جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	**دليل سياسات تقنية المعلومات**	**رقم السياسة**	ت.م-07
		تاريخ بدء العمل بالسياسة	2014/03/02
	الموضوع كلمة المرور	**تاريخ آخر مراجعة**	2013/12/01
		تاريخ المراجعة القادم	2016/09/01
	المكتب المسؤول: مدير تقنية المعلومات	**عدد صفحات هذه السياسة**	**1** من **1**

7. كلمة المرور

نظرة عامة

تبين هذه السياسة والإجراءات الخاصة بها معايير تحديد كلمات المرور الخاصة بمستخدمي نظم تقنية المعلومات بالجامعة

مجال التطبيق

تُطبق هذه السياسة على جميع العاملين الذين لديهم، أو هم مسؤولين عن، حسابات أو أي شكل من أشكال الدخول الذي يتطلب كلمة مرور. ويشمل ذلك أي نظام متواجد بالجامعة أو يتمتع بحق الدخول إلى الشبكة أو يخزن معلومات ليست متاحة للعامة عن الجامعة.

الهدف

تحمي سياسة إدارة كلمات المرور الفعالة بيانات الجامعة وتخفض من مخاطر الدخول غير المسموح به، وتهدف هذه السياسة إلى إنشاء بيئة آمنة لتقنية معلومات من خلال تفعيل استخدام كلمات المرور القوية.

السياسة

1) تُعدّ كلمات المرور جانباً هاماً في أمن الحواسيب، كما تُعدّ خط الدفاع الأول لحماية حسابات المستخدمين، إذ قد تتسبب كلمة المرور المنتقاة بشكل سيء في إلحاق الضرر بكامل الشبكة.

2) تقع على عاتق جميع أعضاء مجتمع الجامعة مسؤولية اتخاذ الخطوات المناسبة لاختيار كلمات مرورهم بشكل آمن.

3) يجب الاحتفاظ بكافة كلمات المرور الخاصة بالنظم في مكان آمن محدد مسبقاً.

4) يجب التعامل مع كلمات المرور كافة بوصفها معلومات حساسة وسرية في الجامعة.

5) تُفعل سياسة كلمة المرور بشكل تلقائي.

جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	دليل إجراءات تقنية المعلومات	رقم السياسة المرتبطة	ت.م-07
		تاريخ بدء العمل بالإجراءات	2014/09/01
	الموضوع كلمة المرور	تاريخ آخر مراجعة	2013/12/01
		تاريخ المراجعة القادم	2016/09/01
	المكتب المسؤول: المدير التنفيذي لقطاع تقنية المعلومات	عدد صفحات الإجراءات	1 من 1

إجراءات السياسة رقم (7) - كلمة المرور

1) عندما يتقدم المستخدم بطلب لإعادة ضبط كلمة المرور فإن ذلك يتطلب التحقق من شخصية المستخدم.

2) يجب أن تتوافق كافة كلمات المرور الخاصة بمستوى النظم والمستخدمين مع المعايير القياسية المدرجة أدناه.

3) على جميع المستخدمين الاتصال بقسم خدمة العملاء لإعادة تفعيل حساباتهم الشخصية.

الضبط	الوصف	الضبط المعرّف الخاص بالمستخدم	الضبط المعرّف الخاص بمدير العمليات
الطول الأدنى لكلمة المرور	يحدد ذلك العدد الأدنى من الحروف التي يمكن أن تتكون منها كلمة المرور	8	8
الفترة القصوى لكلمة المرور بالأيام	يجوز استخدام الفترة الزمنية لاستخدام كلمة المرور قبل أن يجبر النظام المستخدم على تغييرها، ويجوز أن تتراوح مدة الفترة الزمنية بين يوم و999 يوم وتعني القيمة "صفر" أن كلمة المرور لن تنتهي صلاحيتها على الإطلاق. وتُعدّ كلمة المرور التي لا تنتهي صلاحيتها على الإطلاق من المخاطر لأنها قد تتعرض للكشف مع مرور الوقت	تسعون يوماً	تسعون يوماً
تاريخ كلمة المرور	يحدد ذلك احتمالية استخدام كلمات المرور القديمة مجدداً، ويمثل ذلك الرقم عدد كلمات المرور الجديدة اللازم استخدامها قبل إعادة استخدام كلمة مرور قديمة	6	6
درجة تعقيد كلمة المرور	يجب أن تحتوي كلمة السر على الفئات الأربعة التالية: ▪ أحرف كبيرة باللغة الإنجليزية (مثل **A, B, C, ... Z**) ▪ أحرف صغيرة باللغة الإنجليزية (مثل **a, b, c …**) ▪ أرقام عددية من 0 إلى 9 ▪ رموز خاصة (مثل **(^*@#% :"()! .,**)	مفعلة	مفعلة
حد القفل	يشير ذلك إلى عدد محاولات الدخول الفاشلة لحساب المستخدم قبل أن يقفل الحساب	5	3
فترة القفل	الفترة التي سوف تستغرقها عملية القفل قبل إعادة الفتح	30 دقيقة	15 دقيقة
إعادة ضبط كلمة المرور	يتم تفعيل تغيير كلمة السر عند الدخول القادم لإعادة ضبط كلمة المرور أو كلمات مرور الحسابات الجديدة	تفعيل	تفعيل