جامعة الأمير سطام بن عبد العزيز

وثائق نظام إدارة أمن المعلومات

سياسة استخدام التقنية والمعلومات

في

عمادة تقنية المعلومات والتعليم عن بعد

جدول المحتويات

1. تفاصيل الوثيقة 3
   1.1 البيانات الأساسية 3
   1.2 تحرير الوثيقة 3
2. التحكّم بالإصدارات 4
   2.1 الموافقة على التغييرات 4
   2.2 التوزيع 4
3. الأهداف 5
4. النطاق 5
5. الاستثناءات 6
6. إنفاذ السياسة 6
7. مُلكية الوثيقة 6
8. الإطار العام للسياسة 7
   8.1 الاستخدام المقبول للأصول 7
   8.2 كلمة المرور 7
   8.3 أجهزة المستخدمين المتروكة دون إشراف 8
   8.4 سياسة المكتب الخالي من الأوراق والشاشة الخالية من المعلومات 8
   8.5 الحوسبة النقالة والاتصالات 8
   8.6 استخدام الأجهزة 9
   8.7 خدمة البريد الإلكتروني 9
   8.8 خدمة شبكة المعلومات العالمية (الإنترنت) 9
9. الملاحق 10
   9.1 المصطلحات والاختصارات 10
   9.2 الاختصارات 12

1. تفاصيل الوثيقة

1.1 البيانات الأساسية

المؤسسة	جامعة الأمير سطام بن عبد العزيز عمادة تقنية المعلومات والتعليم عن بعد
العنوان	سياسة استخدام التقنية والمعلومات
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 (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 ضبط استخدام كافة الأصول المعلوماتية (مثل: أجهزة، طابعات، برامج، معلومات) الخاصة 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

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. الإطار العام للسياسة

8.1 الاستخدام المقبول للأصول

- ينبغي على الموظف استخدام كافة الأصول المعلوماتية الخاصة بالجامعة لأغراض العمل فقط.
- على الموظف عدم الاشتراك في أي أنشطة غير قانونية كالدخول إلى الأصول غير المصرح بالدخول إليها، أو الاختراق، أو التسبب بإدخال ما يضر بالحواسيب أو إدخال الفيروسات، أو القيام بتصرفات من شأنها التسبب في تعطيل استخدام الأصول المعلوماتية.
- يقتصر استخدام وسائط التخزين والأجهزة الملحقة Peripheral (مثل ناسخات أقراص DVD، ومنافذ توصيل وسائط التخزين النقالة USB، ووسائط التخزين النقالة Flash وغيرها) على احتياجات العمل فقط.
- على الموظف عدم تمرير أو التصريح عن أي معلومات خاصة بالجامعة أو أي معلومات سرية لأي جهة غير مصرح لها.

8.2 كلمة المرور

- يجب على الموظف التقيد بسياسة كلمة المرور كما يلي:
  - ألا يقل الحد الأدنى لطول كلمة المرور عن 8 حروف، على 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 (0-9).
- لا يسمح بترك كلمة المرور خالية.
- تغيير كلمة المرور عند تسجيل الدخول لأول مرة إلى أي نظام.
- يتم تعطيل حساب المستخدم بعد 3 محاولات فاشلة لتسجيل الدخول.
- يتم تغيير كلمة المرور (من قبل نظام التشغيل أو التطبيق) كل 90 يوماً على الأقل. ويجب ألا تكون كلمة المرور الجديدة مماثلة لأي من كلمات المرور الأربع القديمة (كلمات المرور السابقة).
- تستخدم كلمة المرور المبدئية لمرة واحدة فقط.
- في حالة وجود أي شك بانكشاف كلمة المرور، يجب العمل فوراً على تغيرها، وإبلاغ عمادة تقنية المعلومات بذلك.
- يحظر على الموظف القيام بما يلي:
  - إدخال كلمة المرور في رسائل البريد الإلكتروني أو المراسلات الإلكترونية.
  - توزيع كلمة المرور الخاصة به على الموظفين الآخرين، وبالتالي فإنه يتحمل المسئولية الكاملة عن أي أنشطة لها صلة بحقوق الدخول الممنوحة له.
  - التقاط أو الحصول على كلمات المرور، مفاتيح فك التشفير، أو أي آلية أخرى من آليات التحكم بالدخول، من شأنها السماح بالدخول بدون تفويض.
  - الكشف عن كلمة المرور عبر الهاتف لأي كان.
  - الكشف عن كلمة المرور عبر البريد الإلكتروني.
  - الكشف عن كلمة المرور للآخرين بم في ذلك إداريي تقنية المعلومات والرئيس المباشر.
  - التحدث عن كلمة المرور أمام الآخرين.
  - التلميح إلى صيغة كلمة المرور (مثال: اسم عائلتي)
  - الكشف عن كلمة المرور خلال الاستبيانات أو النماذج الأمنية.

