جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	**دليل سياسات تقنية المعلومات**	**رقم السياسة**	ت.م-02
		تاريخ بدء العمل بالسياسة	2018/08/12
	الموضوع التحكم في الوصول للبيانات والمعلومات	**تاريخ آخر مراجعة**	2018/04/15
		تاريخ المراجعة القادم	2021/09/01
	المكتب المسؤول: مدير تقنية المعلومات	**رقم الصفحة**	1 من 1

2. التحكم في الوصول للبيانات والمعلومات

نظرة عامة

تحدد هذه السياسة والإجراءات الخاصة بها كيفية إدارة التحكم في الوصول إلى كافة البيانات والمعلومات الإلكترونية في الجامعة.

مجال التطبيق

تُطبق هذه السياسة على جميع أعضاء مجتمع الجامعة والمتعاقدين كطرف ثالث وأي جهة ترتبط بأي شكل بمعلومات أو بيانات أو برامج أو الموارد أو الأجهزة أو مرافق المعالجة ذات الصلة أو تتعامل بأي شكل مع هذه الأصول.

الهدف

ضمان تطبيق الجامعة لعملية التحكم في الوصول إلى المعلومات الإلكترونية المتعلقة بالجامعة، وضمان توافقها مع المتطلبات القانونية والتجارية والأمنية حيثما تقتضي الحاجة.

السياسة

(1) إن الالتزام بسياسة التحكم في الوصول للمعلومات في الجامعة يقلل فرص التعرض للخروقات الأمنية في الوقت الذي يسمح لمدراء الأنظمة وموظفي الدعم الفني في قطاع تقنية المعلومات بأن يقوموا بأنشطتهم في إطار السياسات.

(2) يتم التحكم في الوصول للمعلومات ونشرها أو التفويض بذلك على أساس المتطلبات الأمنية والعملية.

(3) يقتصر التحكم في الوصول لمعلومات وبيانات الجامعة على المستخدمين المسموح لهم فقط وذلك لمنع تعرض التطبيقات أو البيانات والمعلومات لأي خرق أو تعديل عرضي أو غير مقصود.

جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	**دليل إجراءات تقنية المعلومات**	**رقم السياسة المرتبطة**	ت.م-02
		تاريخ بدء العمل بالإجراءات	2018/08/12
	الموضوع التحكم في الوصول للبيانات والمعلومات	**تاريخ آخر مراجعة**	2018/04/15
		تاريخ المراجعة القادم	2021/09/01
	المكتب المسؤول: مدير تقنية المعلومات	**رقم الصفحة**	1 من 5

إجراءات السياسة رقم (2) - التحكم في الوصول للبيانات والمعلومات

1. تنظيم التحكم في الدخول للبيانات والمعلومات

أ- تسجيل المستخدم

(1) تتحكم إجراءات تسجيل هوية المستخدم في منح صلاحية الدخول للحسابات أو وقفها أو حذفها.
(2) يتم إنشاء وتفعيل حسابات المستخدمين (التابعون للجامعة أو المتعاقدون كطرف ثالث أو المندوبون عن عملاء) لفترة محدودة ووفق الضرورات الأكاديمية أو الإدارية أو العملية.
(3) يجب أن تتبع أسماء حسابات المستخدمين المعايير القياسية المتعلقة باسم المستخدم والسمات وقائمة التوزيع ورابطة المجموعات الأمنية وخواص صندوق البريد الإلكتروني وما إلى ذلك كما هو مدرج في الجزء الخاص بإجراء تسجيل حساب للمستخدم.

ب- التفويض

لا يتم إنشاء أو وقف أو حذف حسابات المستخدمين إلا بموافقة الجهة المعنية، ويتحمل الكادر المفوض المعني بإنشاء حسابات المستخدمين مسؤولية تأكيد مستوى التفويض الفعلي الممنوح للمستخدمين كلما وحيثما اقتضت الحاجة.

