
# جامعة الأمير سطام بن عبد العزيز

## وثائق نظام إدارة أمن المعلومات

## سياسة ضبط الدخول

في

## عمادة تقنية المعلومات والتعليم عن بعد

# جدول المحتويات

# 1. تفاصيل الوثيقة

## 1.1 البيانات الأساسية

| | |
|---|---|
| **المؤسسة** | جامعة الأمير سطام بن عبد العزيز<br>عمادة تقنية المعلومات والتعليم عن بعد |
| **العنوان** | سياسة ضبط الدخول |
| **جهة الإصدار** | فريق نظام إدارة أمن المعلومات |
| **تاريخ الإصدار** | 25 يونيو 2015 |
| **التصنيف الأمني** | ○ عام ⊙ داخلي ○ محظور ○ سري |
| **رقم النسخة** | الإصدار رقم 1 |
| **عدد الصفحات** | 12 |

## 1.2 تحرير الوثيقة

| النسخة | الاسم/ الإدارة | نوع النسخة | راجعها/ اعتمدها | التاريخ | ملاحظات |
|---|---|---|---|---|---|
| 0.1 | مأمون السعيد<br>(مستشار أمن معلومات) | مسوّدة | | 25 يونيو 2015 | |
| | | | | | |
| | | | | | |

# 2. التحكّم بالإصدارات

## 2.1 الموافقة على التغييرات

لا يجوز الاطلاع على هذه الوثيقة، أو طباعتها أو توزيعها إلا من قبل الموظفين المفوضين فقط. وينبغي مراجعة أية تغييرات عليها واعتمادها من قبل مدير نظام إدارة أمن المعلومات.

## 2.2 التوزيع

لا يجوز الاطلاع على هذه الوثيقة، أو طباعتها أو توزيعها إلا من قبل الموظفين المفوضين فقط. يجب العمل باستمرار على إدراج الجهات التي تحصل على نسخة من هذه الوثيقة ضمن الجدول المبين أدناه.

| رقم النسخة | المستلم/ الإدارة | التوقيع |
|---|---|---|
| .1 | عميد تقنية المعلومات والتعليم عن بعد | |
| .2 | مدير أدارة المشاريع | |
| .3 | رئيس قسم التطبيقات وقواعد البيانات | |
| .4 | مدير قسم مركز البيانات | |
| .5 | قسم أنظمة التشغيل والشبكات | |
| .6 | قسم خدمات تقنية المعلومات والدعم | |
| .7 | قسم أمن تقنية المعلومات | |

## 3. الأهداف

تهدف هذه السياسة إلى إدارة الدخول إلى النُظم (المنطقي) والدخول إلى المباني (المادي)، بحيث يقتصر على الأشخاص المفوضين والأجهزة المصرح بها داخل مباني (مثل مركز البيانات وغرف الخوادم) بعمادة تقنية المعلومات والتعليم عن بعد في جامعة الأمير سطام بن عبد العزيز.

فيما يلي أهداف مشروع إدارة نظام إدارة أمن المعلومات ومجهودات أمن المعلومات التي تقوم بها عمادة تقنية المعلومات والتعليم عن بعد.

- إرساء قواعد المسؤولية والمساءلة عن أمن المعلومات في العمادة.
- التأكّد من أن لدى موظفي عمادة تقنية المعلومات والتعليم عن بعد توعية سليمة واهتماماً بأمن أنظمة المعلومات؛ وتقدير كافٍ لمسؤولياتهم على صعيد أمن المعلومات.
- التأكّد من قدرة عمادة تقنية المعلومات والتعليم عن بعد على التعامل مع مخاطر أمن المعلومات وخفضها.
- التأكّد من قدرة عمادة تقنية المعلومات والتعليم عن بعد على مواصلة تقديم خدماتها الحيوية بأسلوب يتسم بالاحترافية والتنظيم ومراعاة الجوانب الأمنيّة.
- التأكّد من مواصلة امتثال عمادة تقنية المعلومات والتعليم عن بعد للقوانين واللوائح، والسياسات الداخلية بما في ذلك معيار الأيزو 27001:2013.
- التأكّد من تطبيق آليات التحكّم المطلوبة لحماية سرية وتكامل وتوافر الأصول المعلومات لعمادة تقنية المعلومات والتعليم عن بعد.

