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

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 التداعيات المحتملة الناتجة عن خروقات السرية أو انقطاعات الخدمة المتاحة.
2) ضمان حماية كافة أصول المعلومات ومرافق الشبكات والحوسبة من التلف أو الفقدان 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 الالكترونية 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 ومصداقية المعلومات.
   د- الحفاظ على إتاحة المعلومات.
   ه- 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.

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

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.