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

1. الاستخدام المقبول لموارد تقنية المعلومات

نظرة عامة

تحدد هذه السياسة والإجراءات الخاصة بها الاستخدام المقبول لموارد تقنية المعلومات والحقوق والواجبات التي تقع على عاتق الأطراف المختلفة التي تستخدم هذه الموارد.

مجال التطبيق

تُطبق هذه السياسة على كافة المستخدمين في الجامعة.

الهدف

تضمن هذه السياسة ما يلي:

1) سلامة وحماية الحواسيب والشبكات والبيانات في الجامعة.
2) توافق استخدام التواصل الإلكتروني مع سياسات الجامعة.
3) وفاء الجامعة بالتزاماتها القانونية حول ضبط الدخول للبيانات.

السياسة

1) تُعتبر الحواسيب والشبكات ونظم المعلومات الإلكترونية موارد أساسية لتحقق الجامعة رسالتها في التدريس والبحث العلمي وخدمة الجامعة والمجتمع. وتمنح الجامعة أعضاءها حق الولوج إلى هذه الموارد بغية دعم تحقيق رسالتها.

2) تُعدّ هذه الموارد مرافق قيمة للمجتمع وينبغي استخدامها وإدارتها على نحو مسؤول لضمان أمنها وسلامتها وإتاحتها للأنشطة التعليمية المناسبة، وعلى كافة مستخدمي هذه الموارد أن يستخدموها بشكل مسؤول وفاعل.

3) يتحمل المستخدمون بالجامعة مسؤولية معرفة حقوقهم وواجباتهم تجاه هذه السياسة. وتوضح هذه السياسة المسؤولية في الاتصالات الشخصية والمسائل الأمنية وتحدد عواقب المخالفات، ويُعتبر المستخدمون مسؤولين عن تعريف أية متطلبات إضافية تتعلق بكليتهم أو الوحدة التي ينتمون إليها.

جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	دليل إجراءات تقنية المعلومات	رقم السياسة المرتبطة	ت.م-01
		تاريخ بدء العمل بالإجراءات	2014/09/01
	الموضوع الاستخدام المقبول لموارد تقنية المعلومات	تاريخ آخر مراجعة	2013/12/01
		تاريخ المراجعة القادم	2016/09/01
	المكتب المسؤول: المدير التنفيذي لقطاع تقنية المعلومات	عدد صفحات الإجراءات	1 من 4

إجراءات السياسة رقم (1) - الاستخدام المقبول لموارد تقنية المعلومات

1) تعريفات

أ- **الاستخدام المقبول**

1- لا تستخدم البيانات/المعلومات والنظم إلا من قبل الأشخاص المخول لهم استخدامها للقيام بمهام تتعلق بأداء أعمالهم، ويمنع استخدام المعلومات والنظم لمكاسب أو أعمال شخصية أو لارتكاب أعمال الغش.
2- يحظر على المستخدمين الافصاح أو الكشف عن أية معلومات دون تفويض أو تخويل رسمي، ويشكل الولوج غير المسموح به للمعلومات أو التلاعب بها أو الإفصاح عنها أو تسريبها خرقاً أمنياً قد يؤدي إلى اتخاذ عمل تأديبي يصل إلى إنهاء الخدمة والملاحقة القضائية من قبل الجهات الحكومية.
3- على المستخدمين الإلمام بحقوق ومسؤوليات مستخدمي الجامعة. وتحدد هذه الوثيقة الخطوط العريضة لمسؤولية الاتصالات الشخصية، وقضايا الأمن والخصوصية، كما تحدد عواقب الانتهاكات.
4- يجب استخدام خدمات الإنترنت لأغراض العمل فقط.
5- يحظر الدخول للمواقع المحظورة أو ذات المحتوى المحظور وفقاً لسياسة الجامعة.
6- على المستخدم عدم الدخول للمواقع المسيئة أو المساهمة فيها أو تحميل ملفات منها، وتشمل هذه المواقع المسيئة ولا تقتصر على: مواقع تروج للعنصرية، مواقع دينية ذات مشاعر تعصبية، مسيئة، أو ذات لغة عدائية، تشهيرية، أو مسيئة لفرد أو جماعة، أو ذات محتوى إباحي.
7- على مستخدمي الإنترنت عدم المساهمة في أي نشاط قد يسهم في إيقاف عمليات أنظمة الحاسب الآلي.
8- على مستخدمي الإنترنت عدم تحميل أو تنزيل أو تثبيت برمجيات من الإنترنت بدون الموافقة المسبقة من خدمات تقنية المعلومات.