## 4. النطاق

تنطبق هذه السياسة على جميع عمليات ومهام تقنية المعلومات بعمادة تقنية المعلومات والتعليم عن بعد، وعلى جميع مستخدمي الأصول المعلوماتية بما في ذلك الموظفين الموقّتين والدائمين في العمادة، وأعضاء هيئة التدريس، والعملاء، والاستشاريين، والموردين، وشركاء العمل والموظفين التابعين للمقاولين؛ بغض النظر عن الموقع الجغرافي.

تشمل هذه السياسة على جميع الأنظمة والأصول المعلومات لتقنية المعلومات بعمادة تقنية المعلومات والتعليم عن بعد، سواء أكانت تُدار من قبل العمادة أو من قبل طرف ثالث، بما في ذلك، على سبيل المثال لا الحصر:

- أجهزة الخادم، ومحطات العمل وجميع معدات البنية التحتية للحاس الآلي.
- البنية التحتية للشبكة ومعداتها.
- برمجيات وتطبيقات تقنية المعلومات.
- المعلومات أو البيانات الإلكترونية المخزّنة في الملفات وقواعد البيانات والوثائق الورقية.
- جميع موظفي ومستخدمي تقنية المعلومات.

## 5. الاستثناءات

قد تنشأ حالات استثنائية أو طارئة تحول دون تطبيق جزء أو أجزاء من هذه السياسة. وفي مثل هذه الحالة، ينبغي تقديم طلب استثناء رسمي مشفوعاً بالمبررات، إلى مدير نظام إدارة أمن المعلومات، والذي يبادر بتقييم الطلب، والبحث في البدائل المجدية، واتخاذ القرار الملائم.

## 6. إنفاذ السياسة و الانتهاكات

يتعين على جميع الإدارات بعمادة تقنية المعلومات والتعليم عن بعد والموظفين والمقاولين والموردين والشركاء، الالتزام الثابت والمتواصل بقواعد وسياسات هذه السياسة.

وعلى رؤساء أقسام تقنية المعلومات بالعمادة تقنية المعلومات والتعليم عن بعد التأكّد من المراقبة الدائمة للالتزام به ضمن الأقسام التي تقع تحت مسؤوليتهم. يخضع الالتزام بالقواعد الواردة في هذه السياسة للمراجعة الدورية من قبل مدير نظام إدارة أمن المعلومات، ومن شأن عدم الالتزام بالإطار العام له أن يُسفر عن القيام بإجراءات تصحيحية قد تشمل تطبيق إجراءات انضباطية، على أن تكون هذه الإجراءات متوافقة مع درجة المخالفة، وقد تشمل على سبيل المثال لا الحصر:

- توجيه إنذار شفوي.
- إنهاء العقد.
- اتخاذ إجراءات قانونية.

## 7. مُلكية الوثيقة

يتولى مدير نظام إدارة أمن المعلومات مُلكيّة هذه الوثيقة، وينبغي الحصول على موافقته الصريحة على أية تغييرات أو تحديثات على هذه الوثيقة.

## 8. الأدوار ومجالات المسئولية

| الدور | مجال المسئوليات |
|---|---|
| مسئول أمن المعلومات | • تنسيق الاستجابة للانتهاكات التي أثرت بالفعل على سرية ودقة وتوافر معلومات العمل الحيوية، وكذلك الانتهاكات التي يشك في احتمال وقوعها.<br>• إدارة التدريب على أمن المعلومات وبرامج التوعية الأمنية بخصوص أعضاء هيئة التدريس والموظفين في الجامعة مع التنسيق مع إدارة شئون الموظفين. |
| عمادة تقنية المعلومات | • ضمان حماية نظم المعلومات/البنية التحتية وفقا للآليات التقنية التي حددها فريق تصميم النظام / التطبيق.<br>• تطبيق ضوابط ملائمة لحماية سرية ودقة وصحة المعلومات الحساسة.<br>• تطبيق ضوابط ملائمة لحماية نظم المعلومات.<br>• المراجعة المنتظمة لحقوق وامتيازات دخول المستخدمين بالتنسيق مع مسئول أمن المعلومات ومالك الأصل المعلوماتي. |
| مالك الأصل | • تحديد حقوق دخول مستخدمي المعلومات إلى الأصول المعلوماتية. |
| المستخدم / الموظف | • الالتزام بسياسات، وإرشادات وإجراءات أمن المعلومات المتعلقة بحماية المعلومات.<br>• إبلاغ عمادة تقنية المعلومات بالحوادث الأمنية الفعلية أو تلك التي تثير الشكوك. |

