المملكة العربية السعودية
وزارة التعليم
جامعة طيبة

عمادة تقنية المعلومات

نظام إدارة أمن المعلومات

سياسة ضبط الدخول

التاريخ : ٢٠١٨/٧/١٧

الإصدار : ١,١

١. الإطار العام للسياسة

١٠,١ سياسة ضبط الدخول

١. يتم ضبط عملية الدخول للمعلومات بناء على متطلبات العمل، والمتطلبات الأمنية، وقواعد ضبط الدخول الخاصة بكل نظام من نظم امن المعلومات. وينبغي لهذه القواعد أن تراعي ما يلي :

أ) المتطلبات الأمنية لتطبيق / تطبيقات العمل.

ب) حظر كافة أشكال الدخول ما لم تصدر موافقة محددة على ذلك بموجب أحكام هذه السياسة.

٢. يمنح المقاولون أو الاستشاريون أو موظفو الطرف الثالث حق الدخول عبر بيئة تجريبية على معلومات العمل في جامعة طيبة بعد إبرام اتفاقية تعاقدية. على أن تتضمن هذه الاتفاقية ما يلي، وذلك على سبيل المثال لا الحصر :

أ) الأحكام والشروط الخاصة بالدخول المصرح به.

ب) المسئوليات الأمنية للمقاولين، والاستشاريين أو الموظفين التابعين للمورّد.

ج) موافقة المقاولين والاستشاريين أو موظفي الطرف الثالث على الالتزام بسياسات أمن المعلومات في جامعة طيبة.

[ISO/IEC ٢٧٠٠١: A.١١,١,١]

١٠,٢ تسجيل المستخدمين

١. تتولى عمادة تقنية المعلومات وضع إجراءات رسمية لضبط الدخول، بحيث تتضمن هذه الإجراءات خطوات واضحة حول طلب، وإنشاء، وتعديل، وتعليق وإلغاء حسابات المستخدمين.

٢. لا يتم التفويض بمنح صلاحيات دخول المستخدمين، والتعديلات على الصلاحيات الحالية للمستخدمين الحاليين، وإلغاء دخول المستخدمين، من قبل مالك الأنظمة الإلكترونية (عمادة تقنية المعلومات) ، مع مراعاة ما يلي:

أ) أقل الامتيازات (مبدأ :الحاجة إلى المعرفة")

ب) الفصل بين الواجبات.

ج) مستوى الدخول المطلوب.

٣. يُزود كل مستخدم ببيانات دخول توضح الصلاحيات الممنوحه له على الأنظمة، على أن تتطلب هذه البيانات ما لا يقل عن عامل واحد من عوامل المصادقة (مثل كلمة السر، رقم رمز المطابقة Token، أجهزة التعرف من خلال الخصائص الحيوية Biometric).

[ISO/IEC ٢٧٠٠١: A.١١,٢,١]

١٠,٣ إدارة الامتيازات

١. يجب العمل على تحديد وتوثيق كافة المستخدمين الذين يدخلون الأنظمة الإلكترونية التابعة لجامعة طيبة. ويتم متابعة وتسجيل إجراءات منح الصلاحية وفقا لما يلي:

أ) تاريخ منح الصلاحية.

ب) تحديد إجراءات الموافقة على منح الصلاحية.

ج) توفير وصف للامتيازات الممنوحة.

د) بيان الأسباب التي دعت إلى منح الصلاحية.

٢. الالتزام بمبدأ الفصل بين الواجبات، ومبدأ أقل الامتيازات عند منح صلاحية الدخول لأعضاء هيئة التدريس، والموظفين، والطلاب والمقاولين والاستشاريين في جامعة طيبة.

[ISO/IEC ٢٧٠٠١: A.١١,٢,٢]

١٠,٤ إدارة كلمات المرور الخاصة بالمستخدمين

١. يجب أن تطلب كافة نظم المعلومات في جامعة طيبة التحقق والمصادقة من خلال كلمات المرور قبل السماح للمستخدم بالدخول:

أ) أن لا يقل الحد الأدنى لطول كلمة المرور عن ١٢ حروفا.

ب) أن تتكون كلمة المرور مكونة من مزيج مما يلي :

- ما لا يقل عن حرف هجائي واحد كبير (Uppercase) [A-Z]
- ما لا يقل عن عدد واحد (٠-٩)

ج) لا يسمح بترك كلمة المرور خالية.

د) على المستخدمين تغيير كلمة المرور عند تسجيل الدخول لأول مرة إلى أي نظام.

هـ) يتم تعطيل حساب المستخدم بعد ٣ محاولات فاشلة لتسجيل الدخول.

