمعايير كلمة المرور التالية:

- يجب ألا يتم تخزين كلمات المرور في نص عادي.
- كلمة المرور يجب أن تتكون من ٨ خانات كحد أدنى.
- كلمة المرور يجب أن تتكون على الأقل على ثلاث مجموعات من المدخلات
  - الأحرف الأنجليزية الكبيرة A-Z،
  - الأحرف الأنجليزية الصغيرة a-z،
  - والأرقام العشرية (٩-٠)،
  - والرموز الخاصة (بإستثناء رمز & و رمز ؟ حيث أنها غير معتمدة من قبل بعض الأنظمة).
- عدم استخدام الإسم الشخصي أو جزء منه ككلمة مرور أو كجزء من كلمة المرور.

- **معايير كلمة المرور لأصحاب الصلاحيات العالية**

يجب أن تكون كلمة المرور قوية جداً لأنظمة المعلومات وللأفراد الذين يملكون صلاحيات عالية (Administrators).

أنظمة المعلومات يجب تهيئتها وإعدادها للإمتثال للحد الأدنى لمعايير كلمة المرور التالية:

- يجب أن يتم تخزين كلمات المرور في صورة مشفرة.
- كلمة المرور يجب أن تتكون من ١٣ خانه كحد أدنى.
- كلمة المرور يجب أن تتكون من أربع مجموعات من المدخلات
  - الأحرف الأنجليزية الكبيرة A-Z،
  - الأحرف الأنجليزية الصغيرة a-z،
  - الأرقام العشرية (٠-٩)،
  - والرموز الخاصة (بإستثناء رمز & و رمز ؟ حيث أنها غير معتمدة من قبل بعض الأنظمة).
- عدم استخدام الإسم الشخصي أو جزء منه ككلمة مرور أو كجزء من كلمة المرور.

- **كلمة المرور الأولية**
  - عند انشاء مستخدم جديد، يجب أن تكون كلمة المرور الأولية للدخول الى النظام مكونة عشوائياً.
  - عند تسجيل الدخول لأول مرة الى النظام باستخدام كلمة المرور الأولية، يجب على نظام المعلومات أن يجبر المستخدم على تغييرها.
  - جميع كلمات السر الإفتراضية لأنظمة المعلومات، بما في ذلك حسابات الخدمة، يجب أن تتغير في أقرب وقت ممكن بعد تركيب النظام وقبل تشغيلة رسمياً.

- **انتهاء صلاحية كلمة المرور**
  - يجب تمكين آلية لأنظمة المعلومات تضمن انتهاء صلاحية كلمات مرور المستخدمين عند عدم تغييرها في فترة أقل من ١٨٠ يوما، ومدة لا تتجاوز ٩٠ يوما لأصحاب الصلاحيات العالية وأنظمة المعلومات الحساسة.
  - يجب أن يتم اعداد أنظمة المعلومات بمطالبة المستخدم بتحديد كلمة مرور جديدة بعد تسجيل الدخول باستخدام كلمة المرور الأولية.

- **تاريخ كلمة المرور**
  - لا يحق للمستخدم اعادة استخدام كلمات المرور المستخدمة لآخر أربع دورات (لا يمكن أن تكون كلمة المرور الجديدة واحدة من آخر أربع كلمات المرور المستخدمة).