# 9. الإطار العام للسياسة التحكّم بالدخول

## 9.1 حاجة العمل إلى التحكّم بالدخول

- يجب أن يكون الدخول إلى المعلومات، والشبكة والخدمة محدداً ومنضبطاً وفقاً لمتطلبات العمل والأمن.
- لا ينبغي السماح بدخول المقاولين أو الاستشاريين أو الموظفين التابعين للموردين إلى الأصول المعلوماتية الحيوية في عمادة تقنية المعلومات والتعليم عن بعد، إلا بموجب اتفاقيات تعاقدية فقط.
- (مبدأ الحاجة إلى المعرفة أو الحاجة إلى العمل): ينبغي السماح للمستخدمين في عمادة تقنية المعلومات والتعليم عن بعد بالدخول فقط إلى أنظمة المعلومات التي يحتاجون إليها للقيام بمهامهم الوظيفية.

## 9.2 إدارة دخول المستخدمين

- تلتزم عملية إنشاء وإزالة حسابات المستخدمين بإجراءات رسمية معتمدة (إجراءات إدارة دخول المستخدمين).
- يُحظر منح حق الدخول إلى الأصول المعلوماتية بعمادة تقنية المعلومات والتعليم عن بعد قبل الحصول على جميع الموافقات المطلوبة.
- يتمتع مالكو الأصول بصلاحية منح أو إلغاء حقوق الدخول إلى الأصول الخاصة بهم بناء على متطلبات العمل.
- يُراجع مالكو الأصول حقوق الدخول إلى الأصول الخاصة بهم كل 6 شهور.
- يتعيّن أن يكون لحسابات المستخدمين من الموظفين المتعاقدين، والاستشاريين وجميع موظفي الأطراف الثالثة الأخرين تاريخ انتهاء تلقائي، وألا يتجاوز تاريخ إنجاز المشروع المتعاقد عليه.
- يجب أن يكون لدى كل مستخدم من مستخدمي أنظمة المعلومات هوية مستخدم (User ID).
- يجب تخزين جميع أسماء المستخدمين وكلمات المرور إلى أنظمة المعلومات على نحو آمن، وأن يتم تهيئة أنظمة عمادة تقنية المعلومات والتعليم عن بعد بحيث تطبق تلقائياً متطلبات كلمة المرور التالية:
  - التعقيد: استخدام الحروف والأرقام
  - أدنى طول لكلمة المرور: 8 حروف
  - تاريخ كلمة المرور: أخر خمس كلمات مرور
  - محاولات الدخول الفاشلة: ثلاثة (يتم تعطيل الحساب بعد ثلاثة محاولات فاشلة)
  - استخدام كلمة المرور المبدئية لمرة واحدة فقط
  - قيام النظام بإلزام المستخدم بتغيير كلمة المرور عند أول تسجل للدخول
  - أدنى مدة لصلاحية كلمة المرور: 30 يوماً.
  - أقصى مدة لصلاحية كلمة المرور: 90 يوماً.
- يتعيّن على المستخدمين الالتزام بالمتطلبات المبينة أعلاه حتى إن لم يتم إلزامهم بذلك من قبل النظام (سياسة النطاق).
- يجب أن تعمل أقسام تقنية المعلومات على تغيير جميع أسماء المستخدمين وكلمات المرور الافتراضية للنظام الجديد، قبل نقله إلى البيئة التشغيلية. يشمل ذلك جميع أنواع أنظمة تقنية المعلومات.

## 9.3 مسؤوليات المستخدم

- على المستخدمين التعامل مع كلمات المرور الخاص بهم على نحو آمن وعدم مشاركتها مع الآخرين.
- على المستخدمين الالتزام بمتطلبات أمن كلمات المرور المحددة.
- على المستخدمين الالتزام بسياسة المكتب الخالي من الأوراق والشاشة الخالية من البيانات.