و) ينبغي فرض عملية تغيير كلمة المرور (من قبل نظام التشغيل أو التطبيق) كل ١٨٠ يوما على الأقل. ويجب أن لا تكون كلمة المرور الجديدة مماثلة لأي من كلمات المرور الأربع القديمة (كلمات المرور السابقة).

٢. في حالة وجود أي شك بانكشاف كلمة المرور، يجب العمل فورا على تغيرها، وإبلاغ عمادة تقنية المعلومات بذلك.

٣. تتولى عمادة تقنية المعلومات تغيير كافة أسماء المستخدمين وكلمات المرور الافتراضية قبل بدء تشغيل نظام.

٤. يجب تعطيل بيانات الدخول الخاصة بالمستخدم كما يلي:

أ) **أعضاء هيئة التدريس والموظفين**: يجب، ومن خلال إجراءات براءة الذمة، تعطيل بيانات دخول المستخدم فور ترك العمل بجامعة طيبة بسبب إنهاء الخدمة. وينبغي أيقاف الحساب ذي العلاقة والبيانات الخاصة به من أي نظام فور صدور قرار إنهاء الخدمة.

ب) **الطلاب**: يجب تعطيل بيانات دخول المستخدم عند انتهاء صفته كطالب في السجلات. وينبغي إيقاف الحساب ذي العلاقة والبيانات الخاصة به من نظم المعلومات وحذفه بعد مرور شهر واحد على من تاريخ تعطيله.

٥. يجب أن تعمل عمادة تقنية المعلومات على إعادة ضبط كلمات مرور المستخدمين بعد التحقق رسميا من هوية المستخدم، بعد تعثر استعادة كلمة السر آلياً.

[ISO/IEC ٢٧٠٠١: A.١١,٢,٣]

١٠,٥ مراجعة صلاحيات دخول المستخدمين

١. تتولى عمادة تقنية المعلومات بالتعاون مع مالك الأنظمة الإلكترونية ومسئول أمن المعلومات مراجعة صلاحيات دخول المستخدمين كل ستة أشهر في العام.

٢. فور اكتشاف أي سوء تصرف في صلاحيات الدخول الممنوحة، تقوم عمادة تقنية المعلومات بتقييد هذه الصلاحيات.

[ISO/IEC ٢٧٠٠١: A.١١,٢,٤]

١٠,٦ التعامل مع كلمة المرور

١. يحظر على المستخدمين إدخال كلمات المرور في رسائل البريد الإلكتروني أو المراسلات الإلكترونية.
٢. يحظر على المستخدمين توزيع كلمات المرور الخاصة بهم على المستخدمين الآخرين، وبالتالي فإنهم يتحملون المسئولية الكاملة عن أية أنشطة وتحركات تتم عبر الأنظمة الإلكترونية من خلالها.
٣. يحظر على المستخدمين التقاط أو الحصول على كلمات المرور، مفاتيح فك التشفير، أو أية آلية أخرى من آليات التحكم بالدخول، من شأنها السماح بالدخول بدون تفويض.
٤. **يحظر** على المستخدمين القيام بما يلي :

أ) الكشف عن كلمة المرور عبر الهاتف لأي كان.

ب) الكشف عن كلمة المرور عبر البريد الإلكتروني.

ج) الكشف عن كلمة المرور للأخرين بما في ذلك إداريي عمادة تقنية المعلومات والرئيس في العمل.

د) التحدث عن كلمة المرور أمام الآخرين.

هـ) التلميح إلى صيغة كلمة المرور (مثال: اسم عائلتي)

و) الكشف عن كلمة المرور خلال الاستبيانات أو النماذج الأمنية.

ز) مشاركة كلمة المرور مع أعضاء العائلة.

ح) الكشف، أثناء الإجازة، عن كلمة المرور لأحد الزملاء في العمل.

ط) كتابة كلمة المرور على الورق.

[ISO/IEC ٢٧٠٠١: A.١١,٣,١]

١٠,٧ أجهزة المستخدمين المتروكة دون إشراف

١. يتعيّن على المستخدمين تفعيل شاشات التوقف المزودة بكلمات مرور بخصوص كافة الخوادم وأجهزة الحاسب الآلي للحيلولة دون عمليات الدخول غير المصرح بها. وينبغي إعداد المؤقّت لتشغيل شاشة التوقف بعد مرور ١٠ دقائق من عدم استخدام الجهاز أو إيقاف الجهاز عن العمل.
٢. على كافة المستخدمين، وعند الانتهاء من أداء أعمالهم، إنهاء كافة فترات الاتصال النشط بالشبكة (Active Sessions).
٣. على كافة المستخدمين إغلاق الأجهزة الخاصة بكل منهم قبل مغادرة المكتب.