- مشاركة كلمة المرور مع أعضاء العائلة.
- الكشف، أثناء الإجازة، عن كلمة المرور لأحد الزملاء في العمل.
- كتابة كلمة المرور على الورق.

8.3 أجهزة المستخدمين المتروكة دون إشراف

- على الموظف، وعند الانتهاء من أداء عمله، إنهاء كافة فترات الاتصال النشط بالشبكة (Sessions Active).
- على الموظف إغلاق الجهاز الخاص به قبل مغادرة المكتب.

8.4 سياسة المكتب الخالي من الأوراق والشاشة الخالية من المعلومات

- على الموظف اتباع الإرشادات التالية وتطبيقها:
  - عند عدم استخدام الأوراق ووسائط الحاسوب، وخصوصاً بعد ساعات الدوام الرسمي، ينبغي حفظها في خزانات مناسبة ومقفلة و/أو أي نوع آخر من الأثاث الذي يوفر الحماية.
  - ينبغي حفظ الوثائق الحساسة أو الحيوية المرتبطة بالعمل في مكان بعيد ومقفل عند عدم الحاجة إليها (ويفضل أن يكون ذلك ضمن خزنة أو كابينة مقاومة للحريق)، أو عندما تخلو المكاتب من الموظفين.
  - يتعين عدم ترك الحواسيب الشخصية والطابعات في وضعية تسجيل الدخول (Logged on) في حالة تركها بدون إشراف، وينبغي حمايتها من خلال شاشة توقف مزودة بكلمة مرور.
  - يجب إقفال أجهزة تصوير الوثائق والفاكس (أو حمايتها من الدخول غير المصرح به بطريقة أو بأخرى) بعد ساعات الدوام الرسمي.
  - عند طباعة المعلومات السرية، يتوجب على الفور إزالة الوثائق ذات العلاقة من الطابعة.

8.5 الحوسبة النقالة والاتصالات

- عند التعامل مع الحواسيب النقالة (Laptop)، يجب على الموظف مراعاة الإرشادات التالية:
  - في حالات السفر والتنقل، يجب عدم ترك الأجهزة (والوسائط)، دون إشراف في الأماكن العامة.
  - عند استخدام الحواسيب النقالة، يجب عدم معالجة المعلومات الشخصية أو الحساسة في الأماكن العامة (كوسائل المواصلات العامة).
  - يجب عدم تخزين كلمات المرور، أو أي رموز للمصادقة على الدخول إلى نظم الجامعة على الأجهزة النقالة حيث يمكن أن تتعرض للسرقة، أو تسمح بالدخول بدون تصريح إلى الأصول المعلوماتية.
- في حالة فقدان أي جهاز متنقل يخص الجامعة يحتوي على بيانات حساسة، أو حصول أي انتهاك آخر للحماية، القيام فوراً بإبلاغ عمادة تقنية المعلومات.

8.6 استخدام الأجهزة

- يجب على الموظف استخدام أجهزة الحواسيب وفقاً لمعايير الأمان (عدم التغيير أو العبث المتعمد بأجزاء الجهاز وعدم إتلافه بسوء الاستخدام).
- لا يحق للموظف تحميل أي برامج على الجهاز مثل: الألعاب، برامج المحادثة، برامج التحكم عن بعد أو أي برامج أخرى غير معتمدة من عمادة تقنية المعلومات.

8.7 خدمة البريد الإلكتروني

- عند استقبال أي ملف عبر البريد الإلكتروني، يجب على الموظف إجراء فحص له عن طريق برنامج مكافح الفيروسات.
- يحظر على الموظف استخدام البريد الإلكتروني للأغراض التالية:
  - استخدام البريد الإلكتروني في أشياء لا تخص العمل أو لأغراض شخصية.
  - استخدام البريد الإلكتروني لأغراض دعائية أو ربحية.
  - إرسال أي مواد إباحية أو مخالفة للأنظمة المتبعة بها في المملكة العربية السعودية.
  - إرسال أي بريد إلكتروني يحتوي على سب أو شتم أو انتقاص لأي جهة أو شخص.
  - إرسال فيروسات بشكل متعمد.
  - الاشتراك في المجموعات البريدية التي ليس لها علاقة بالعمل.

8.8 خدمة شبكة المعلومات العالمية (الإنترنت)

- الموظف هو المسؤول عن جميع الأنشطة التي يقوم بها خلال استخدامه لخدمة شبكة الإنترنت.
- يحظر على الموظف استخدام شبكة الإنترنت للأغراض التالية:
  - استخدام شبكة الإنترنت في أشياء لا تخص العمل أو لأغراض شخصية.
  - تحميل برامج تجسس أو فحص الشبكة أو اختراق أو فيروسات أو برامج غير مرخصة أو غير معتمدة من عمادة تقنية المعلومات.
  - استخدام برامج المحادثة الفورية بدون الحصول على تصريح من عمادة تقنية المعلومات.

9. الملاحق

9.1 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.

9.2 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