## 9.4 التحكّم بالدخول إلى الأنظمة والتطبيقات

- يجب ألا تكشف إجراءات تسجيل الدخول إلى النظام إلا عن أدنى قدر من معلومات النظام.
- خلال إجراءات تسجيل الدخول، يجب ألا يعمل النظام على تقديم رسالة مساعدة قد تُسهل الأمر على المستخدمين غير الشرعيين.
- يجب أن يعمل النظام على تحديد عدد محاولات تسجيل الدخول الفاشلة المسموح بها.
- يجب أن يقتصر الدخول إلى أدوات النظام على المسؤولين الإداريين عن الأنظمة وموظفي الدعم.
- ينبغي تعمل التطبيقات الحساسة التي تنطوي على بيانات حساسة باستخدام نظام تشغيل مخصص، بحيث لا تتقاسم نفس جهاز الخادم مع العديد من الخدمات والتطبيقات.

# 10. الملاحق

## 10.1 المصطلحات والاختصارات

| المصطلح | Term | التعريف |
|---|---|---|
| **مساءلة** | **Accountability** | مبدأ أمني يدل على وجوب تحديد الأشخاص وتحميلهم مسؤولية تصرفاتهم. |
| **حقوق/ امتيازات الدخول** | **Access Rights / Privileges** | تحدد حقوق دخول (أو امتيازات الدخول) المستخدم إلى أصل معلوماتي الإجراءات التي يُسمح للمستخدم القيام بها عند الدخول إلى الأصل المعلوماتي. |
| **أصل** | **Asset** | الأصل كل ما له قيمة بالنسبة للمؤسسة. |
| **مالك الأصل** | **Asset Owner** | الشخص أو الجهة المفوّضة باتخاذ قرارات فيما يتعلق بالأصل. |
| **سجل التدقيق (ملفات الأنشطة)** | **Audit Logs (log files)** | الملف حيث يتم تسجيل الأحداث التي تجري في النظام. |
| **أصالة** | **Authenticity** | ضمان بان الطرف هو/هي بالفعل من هو الشخص المزعوم. |
| **توافر** | **Availability** | خاصية إتاحة الدخول والاستخدام عند الحاجة من قبل جهة مفوّضة. |
| **تحليل الآثار على العمل** | **Business Impact Analysis** | إحدى عمليات العمل حيث يتم التنبؤ بعواقب الخسارة المحتملة لسرية الأصل أو تكامله أو توافره. |
| **سرية** | **Confidentiality** | خاصية عدم توفير المعلومات أو إفشائها إلى أشخاص، او جهات أو عمليات غير مفوّضة. |
| **آلية تحكّم (احتياطات)** | **Control (measure)** | وسيلة لإدارة المخاطر، بما في ذلك السياسات، والإجراءات، والإرشادات ...إلخ، وتكون ذات طبيعة إدارية أو تقنية أو قانونية. |
| **إخفاء** | **Cryptography** | الإخفاء ضمن سياق هذا الكتيّب، هو النظام الكلي الذي يدعم ويدير تشفير وفك تشفير المعلومات. |
| **تشفير** | **Encryption** | تحويل النص القابل للقراءة إلى صيغة غير مقروءة. |
| **حادثة** | **Incident** | أي حدث (نشاط) تتوفر فيه القدرة على الإضرار بأمن أصل أو أكثر من أصول المؤسسة. |
| **تصنيف المعلومات** | **Information Classification** | عملية ترتيب المعلومات وفقاً لأهميتها بالنسبة للعمل. |
| **تسهيلات/مرافق معالجة المعلومات** | **Information Processing Facilities** | أي نظام أو خدمة أو بنية تحتية لمعالجة المعلومات، أو الموقع الذي يحتويها. |
| **أمن المعلومات** | **Information Security** | المحافظة على سرية وتكامل وتوافر المعلومات؛ كما يمكن أن تشترك في ذلك خصائص أخرى مثل الأصالة، المساءلة، عدم التنصّل، والموثوقية. |
| **تسجيل (تسجيل الأحداث)** | **Logging (Event Logging)** | توليد وتخزين معلومات محددة بخصوص أنشطة (أحداث) جرت على النظام. |
| **برنامج خبيث (رموز برمجية خبيثة)** | **Malware (malicious code)** | برنامج يُستخدم في التشويش على تشغيل الحاسب الآلي، وجمع معلومات حساسة، أو الحصول على دخول غير مصرح به إلى أنظمة الحاسب الالي. |
| **اختبار اختراق** | **Penetration Testing** | محاولة منضبطة لاختراق نظام الحاسب الالي، ومحاكاة الطرق والتقنيات التي ينفذها المخترق ذو النوايا السيئة، من أجل تحديد كيفية قيام المهاجم الحقيقي باختراق النظام؛ وما هو الضرر الذي يمكن أن يتسبب به. |

