

تابع قرار الرئيس الأعلى للجامعة رقم (16) لسنة 2014

06-م	رقم السياسة	دليل سياسات تقنية المعلومات	 <b>جامعة الإمارات العربية المتحدة</b> United Arab Emirates University 
2014/03/02	تاريخ بدء العمل بالسياسة		
2013/12/01	تاريخ آخر مراجعة	الموضوع أمن المعلومات	
2016/09/01	تاريخ المراجعة القادم		
1 من 2	عدد صفحات هذه السياسة	المكتب المسؤول: مدير تقنية المعلومات	

## 6. أمن المعلومات

### نظرة عامة

تبين هذه السياسة والإجراءات الخاصة بها الآليات المتبعة لتحقيق الأمن للبنى التحتية ونظم تقنية المعلومات ضد المخاطر التي تهددها.

### مجال التطبيق

تطبق هذه السياسة على أنواع الأمن التالية بالجامعة:

(1) أمن تطبيقات ونظم الحاسب

(2) الأمن المادي

(3) الأمن التشغيلي

(4) الأمن الإجرائي

(5) أمن الشبكات

### الهدف

- (1) تأمين الحماية من التدايعيات المحتملة الناتجة عن خروقات السرية أو انقطاعات الخدمة المتاحة.
- (2) ضمان حماية كافة أصول المعلومات ومرافق الشبكات والحوسبة من التلف أو فقدان أو سوء الاستخدام.
- (3) ضمان معرفة أعضاء مجتمع الجامعة بمبادئ استخدام المعلومات الإلكترونية والالتزام بها.
- (4) زيادة مستوى الوعي والفهم تجاه متطلبات أمن المعلومات في الجامعة.
- (5) زيادة الوعي من جانب المستخدمين تجاه مسؤولياتهم المباشرة عن حماية سرية وسلامة البيانات التي يمتلكونها أو يتعاملون بها.

### السياسة

- (1) تعتمد الجامعة على إتاحة وسلامة خدماتها الإلكترونية في مجالات التدريس والتعلم والبحث والإدارة. وفي إطار ذلك يكون من الضروري حماية نظم تقنية المعلومات والبنى التحتية من مخاطر أمنية سواء أكانت داخلية أو خارجية أو متعمدة أو عرضية.
- (2) يُعدّ جميع أعضاء مجتمع الجامعة مسؤولين عن الالتزام بمعرفة الآليات واللوائح التي تضمن ما يلي:
  - أ- حماية المعلومات من أي اختراق غير مسموح به.
  - ب- سرية المعلومات.
  - ج- الحفاظ على سلامة ومصادقية المعلومات.
  - د- الحفاظ على إتاحة المعلومات.
  - هـ- تحقيق المتطلبات التنظيمية والتشريعية.
  - و- تطوير خطة استمرارية العمل وفحصها والحفاظ عليها.
  - ز- إتاحة التدريب والمعرفة بأمن المعلومات بالنسبة لأعضاء هيئة التدريس والطلبة والعاملين.
  - ح- إبلاغ "خدمات تقنية المعلومات" عن كافة أشكال الخروقات الفعلية أو المحتملة لأمن المعلومات من أجل القيام بالإجراء اللازم.
  - ط- إيجاد إجراءات من شأنها دعم هذه السياسة بما في ذلك إجراءات ضبط الفيروسات وكلمات المرور وخطط الاستمرارية.
  - ي- تحقيق متطلبات إتاحة النظم والمعلومات.
  - ك- عدم السماح لأي نوع من النظم الاتصال بالشبكة دون برنامج مكافحة الفيروسات.
  - ل- تحديث جميع برمجيات مكافحة الفيروسات من قبل خدمات تقنية المعلومات بانتظام، مع التحقق من الأنظمة.
  - م- التحقق من أن جميع الملفات التي تم تحميلها عن طريق البريد الإلكتروني خالية من الفيروسات.
  - ن- التأكد من أن جميع الخوادم قد تم تزويدها ببرامج مكافحة الفيروسات وأن كفاءتها ضد الفيروسات مضمونة.
  - س- التحقق من مسح جميع الوسائط غير المثبتة من الفيروسات قبل الاستخدام من قبل المستخدم.

تابع قرار الرئيس الأعلى للجامعة رقم (16) لسنة 2014

06-م	رقم السياسة	دليل سياسات تقنية المعلومات	 <b>جامعة الإمارات العربية المتحدة</b> United Arab Emirates University 
2014/03/02	تاريخ بدء العمل بالسياسة		
2013/12/01	تاريخ آخر مراجعة	الموضوع	
2016/09/01	تاريخ المراجعة القادم	أمن المعلومات	
2 من 2	عدد صفحات هذه السياسة	المكتب المسؤول: مدير تقنية المعلومات	