ج- تتبع المستخدمين

(1) يتم إنشاء حسابات مميزة لا تتكرر حتى يتم التعرف على هويات المستخدمين دائماً أثناء استخدامهم للحاسب أو للمرافق ذات الصلة.
(2) يتم عمل تسوية ومراجعة لحسابات المستخدمين بشكل دوري.
(3) يتم إرفاق رقم مرجعي لا يتكرر مع كل طلب بإنشاء حساب للمستخدمين وذلك للتمكن من تتبع المستخدمين.
(4) يسمح بإنشاء حسابات مشتركة تضم أكثر من مستخدم بشرط أن يظل الاستخدام داخلياً، ويتم إيقاف خدمة الانترنت عن هذه الحسابات.
(5) يسمح بإنشاء صناديق بريد إليكترونية مشتركة تضم أكثر من مستخدم على أن يتم تعيين اسم مالك واحد لكل حساب لأغراض تتعلق بالتتبع والمسؤولية.

د- المسؤولية

تشمل عملية تسجيل حساب للمستخدم مسؤوليات محددة بالنسبة للكادر الذي يقوم بتشغيل عمليات حساسة في إنشاء ووقف وحذف حسابات المستخدمين أو غير ذلك، وهذا يضمن عدم تضارب المصالح كأن يكون نفس الشخص طالباً لحساب ومنشئاً له.

ه- تنظيم الامتيازات

(1) يقتصر الدخول إلى نظم التشغيل وتطبيقاتها بشكل عام على مديري النظم المسؤولين وفريق الدعم المرتبط بإدارة وصيانة أساسيات الحواسيب فيما يخص الكيانين المادي والبرمجي.
(2) يمنح المستخدمون امتيازات مع حساباتهم وفق ما يحدده ويفوضه لهم رئيسهم وذلك حسب ما يتناسب ودورهم ووظيفتهم على وجه الخصوص.
(3) يتم تقييم امتيازات المستخدمين على أساس دوري منتظم (على أن تحدد مواعيد التقييمات بالاتفاق مع الأمين على البيانات أو مالك النظام) ويجب اتخاذ الإجراء اللازم وفق نتيجة عملية التقييم، وسيتم إبطال صلاحية التحكم في الدخول للبيانات والمعلومات عندما لا توجد الحاجة لمنح هذه الصلاحية.

و- تنظيم كلمة المرور

يتم التحكم باستخدام أو منح كلمة المرور وفق سياسة كلمة المرور.

ز- تنظيم تقييم دخول المستخدمين

(1) يشرف "قطاع تقنية المعلومات" على تنظيم وتطبيق الإجراءات التي تقوم من خلالها الفرق المسؤولة بتقييم تداول رموز التعريف وصلاحيات الدخول للبيانات.
(2) تضمن التدقيقات نصف السنوية إلغاء حسابات ورموز تعريف المستخدمين الذين انقطعت علاقاتهم بالجامعة.
(3) يجب أن تكون هناك إجراءات واضحة لضمان تغير صلاحية الدخول للمستخدمين الذين نقلوا لمواقع أو أقسام أخرى في ضوء تغير متطلبات العمل وبالتالي تعديل ذلك في النظام. وتتم هذه العملية بناء على إشعار من إدارة الموارد البشرية.
(4) يجب تقييم حقوق دخول المستخدمين على فترات منتظمة.

ح- الأجهزة غير المستخدمة

(1) يجب حماية كافة أجهزة الحاسب التي تنتمي للشبكة بكلمة مرور وشاشة توقف معيارية.
(2) توقف الأجهزة النشطة بعد الإطار الزمني المحدد مسبقاً.
(3) ينصح المستخدمون بإيقاف أجهزتهم النشطة التي لا يعملون عليها.
(4) مسؤولية ترك أجهزة الحاسب غير مستخدمة تقع على عاتق المستخدمين.
(5) أفضل طريقة للقفل التلقائي لشاشة التوقف هي أن يضبط المؤقت على 15 دقيقة بحيث يتم توفير الأمن الضروري، في الوقت الذي لا يتسبب ذلك في إزعاج المستخدم.

ط- بث الرسائل

(1) يتم بث الرسائل الهامة لجميع أعضاء مجتمع الجامعة عبر البث الشامل بالبريد الالكتروني.
(2) نشر رسائل البث والولوج إليها من صلاحيات قطاع تقنية المعلومات بالجامعة تحت إشراف مدير تقنية المعلومات.
(3) صلاحية إرسال رسائل البريد الإلكتروني عبر البث الشامل تكون للموظفين المصرح لهم فقط من الجامعة.
(4) منح وإدارة صلاحيات إرسال رسائل البريد الإلكتروني عبر البث الشامل يتم على أساس صلاحيات التوقيع المرفقة بهذا الدليل.