| | | |
|---|---|---|
| **المصطلح** | **Term** | **التعريف** |
| **سياسة** | **Policy** | خطة عمل لتوجيه القرارات والإجراءات. وقد ينطبق المصطلح على القطاع الحكومي، وعلى مؤسسات ومجموعات القطاع الخاص، والإفراد. تشمل السياسة تحديد البدائل المختلفة، مثل البرامج أو أولويات الإنفاق، والاختيار من بينها على أساس الأثر الذي قد تتركه. |
| **نقطة الاستعادة المستهدفة** | **Recovery Point Objective** | الحد الأقصى المقبول لخسارة البيانات، مقاساً بالوقت، في أعقاب وقوع كارثة. |
| **وقت الاستعادة المستهدف** | **Recovery Time Objective** | الحد الأقصى المرغوب للوقت والذي يسمح به بين الفشل غير المتوقّع أو كارثة، واستئناف المستويات الطبيعية للتشغيل أو الخدمة. |
| **خطر** | **Risk** | الخطر هو مزيج من احتمال وقوع حادث وعواقبه فيما لو وقع. |
| **الفصل بين الواجبات** | **Segregation of Duties** | آليات تحكّم أمنية وقائية تقتضي وجود أكثر من شخص لإنجاز عملية حيوية. |
| **طرف ثالث** | **Third Party** | ذلك الشخص أو الجهة الذي يُنظر إليه على أنه مستقل عن الأطراف المشاركة فيما يختص بالقضية مدار البحث. |
| **تهديد** | **Threat** | تهديد يتوفر فيه احتمال التسبب بحادثة غير مرغوب بها قد تسفر عن الإضرار بالنظام. |
| **نقطة ضعف أمنيّة** | **Vulnerability** | وهي عبارة عن ثغرة في أحد الأصول. |

## 10.2 الاختصارات

| الاختصار | المعنى الإنجليزي | المعنى بالعربي |
|---|---|---|
| BCP | Business Continuity Plan | خطة استمرارية الأعمال |
| BIA | Business Impact Analysis | تحليل التأثيرات على العمل |
| CCTV | Closed Circuit Television | دائرة تلفزيونية مغلقة |
| IPS | Intrusion Prevention System | نظام منع الاختراق |
| IRT | Incident Response Team | فريق الاستجابة للحوادث |
| ISO | International Standardization Organization | المنظّمة الدوليّة للمعايير |
| ISSC | Information Security Steering Committee | لجنة توجيه أمن المعلومات |
| ISMS | Information Security Management System | نظام إدارة أمن المعلومات |
| ITDL | IT and Distance Learning Deanship | عمادة تقنية المعلومات والتعليم عن بعد |
| RA | Risk Assessment | تقييم مخاطر |
| RPO | Recovery Point Objective | نقطة الاستعادة المستهدفة |
| RTO | Recovery Time Objective | زمن الاستعادة المستهدف |
| SAT | Security Awareness Training | التدريب على التوعية بأمن المعلومات |
| SLA | Service Level Agreement | اتفاقية مستوى خدمة |
| NDA | Non-Disclosure Agreement | اتفاقية المحافظة على المعلومات السرية |
| SoD | Segregation of Duties. | الفصل بين الواجبات |
| UPS | Uninterruptible Power Supply | مصدر للطاقة الاحتياطية |