ب- **المستخدم**

يطلق هذا الاسم على الشخص أو الجهة المسموح لها باستخدام موارد شبكات أو حواسيب الجامعة. ويشمل ذلك الطلبة والموظفين والهيئة التدريسية والخريجين والجهات التي لها ارتباطات بالجامعة تخول لها استخدام موارد تقنية المعلومات الخاصة بالجامعة. وقد يمنح بعض المستخدمين تفويضاً إضافياً للدخول إلى البيانات المؤسسية وذلك بتفويض من قبل صاحب البيانات أو الأمين عليها.

ج- **الأمين على البيانات**

الأمناء على البيانات هم ممثلي الجامعة المفوض لهم مسؤولية القيام بالإشراف على بيانات الجامعة في مجال معين. وينوط بهؤلاء الأمناء مسؤولية تطوير الاجراءات اللازمة لعمل وحفظ واستخدام هذه البيانات وفق سياسات وإجراءات معلنة.

د- **موارد تقنية المعلومات**

تشمل هذه الموارد المرافق والتقنيات وموارد المعلومات التي تستخدم لمعالجة بيانات الجامعة وتداولها وتخزينها. ويدخل ضمن نطاق هذا التعريف مختبرات الحواسيب وتقنيات الفصول الدراسية والحوسبة وطرق وخدمات التواصل الإلكتروني كالمودم والنقاط اللاسلكية للاتصال بالإنترنت والبريد الإلكتروني والشبكات والهواتف والبريد الصوتي والفاكس والفيديو والوسائط المتعددة والمواد التدريسية وغيرها من خدمات وموارد ومعدات الجامعة.

ه- **الحوادث الأمنية**

يشمل ذلك أي حادث سواءً كان مقصوداً أو غير مقصود من شأنه أن يؤثر على المعلومات أو التكنولوجيا ذات الصلة التي تتسبب في تسرب أو سلامة المعلومات أو اضطراب و/أو عدم القدرة على الدخول إلى البيانات المطلوبة.

و- **الإجراءات الأمنية**

يُقصد بها العمليات والبرمجيات والأجهزة التي تُستخدم من قبل مديري النظم والشبكات لضمان سرية وسلامة وإتاحة موارد تقنية المعلومات التي تمتلكها الجامعة. وقد تتضمن الإجراءات الأمنية مراجعة الملفات من أجل اكتشاف أي خروقات للسياسة وللتحري عن الأمور المرتبطة بأمن المعلومات.

جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	**دليل إجراءات تقنية المعلومات**	**رقم السياسة المرتبطة**	ت.م-01
		تاريخ بدء العمل بالإجراءات	2014/09/01
	الموضوع الاستخدام المقبول لموارد تقنية المعلومات	**تاريخ آخر مراجعة**	2013/12/01
		تاريخ المراجعة القادم	2016/09/01
	المكتب المسؤول: المدير التنفيذي لقطاع تقنية المعلومات	**عدد صفحات الإجراءات**	2 من 4

2) المسؤوليات

أ- **حقوق وواجبات ومسؤوليات المستخدم**

1- يصرح لأعضاء أسرة الجامعة باستخدام موارد تقنية المعلومات بغية تسهيل أنشطتهم العلمية والبحثية والوظيفية المتعلقة بالجامعة. بيد أن المستخدمين يوافقون باستخدامهم هذه الموارد على التقيد والالتزام بكل إجراءات وسياسات الجامعة في المجالات التي تتضمن على سبيل المثال لا الحصر المضايقات والسرقة الأدبية والاستخدام التجاري والأمن الإلكتروني والتصرف غير الأخلاقي والقوانين التي تحظر السرقة والخروقات المتعلقة بحقوق الطبع والتراخيص والتدخلات غير القانونية وقوانين سرية البيانات.

2- تنطبق هذه القيود والالتزامات بسياسات الجامعة في هذا المجال على الضيوف المصرح لهم باستخدام موارد تقنية المعلومات الخاصة بالجامعة.