2. ضبط الدخول للشبكة

أ- **التحقق من المستخدم في حال الاتصالات الخارجية**

(1) يزود المستخدمون عن بعد بنظام اتصال بشبكة خاصة افتراضية بعد أخذ الموافقات المطلوبة.
(2) يتم تفعيل تشفير حركة المرور الإلكتروني بين المستخدم والخادم من أجل المستخدمين عن بعد.

ب- **أمن محيط الشبكة**

(1) يتم حماية الشبكات الداخلية وعزلها عن الإنترنت وشبكات الجهات الأخرى من خلال جدران الحماية.
(2) يتم تعريف أجهزة الموجه وجدران الحماية لمنع اختراق عنوان تعريف الإنترنت وإيقاف الخدمة والمشاكل الشائعة الأخرى المتعلقة بالإنترنت.
(3) يجب تعريف جدران الحماية على وجه الخصوص لمنع كافة الاتصالات القادمة عدا الاتصالات المطلوبة تحديداً من أجل متطلبات العمل والتي يجب توثيقها والموافقة عليها بشكل رسمي، ويجب توفير أي اتصال من الشبكة الخارجية من خلال جداران حماية بعد الموافقات اللازمة.
(4) يُحظر الدخول إلى الشبكة من خلال أي آلية تحكم عن بعد غير مرخص لها.

ج- **أمن وسلامة الخادم**

(1) لا يجب تعريض أي خادم للإنترنت مباشرة، إذ يجب وضع كافة الخادمات التي تقع تحت مسؤولية "قطاع تقنية المعلومات" أو أي جهة أخرى داخل الجامعة ضمن منطقة داخلية لجدران الحماية.
(2) يتم وضع الخادمات التي يمكن الدخول لها من الإنترنت في منطقة معزولة وتتم ترجمة عناوين تعريف الإنترنت كترجمة في عنوان الشبكة.

(3) يتم تقوية وتدعيم كافة الخادمات وفق وثائق التدعيم المحددة التي يقدمها موردو أنظمة التشغيل والأجهزة.
(4) يتم توزيع الخادمات في شبكة منطقة محلية افتراضية.
(5) تحتفظ كافة الخادمات الموجودة في الشبكة بالتزامن الوقتي لضمان دقة التدقيقات.
(6) يجب إجراء اختبارات اختراق نقاط الضعف قبل الانتقال إلى شبكة الإنتاج.
(7) يجب على كافة الأنظمة توجيه جميع السجلات إلى نظام تسجيل مركزي موحد يتم توفيره من خلال قطاع تقنية المعلومات بالجامعة.
(8) يجب تثبيت الخوادم في غرف آمنة، بعد موافقة قطاع تقنية المعلومات بالجامعة.

د- **أمن أجهزة الشبكة**
(1) تبقى منافذ الاتصال القابلة للدخول عليها بشكل خارجي غير مفعلة في كافة عناصر الشبكة النشطة والنظم مالم يتم فتحها تحديداً لنشاط ما (مثل متطلبات تتعلق بالعميل وأنشطة أخرى كاختبار الاختراق وتقييم مستوى الضعف)، ويجب الحصول على موافقة مسبقة من "قطاع تقنية المعلومات" قبل الشروع بأي نشاط.
(2) تحتفظ كافة عناصر الشبكة بالتزامن الوقتي لضمان دقة التدقيقات.

ه- **أمن الشبكة الداخلية**
يتم تعريف أجهزة الشبكات لضمان تحديد دخول المستخدمين للنظام حسب الحاجة ولضمان تجنب تجوال الشبكة بشكل مطلق وغير محدود. ويتم تحقيق ذلك من خلال ما يلي:
(1) فصل وعزل شبكات الإنتاج عن شبكات عدم الإنتاج.
(2) فصل معدات توصيل الشبكات والخادمات عن بيئة المستخدم.

و- **أمن الشبكة الخارجية**
(1) يجب أن تمر كافة اتصالات تصفح الإنترنت ضمن الجامعة من خلال خادمات مزودة ببديل.
(2) تكون كافة الاتصالات بالجامعة عبر الإنترنت مؤمّنه من خلال استخدام شبكة خاصة.
(3) تخضع كافة متطلبات الدخول الخارجية لتقييم المخاطر وفقاً لمتطلبات العمل ولن يتم السماح بذلك إلا بعد اكتمال كافة متطلبات الأمان المطلوبة.