- (3) يُسمح لأي مستخدم باستخدام شريحة ذاكرة في أجهزة الحواسيب المكتبية الخاصة به، بعد التحقق من خلوها من الفيروسات.
- (4) يجب أن يتم مسح جميع مراسلات البريد الإلكتروني الصادر والوارد للتأكد من خلوها من الفيروسات والمحتوى الضار.
- (5) يتم تحديث خادم البريد بشكل دوري بأحدث برامج (service packs/ patches) لمكافحة الفيروسات.
- (6) يتم عزل رسائل البريد الإلكتروني المصابة والاحتفاظ بها في الحجر الصحي مع إخطار المستخدم، وتقديم الحل الأمثل من خدمات تقنية المعلومات.
- (7) لن يحصل المستخدم على أي تفويض إداري في تفعيل أو تعطيل ميزات برنامج مكافحة الفيروسات.
- (8) يتم قفل حساب المستخدم المتضرر وفصل النظام المتضرر من الشبكة وعزله وتطويقه الى أن يتم تطهيره من قبل خدمات تقنية المعلومات.
- (9) لن يتم الوصول للبريد الإلكتروني ذو المحتوى الضار أو المشكوك فيه من قبل المستخدم دون تعليمات من قبل خدمات تقنية المعلومات.
- (10) تُعتبر "خدمات تقنية المعلومات" مسؤولة عن الحفاظ على هذه السياسة وعن تقديم الدعم والنصيحة أثناء تنفيذها.

رقم السياسة المرتبطة	ت.م-06	دليل إجراءات تقنية المعلومات	 جامعة الإمارات العربية المتحدة United Arab Emirates University 
تاريخ بدء العمل بالإجراءات	2014/09/01		
تاريخ آخر مراجعة	2013/12/01	الموضوع أمن المعلومات	
تاريخ المراجعة القادم	2016/09/01		
عدد صفحات الإجراءات	1 من 1	المكتب المسؤول: المدير التنفيذي لقطاع تقنية المعلومات	

## إجراءات السياسة رقم (6) - أمن المعلومات

### 1) السرية والخصوصية

يتحتم على جميع أعضاء مجتمع الجامعة احترام وحماية خصوصية البيانات. وبينما لا تراقب الجامعة محتوى صفحات المواقع الشخصية أو البريد الإلكتروني أو أية وسائل أخرى للتواصل الإلكتروني إلا أن للجامعة الحق في معاينة سجلات الحواسيب أو في مراقبة أنشطة الحواسيب الشخصية وذلك بموافقة إدارة الجامعة.

### 2) الولوج

لا يجوز لأحد في الجامعة الدخول إلى السجلات الخاصة إلا إذا كان مفوضاً بذلك على وجه التحديد، ويجوز للأشخاص المفوضين أن يستخدموا السجلات الخاصة لأسباب مشروعة فقط، ويجب الحفاظ على الممتلكات التكنولوجية في مكان آمن ومناسب، وينبغي على فريق الإدارة التأكد من وجود الضوابط اللازمة للحيلولة دون دخول غير المفوضين إلى النظم والشبكات وللكشف عن أي محاولات من هذا القبيل.

### 3) المساءلة

يُعتبر جميع أعضاء مجتمع الجامعة مسؤولين عن ضمان عدم استخدام الغير لامتيازاتهم وحقوقهم المتعلقة بنظام تقنية المعلومات، كما يعتبر الموظفون المخولون بالجامعة مسؤولين عن مراجعة سجلات الدخول وتحديد الخروقات الأمنية المحتملة. هذا ويجب أن تحتفظ كافة النظم المضبوطة بسجلات حتى يمكن متابعة استخدام المعلومات بدرجة مناسبة لكل نظام، كما يتعين على المسؤولين المخولين القيام بإخطار الإدارة فوراً في حالة الاشتباه في حدوث أية خروقات.

### 4) التوثيق

يتم تنفيذ التوثيق للاتصال من نقطة إلى نقطة لجميع النظم التي ترسل وتستقبل بيانات.

### 5) الإتاحة

يتوقع أن تكون نظم المهمات الحساسة متاحة في كل الأوقات. ويجب أن يكون هناك نظام حساس إضافي يتمتع بإجراءات استرداد المعلومات بشكل مفصل والإبلاغ عن الفترات التي تكون فيها النظم خارج الخدمة (أثناء عطل أو صيانة أو إصلاح)، كما ينبغي اختبار إجراءات النسخ الاحتياطية من البيانات وأن توثق بشكل جيد.

### 6) الإبلاغ عن الخروقات

تقع هذه المسؤولية على مالكي نظم التطبيقات والشبكات والحواسيب إضافة إلى مستخدمي هذه الأنظمة وتتمثل في الإبلاغ عن أية خروقات أمنية واضحة. ويجب أن تتاح الإرشادات الخاصة بالإبلاغ عن الخروقات لكل فرق الإدارة والمستخدمين، كما ينبغي أن تشمل على إرشادات تتعلق بطبيعة هذه الخروقات والزمن والمكان والشخص والإطار الزمني الذي ينبغي من خلاله الإبلاغ عن هذه الخروقات.