ب- **تقع على عاتق المستخدمين مسؤولية ما يلي:**

1- استعراض وفهم كل السياسات والإجراءات والقوانين المتعلقة بالدخول واستخدام موارد تقنية المعلومات والتقيد بها.

2- الاستفسار من مدراء النظم أو الأمناء على البيانات عن توضيح سبل الدخول أو الاستخدام المقبول والآمن لموارد تقنية المعلومات في الجامعة.

3- الإبلاغ عن أي خروقات للسياسة المعتمدة للجهات المعنية أو للإدارة.

ج- **المسؤولية عن الاتصالات الشخصية**

يُعتبر مستخدمو موارد تقنية المعلومات في الجامعة مسؤولين عن محتوى اتصالاتهم الشخصية. ولا تقبل الجامعة أي مسؤولية عن أي استخدام شخصي أو غير مصرح به لمواردها من قبل مستخدميها.

د- **السرية والوعي الأمني**

يجب أن يعي المستخدمون أن الجامعة لا تضمن السرية أو الأمن الإلكتروني المطلقين رغم اتخاذها إجراءات أمنية جيدة لحماية أمن مواردها الحاسوبية وحساباتها الخاصة بأعضائها، ويجب على المستخدمين أن يتبعوا الإجراءات الأمنية المناسبة.

ه- **تبعات الخروقات والمخالفات**

لا يتم ايقاف امتيازات استخدام موارد تقنية المعلومات في الجامعة دون سبب، ويجوز للجامعة أن توقف الدخول مؤقتاً لبعض الموارد إذا تبين لها أثناء التحري أنه ضروري لحماية سلامة وأمن حواسيبها وشبكاتها. ويتم إحالة المخالفات المزعومة للسياسة للجهة المعنية في الجامعة، وبناء على طبيعة وخطورة المخالفة قد يتسبب ذلك في سحب امتيازات الدخول أو إجراء تأديبي من قبل الجامعة أو الملاحقة الجنائية.

و- **حقوق وواجبات الجامعة**

1- تمتلك الجامعة - بصفتها مالكة الحواسيب والشبكات التي تشكل البنية التحتية الفنية للجامعة - كافة البيانات الأكاديمية والإدارية الرسمية الموجودة في نظمها وشبكاتها. وتُعدّ الجامعة مسؤولة عن اتخاذ الإجراءات اللازمة لضمان أمن نظمها وحسابات وبيانات مستخدمي مواردها، وعند إحاطة الجامعة بأية مخالفات وخروقات إما من خلال الأنشطة الروتينية لإدارة النظم أو من خلال شكوى، تُعتبر مسؤولية الجامعة حينئذ القيام بإجراء التحريات اللازمة، ولها أن تتخذ الإجراءات الضرورية لحماية مواردها و/أو توفير المعلومات المتعلقة بالتحريات.

2- يجوز للوحدات المختلفة بالجامعة أن تحدد شروطاً إضافية لاستخدام الموارد أو المرافق التي تقع تحت مسؤوليتها، ويجب أن تكون هذه الشروط الإضافية متوافقة مع سياسات الجامعة عموماً ولها أن توفر تفاصيل وخطوطاً إرشادية و/أو قيوداً إضافية.

3- فيما يلي أدوار ومسؤوليات الجهات والأشخاص المعنيين بتقنية المعلومات في الجامعة:

– المدير التنفيذي لقطاع تقنية المعلومات

جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	**دليل إجراءات تقنية المعلومات**	**رقم السياسة المرتبطة**	ت.م-01
		تاريخ بدء العمل بالإجراءات	2014/09/01
	الموضوع الاستخدام المقبول لموارد تقنية المعلومات	**تاريخ آخر مراجعة**	2013/12/01
		تاريخ المراجعة القادم	2016/09/01
	المكتب المسؤول: المدير التنفيذي لقطاع تقنية المعلومات	**عدد صفحات الإجراءات**	3 من 4

(1) إنشاء ونشر وتطبيق القوانين الخاصة باستخدام موارد تقنية المعلومات.
(2) وضع سياسات وإجراءات أمنية كافية لحماية البيانات والأنظمة.
(3) مراقبة وإدارة استخدام موارد النظام.
(4) التحري عن المشاكل والمخالفات المزعومة لسياسات تقنية المعلومات في الجامعة.
(5) إحالة المخالفات لمكاتب الجامعة المعنية لاتخاذ قرارات أو إجراءات تأديبية.