ز- **إدارة تغيير الشبكة**
يجب أن تتقيد كافة التغييرات التي تطرأ على بنية الشبكة أو تعريفاتها لعناصر الشبكة والتي قد تؤثر على الأمن (حركة الخادمات وإضافة خادمات جديدة وأجهزة شبكات) بعملية التغيير كما هي معرفة من خلال "قطاع تقنية المعلومات".

3. ضبط الدخول لنظام التشغيل

أ- **إجراءات الدخول الآمن**
(1) تتم إتاحة خدمات المعلومات من خلال عملية الدخول الآمن، حيث تتعرف عملية الدخول لنظام الحاسب على الحد الأدنى من المعلومات الخاصة بالنظام لمنع المستخدمين غير المسموح لهم من الدخول إلى المعلومات غير الضرورية.
(2) تشمل إجراءات تسجيل الدخول السمات التالية:
- يجب أن يكون لكل النظم تسجيل دخول معرف يذكر فيه أن النظام لمستخدمي الجامعة فقط ويجوز أن يخضع للمراقبة.
- يجب ألا تحوي إجراءات تسجيل الدخول توضيح الأخطاء التي من الممكن أن تحدث أثناء عملية الدخول.
- يتم تعريف النظم لإغلاق حساب المستخدم بعد تحديد مسبق لعدد المحاولات غير الناجحة.
- محاولات تسجيل الدخول غير الناجحة يتم تسجيلها لكل المستخدمين.
- يتم تسجيل كافة محاولات الدخول بالنسبة للمستخدمين الفنيين (مثل مدراء النظم ومدراء قواعد البيانات ومدراء الشبكات) لفترة تحدد مسبقاً.

جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	**دليل إجراءات تقنية المعلومات**	**رقم السياسة المرتبطة**	ت.م-02
		تاريخ بدء العمل بالإجراءات	2018/08/12
	الموضوع التحكم في الوصول للبيانات والمعلومات	**تاريخ آخر مراجعة**	2018/04/15
		تاريخ المراجعة القادم	2021/09/01
	المكتب المسؤول: مدير تقنية المعلومات	**رقم الصفحة**	4 من 5

ب- **التحقق والتأكد من المستخدم**

(1) يكون لكل مستخدم بما في ذلك طاقم الدعم الفني كالمشغلين ومدراء الشبكات ومبرمجي النظم ومدراء قواعد البيانات اسم مستخدم مختلف ومميز حتى يتسنى تتبع الأنشطة وربطها بمستخدمها، ويجب ألاّ يحمل اسم حساب المستخدم أي مدلول على المستوى الوظيفي للمستخدم كالمدير أو المشرف.

(2) يتم وضع كل المستخدمين ذو صلاحية استخدام نظام ما في مجموعة مستقلة كي يتسنى تدقيق حساباتهم.

(3) يتم التعطيل المؤقت لحسابات المستخدمين التي يشتبه في تعرضها للخطر أو تعرض كلمات المرور الخاصة بها للسطو أو السرقة. عندئذ يتم إبلاغ صاحب الحساب ذي الصلة وتُقيد الواقعة في سجلات مكتب خدمة العملاء باعتبارها حادثاً ذي صبغة أمنية يستحق إجراء المزيد من التحقيقات واتخاذ القرارات المناسبة.

ج- **نظام إدارة كلمة المرور**

يساعد نظام إدارة كلمة المرور على اختيار كلمة مرور قوية ويؤكد على تطبيق إرشادات معينة تتعلق بكلمة المرور يجب التقيد بها. ولنظام إدارة كلمة المرور السمات التالية على الأقل:

(1) يجب ألاّ يسمح النظام باختيار كلمات المرور إلا كما هو مدرج في سياسة كلمة المرور.

(2) يجب أن يسمح النظام للمستخدمين بتغيير كلمات مرورهم.

(3) يجب على النظام أن يكون قادراً على حفظ عمر وتاريخ كلمة المرور كما هو مبين في سياسة كلمة المرور وأن يمنع استخدام كلمة المرور نفسها.

(4) يجب على النظام ألاّ يخزن كلمات المرور في شكل نص واضح، بل عليه أن يحفظ كلمات المرور باستخدام التشفير والترميز.