[ISO/IEC ٢٧٠٠١: A.١١,٣,٢]

١٠,٨ إجراءات الدخول المحمي

١. ينبغي أن يعمل النظام على عرض ملاحظة عامة تدل على أنه يحظر الدخول إلى الحاسوب إلا من قبل المستخدمين الحاصلين على تفويض بذلك.
٢. يتعين أن تعمل إجراءات تسجيل الدخول الخاصة بأي نظام على عرض أقل قدر من المعلومات حول النظام والغرض من استخدامه.

٣. ينبغي للنظام أن يعمل على تقييد عدد مرات محاولات تسجيل الدخول الفاشلة المسموح بها مع مراعاة ما يلي :

أ) تسجيل المحاولات الفاشلة والناجحة على حد سواء.

ب) فرض فترة انتظار زمنية قبل السماح بمواصلة أو رفض محاولات الدخول دون توفر تفويض محدد.

ج) توجيه رسالة تحذير إلى وحدة التحكم (Console) الخاصة بالنظام، عند الوصول إلى الحد الأقصى من محاولات الدخول.

٤. على إداريي تقنية المعلومات (مثل: مسئول النظام، مسئول التطبيق، مسئول الشبكة) مراجعة كافة محاولات الدخول الفاشلة على أساس منتظم.

[ISO/IEC ٢٧٠٠١: A.١١,٥,١]

١٠,٩ التحقق من هوية المستخدم والمصادقة عليه

١. يتعين على النظام المصادقة على معلومات تسجيل الدخول بعد استكمال إدخال كافة البيانات. وفي حالة ظهور ما يدل على وقوع خطأ، ينبغي أن لا يعمل النظام على بيان أية جزئية من البيانات كانت خاطئة وأية جزئية كانت صحيحة.

٢. يتعين على عمادة تقنية المعلومات تخصيص هوية / مصادقة مُميزة لكافة المستخدمين قبل منحهم الدخول إلى النظام.

[ISO/IEC ٢٧٠٠١: A.١١,٥,٢] [ISO/IEC ٢٧٠٠١: A.١١,٥,٣]

١٠,١٠ استخدام أدوات النظام (Utilities)

١. يكون الدخول إلى برامج النظام محدودا ويخضع للسيطرة.

٢. يتوجب إزالة كافة أدوات النظام (System Utilities) والبرامج غير الضرورية

[ISO/IEC ٢٧٠٠١: A.١١,٥,٤]

٢. المصطلحات

فيما يلي المصطلحات والتعريفات التي وردت في سياق هذه السياسة.

المصطلح		التفاصيل
المساءلة	Accountability	مبدأ أمني يشير إلى القدرة على التعرف على الأفراد وتحميلهم المسئولية عن أفعالهم.
الأصل	Asset	المعلومات التي لها قيمة بالنسبة للمؤسسة مثل النماذج، الوسائط، الشبكات، الأجهزة، البرمجيات ونظم المعلومات.
مالك الأصل	Asset Owner	فرد أو مجموعة من الأفراد الذين فوضتهم الإدارة بتحمل مسئولية إدامة سرية، توافر، ودقة الأصل. وقد يتغير مالك الأصل على امتداد دورة حياة الأصل.
التدقيق	Audit	فحص الحقائق بغرض إعطاء رأي وقد يتضمن ذلك اختبار الدليل لدعم هذا الرأي.
سجلات التدقيق	Audit Logs	كافة سجلات الأحداث مثل الأمن، والتدقيق، والتطبيق، والدخول والشبكات عبر كافة نظم التشغيل، وأجهزة الشبكة، والتطبيقات وقواعد البيانات.
المصادقة	Authentication	التحقق من هوية مستخدم أو عملية.
التوافر	Availability	خاصية الوصول والاستخدام عند الطلب من قبل جهة مفوضة.
الضبط	Control	وسائل لإدارة المخاطر، بما في ذلك السياسات، والإجراءات، والإرشادات، وغيرها، والتي قد تكون ذات طبيعة إدارية، أو تقنية، أو قانونية.
التشفير	Cryptography	العلم الذي ينطوي على مبادئ، ووسائل وأساليب لتحويل البيانات بهدف إخفاء محتواها من المعلومات، والحيلولة دون اكتشافها وتعديلها، أو استخدامها دون تفويض.
إرشادات	Guideline	وصف يوضح ما الذي ينبغي القيام به وكيفية القيام به لتحقيق الأهداف التي نصت عليها السياسات.
الحادثة الأمنية	Incident	ينجم عن وجود نقطة ضعف أمنية وتهديد معاً حادثة أمنية. والحادثة الأمنية هي عبارة عن حدث أو سلسلة من أحداث أمن المعلومات غير المرغوب بها أو غير المتوقعة، تقترن باحتمال كبير بأن تتعرض العمليات للخطر، وتهدد أمن المعلومات.
تسهيلات معالجة أمن المعلومات	Information Processing Facilities	أي نظام لمعالجة المعلومات، أو خدمة أو بنية تحتية أو الموقع المادي الذي توجد به هذه التسهيلات. يمكن أن تكون التسهيلات إما نشاط أو مكان، ويمكن أن يكون ملموسا أو غير ملموس.