- الكليات والأقسام

(1) إنشاء ونشر وتطبيق شروط الاستخدام التي يجب أن تتفق مع سياسات الجامعة بالنسبة للمرافق والموارد التي تقع تحت سلطتهم.
(2) مراقبة استخدام موارد الجامعة التي تقع تحت سلطتهم.
(3) إحالة المخالفات لمكاتب الجامعة المعنية لاتخاذ قرارات أو إجراءات تأديبية، ويجب الإبلاغ عن مخالفات السياسة للمدير التنفيذي لقطاع تقنية المعلومات.

- الأمناء على البيانات

(1) منح المستخدمين حق الدخول للبيانات والتطبيقات التي يعملون عليها بالتنسيق مع "خدمات تقنية المعلومات"، انطلاقاً من الحاجة التي تتوقف على طبيعة العمل.
(2) مراجعة حقوق الدخول بالنسبة للمستخدمين بشكل دوري.
(3) الإجابة عن أسئلة واستفسارات المستخدمين المتعلقة بالاستخدام المناسب للبيانات.
(4) تحديد مدى حساسية وخطورة البيانات والتطبيقات التي يتعاملون معها.

- مدراء النظم والشبكات

(1) اتخاذ إجراءات مناسبة لضمان الاستخدام المسموح به وضمان أمن البيانات والشبكات.
(2) المشاركة وتقديم النصح والإرشاد في مجال تطوير شروط الاستخدام أو إجراءات الاستخدام المسموح به.
(3) التعاون مع أقسام الجامعة وموظفي تطبيق القانون في التحقيق في المخالفات والخروقات المزعومة للسياسة أو القانون بما في ذلك حق الدخول لموارد الجامعة الإلكترونية بعد أخذ الموافقات اللازمة.

- ضابط أمن المعلومات

حماية البيانات والنظم والشبكة والتنسيق مع كادر فني يعنى بأمن المعلومات لضمان سرية وخصوصية وسلامة وإتاحة النظم والبيانات ولضمان اتخاذ الإجراء المناسب في الوقت المناسب.

3) الحقوق والمسؤوليات والإذن بالدخول

أ- **سوء الاستخدام**

1- على أي عضو من أعضاء مجتمع الجامعة يشك في وجود خرق للاستخدام المقبول لموارد تقنية المعلومات أن يبلغ مديره المباشر بذلك.

2- عند إبلاغ المدير المباشر بحالة سوء استخدام أحد أجهزة موارد تقنية المعلومات، يقوم بإبلاغ مكتب خدمة العملاء التابع لـ"خدمات تقنية المعلومات" أو طاقم تقنية المعلومات التابع لإدارته كي يقوموا بعزل الجهاز وإعداد "تقرير حالة" لتوثيق حالة سوء الاستخدام.

3- يقوم المدير المباشر أيضاً بإبلاغ رئيس الوحدة بحادثة الخرق لمناقشة الإجراء الذي سيتخذ.

ب- **الدخول لموارد تقنية المعلومات**

1- يتم توفير كافة موارد تقنية المعلومات والخدمات ذات الصلة وإتاحتها للمستخدمين. وتحدد إدارة الموارد البشرية في الجامعة وإدارة التسجيل الطلبة وأعضاء هيئة التدريس والعاملين الذين لهم حق استخدام هذه الموارد، كما يحدد رئيس كل وحدة حقوق الدخول بالنسبة لأعضاء هيئة التدريس الزائرين والعاملين المؤقتين والاستشاريين.

جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	دليل إجراءات تقنية المعلومات	رقم السياسة المرتبطة	ت.م-01
		تاريخ بدء العمل بالإجراءات	2014/09/01
	الموضوع الاستخدام المقبول لموارد تقنية المعلومات	تاريخ آخر مراجعة	2013/12/01
		تاريخ المراجعة القادم	2016/09/01
	المكتب المسؤول: المدير التنفيذي لقطاع تقنية المعلومات	عدد صفحات الإجراءات	4 من 4

2- لا يجوز لأصحاب أو مستخدمي أي حاسب أو خادم أو أجهزة وخدمات تقنية معلومات ضمن الشبكة أن يمنحوا للغير حقاً بالدخول أو حسابات على موارد تقنية المعلومات إلا بموافقة مسبقة.