(5) يجب أن يجبر النظام المستخدمين على تغيير كلمات مرورهم المؤقتة عند الدخول الأول لهم.

(6) يجب على النظام ألاّ يعرض كلمات المرور على الشاشة عند إدخالها.

(7) يجب على النظام التأكيد على قبول كلمة السر الجديدة عند تغييرها بنجاح.

د- **استخدام مرافق النظام**

تحتوي معظم أجهزة الحاسب على برنامج واحد أو أكثر للنظام (Editors, Compilers, Ntbackup, Disk Fragmentors) وتكون هذه البرامج قادرة على إبطال التطبيقات والنظام والسيطرة عليها ،لذا فإنه من الضروري أن يكون استخدامهم محدوداً ومراقباً جداً. وينبغي التقيد بما يلي على الأقل:

(1) يجب تعريف كافة النظم بأدنى حد لصلاحيات الدخول وذلك وفق المتطلبات الضرورية للمستخدم، وستتقيد جميع تركيبات النظم بسياسات تدعيم لها.

(2) لا يجوز تركيب طرف ثالث مساعد على أي نظام دون تخويل مسبق من "قطاع تقنية المعلومات".

ه- **فترة التوقف**

إن التوقف النهائي للجهاز المستخدم مطلوب لإغلاق الاتصال بعد فترة محددة من عدم النشاط. ويتم تعريف التوقف النهائي للجهاز المستخدم في نظم العاملين وفق المتطلبات الأمنية والفنية التي يحددها المستفيدين. وبالنسبة للجامعة يتم تعريف ما يلي:

(1) جلسة Telnet/SSH كلما كانت في وضع العمل، يتم تعريف وقت التوقف بالنسبة لأجهزة الشبكة لمدة لا تتجاوز 5 دقائق.

(2) وتشتمل أيضاً التطبيقات الداخلية الأخرى (Client/Server. Web based) على وقت توقف كما هو محدد.

و- **تقييد وقت الاتصال**

(1) يجب تحديد الفترة الزمنية التي يسمح خلالها لخدمات الحاسب بالاتصال بالنسبة للنظم الحرجة/ذات المخاطر الكبيرة.

(2) يجب تحديد الفترة الزمنية التي يتم بعدها تقييد الجلسات النشطة.

جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	**دليل إجراءات تقنية المعلومات**	**رقم السياسة المرتبطة**	ت.م-02
		تاريخ بدء العمل بالإجراءات	2018/08/12
	الموضوع التحكم في الوصول للبيانات والمعلومات	**تاريخ آخر مراجعة**	2018/04/15
		تاريخ المراجعة القادم	2021/09/01
	المكتب المسؤول: مدير تقنية المعلومات	**رقم الصفحة**	5 من 5

4. ضبط الدخول للمعلومات والتطبيقات

أ- **تقييد الدخول للمعلومات**

يمنح المستخدمون صلاحية الوصول للمعلومات وفق متطلبات العمل فقط، ويتم تحديد الموافقات بناءً على دور كل شخص في العمل، ويكون لتطبيقات الأعمال في الجامعة الضوابط التالية:

(1) يمنح الدخول لخيارات القائمة المطلوبة وفق احتياجات المستخدم وكما هو محدد بوضوح في الوثائق الخاصة بكل تطبيق.

(2) يتم ضبط صلاحيات الدخول وفق احتياجات العمل وكما هو محدد بوضوح في الوثائق الخاصة بكل تطبيق.

(3) ينتج عن التطبيقات مخرجات محددة وفق الأدوار المدرجة في الوثائق الخاصة بكل تطبيق.

ب- **عزل النظم الحساسة**

قد تتطلب النظم الحساسة بيئة حاسوبية منفصلة، وقد تشير الحساسية إلى وجوب تشغيل نظام التطبيقات في حاسب منفصل أو وجوب مشاركة الموارد مع نظم تطبيقات موثوق بها. ويتم اتخاذ القرار بناء على كل حالة على حده وبإذن ومراقبة "قطاع تقنية المعلومات".

5. الاتصالات والحوسبة المتنقلة

يُسمح لأجهزة الحوسبة المتنقلة المعتمدة من الجامعة بأن تتصل بالشبكة، كما يجب أن تتوافق جميع هذه الأجهزة مع سياسات الحوسبة المتنقلة في الجامعة.