أمن المعلومات	Information Security	الحفاظ على سرية، ودقة، وتوفر المعلومات. وقد يتضمن خصائص أخرى كالأصالة، والمساءلة، وعدم الإنكار، والاعتمادية.
نظام معلومات	Information System	أداة أو نظم مترابطة داخليا أو نظم فرعية لأدوات تستخدم في شراء، وتخزين، وتعديل، وضبط، وعرض، وتحويل، وتغيير، وبث، أو استقبال البيانات، ويتضمن ذلك برامج الحاسب الآلي، والبرامج الثابتة والأجهزة.
الدقة	Integrity	خاصية حماية دقة واكتمال الأصل.
مبدأ أقل الامتيازات	Least Privilege Principle	مبدأ أمني يتطلب منح كل جهة في النظام مجموعة من الامتيازات تكون مقيدة تقيدا مشددا (أو أقل مستوى من السماح) لتنفيذ المهام المفوض بها. ومن شأن تطبيق هذا المبدأ أن يحد من وقوع الحوادث الأمنية، والأخطاء، أو الاستخدام غير المصرح به.
الرموز المشفرة المتنقلة	Mobile Code	برنامج يتم الحصول عليه من النظم البعيدة، وينتقل عبر الشبكة، ومن ثم يتم تحميله وتنفيذه على النظام المحلي دون تركيبه أو تنفيذه بصورة صريحة من قبل الجهة المتلقية.
مبدأ الحاجة إلى المعرفة	Need to Know Principle	مبدأ للخصوصية يقوم على حصر الدخول في الأفراد المفوضين والذين تقتضي طبيعة الواجبات الموكولة إليهم مثل هذا الدخول. ولا يسمح للأفراد بالدخول بفضل وضعهم الوظيفي، أو رتبهم أو مناصبهم. ويمكن تطبيق هذا المبدأ بطرقة مختلفة كالعمل على تطبيق فصل فعلي، وضبط الدخول إلى سجلات معينة، وإعداد قوائم بالأفراد الذين يمكنهم الدخول إلى بعض السجلات، أو تركيب ضوابط للدخول على نظم المعلومات.
السياسة	Policy	خطة عمل لتوجيه القرارات والإجراءات. وقد ينطبق هذا المصطلح على الحكومة، مؤسسات القطاع الخاص، والمجموعات، والأفراد. وتتضمن إجراءات السياسة تحديد البدائل المختلفة، كالبرامج أو أولويات الإنفاق، والاختيار من بينها على أساس مدى الأثر الذي تحدثه.
الخصوصية	Privacy	حق الفرد في الحصول على الحماية من الإفشاء غير المصرح به للمعلومات المتعلقة به والمتواجدة ضمن وثيقة.
الخطر	Risk	مزيج من احتمال وقوع الحدث والعواقب المترتبة على ذلك.
	Teleworking	العمل عن بُعد، العمل عبر الإنترنت، العمل الإلكتروني، أو العمل من المنزل أو في المنزل. عبارة عن ترتيبات عمل يتمتع الموظف خلالها بالمرونة فيما يتعلق بمكان وساعات العمل. حيث يتم استبدال عملية السفر اليومي لموقع العمل بوصلة إلكترونية للعمل عن بُعد.
تحليل الخطر	Risk Analysis	الاستخدام المنظم للمعلومات لتحديد الموارد وتقدير المخاطر.

طرف ثالث	Third Party	الشخص أو الجهة التي تعتبر مستقلة عن الأطراف ذات العلاقة المهتمة بالموضوع مدار الاهتمام.
تهديد	Threat	احتمال التسبب في حادثة غير مرغوب بها قد تؤدي إلى إلحاق الضرر بنظام كإفشاء المعلومات، إتلاف، أو إزالة، أو تعديل أو التشويش على المعلومات الحساسة، أو الأصول أو الخدمة، أو إصابة العناصر البشرية. وقد يكون التهديد مقصودا، عرضيا أو من أحد المصادر الطبيعية.
نقط ضعف أمنية	Vulnerability	نقطة ضعف في الإجراءات، والعمليات، أو الضوابط الأمنيّة بحيث تتاح إمكانية استغلالها من قبل التهديدات بهدف الدخول غير المصرح به إلى المعلومات أو التشويش على العمليات الحيوية.