3- يحظر تركيب البرامج غير المرخصة، والتشفير غير القياسي.

4- يحظر استخدام برامج مسح الشبكة، ونسخ البرامج، وتوزيع أو اعتراض المعلومات، أو الاستيلاء على كلمات السر دون إذن مسبق.

5- يجب أن تؤخذ شروط الترخيص لأي برامج في الاعتبار دائما.

6- يتم استخدام البرامج وفقاً للقوانين الاتحادية والمحلية في الدولة، بما فيها تحديداً قوانين حقوق التأليف والنشر، والمعاملات التجارية وبراءات الاختراع.

7- ظروف خاصة
- صلاحية منح الدخول لموارد الشبكة المشتركة داخل كل وحدة هي مسؤولية رئيس الوحدة التي تملك هذه الموارد.
- صلاحية منح الدخول لموارد الشبكة المشتركة والخاصة بالجامعة ككل هي مسؤولية رئيس كل وحدة بالإضافة إلى المدير التنفيذي لقطاع تقنية المعلومات.

ج- **صلاحية الدخول لبيانات المستخدمين**

1- تُعتبر سرية وأمن البريد الإلكتروني ذات أهمية كبرى. ويجب الحصول على موافقة خطية من مكتب المدير قبل السماح بالدخول إلى البريد الإلكتروني لأي من أعضاء مجتمع الجامعة.

2- الدخول إلى البريد الإلكتروني لأي قسم وقائمة المراسلات الخاصة به يجب أن يكون بموافقة رئيس القسم أو المدير المباشر.

3- يجب أن يقوم المدير التنفيذي لقطاع تقنية المعلومات بالموافقة على طلبات الدخول إلى سجلات البيانات الخاصة باستخدام المعلومات وتقنية الاتصالات.

4- يجب الحصول على موافقة خطية من رئيس الوحدة المعنية أو العميد والمدير التنفيذي لقطاع تقنية المعلومات قبل السماح بالدخول للبيانات الموجودة في جهاز حاسب مكتبي.

د- **فقدان البيانات**

يُعدّ المستخدمون مسؤولون عن عمل نسخ احتياطية من ملفاتهم الخاصة، كما يجب ألا يفترضوا وجود نسخ احتياطية لتلك الملفات على أجهزتهم. ويتعين على المستخدمين الحفاظ على نسخ احتياطية وأرشفتها وذلك بالنسبة للبيانات المهمة على أجهزتهم، علماً بأن رسائل البريد الإلكتروني المحذوفة والتي تكون أقدم من 30 يوما غير قابلة للاسترداد؛ كما أن استرداد رسائل البريد الإلكتروني المحذوفة هو خدمة ذاتية، يتم تنفيذها بواسطة مالك البريد الالكتروني.

ه- **الاستخدام والمسؤوليات**

1- المستخدم هو المسؤول عن حماية والمحافظة على المعلومات المخزنة في الحاسب المكتبي والحاسب المحمول من الضرر، أو السرقة أو الضياع.
2- في حالة سرقة الحاسب المحمول/الهاتف النقال، يجب على المستخدم إبلاغ الشرطة وخدمات تقنية المعلومات على الفور.
3- في حالة ضرر أو ضياع الحاسب المحمول/ الهاتف النقال، يجب على المستخدم ابلاغ خدمات تقنية المعلومات.
4- يجب على المستخدم عدم ترك الحاسب المحمول/ الهاتف النقال في الأماكن العامة دون مراقبة.
5- يجب استخدام كلمة مرور حماية لإغلاق الشاشة للحاسب المحمول/ الهاتف النقال بعد الانتهاء من استخدامهما.
6- يجب على المستخدم عدم توصيل أجهزة الحاسب الآلي الشخصية على شبكة الجامعة.
7- يجب على المستخدم عدم تغير الوظائف الإدارية في الحاسب المحمول بأي شكل من الأشكال، مثل نظام التشغيل في الجهاز، أو تعريف مسؤول النظام، وكلمة المرور.