جامعة الأمير سطام بن عبد العزيز

وثائق نظام إدارة أمن المعلومات

سياسة أمن الاتصالات

في

عمادة تقنية المعلومات والتعليم عن بعد

جدول المحتويات

1. تفاصيل الوثيقة

1.1 البيانات الأساسية

المؤسسة	جامعة الأمير سطام بن عبد العزيز عمادة تقنية المعلومات والتعليم عن بعد
العنوان	سياسة أمن الاتصالات
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	13

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 سياسة أمن الاتصالات إلى ضمان الالتزام بالتشغيل الصحيح والآمن لتسهيلات معالجة المعلومات لتقليص الخطر الناجم عن تعطل النظام، وحماية سرية ودقة وتوافر الأصول المعلوماتية لعمادة تقنية المعلومات والتعليم عن بعد في جامعة الأمير سطام بن عبد العزيز. كما تنطوي هذه السياسة على إرشادات وتوجيهات مقترحة ترمي إلى ضمان حماية تشغيل الشبكة وتبادل المعلومات في بيئة الجامعة.

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 والانتهاكات

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	• وضع وتحديد إجراءات مناسبة لتداول، ومعالجة، وتخزين وتعميم المعلومات. • تحديد الأدوار والمسئوليات الأمنيّة لكل اتفاقية من اتفاقيات مستوى الخدمة. • التدقيق على دخول الطرف الثالث من حيث الانتهاكات الأمنية، أو إساءة الاستخدام وتقييم الاحتياجات.
عمادة تقنية المعلومات	• المراقبة الأمنية للنظام/ التطبيق/ الشبكة. • تركيب البنية التحتية الحيوية لأمن المعلومات (مثل البنية التحتية لبرامج مكافحة الفيروس) • تصميم وتطبيق أمن الشبكة والنظام. • تطبيق ضوابط ملائمة لحماية سرية ودقة وصحة المعلومات الحساسة. • تنسيق الاستجابة للانتهاك الفعلية، أو التي يُشك بحدوثها، لسرية، أو دقة، أو توافر نظم المعلومات الحيوية. • التحقيق في انتهاكات الضوابط، وتطبيق ضوابط تعويضية إضافية عند الضرورة. • تطبيق ضوابط ملائمة لحماية وضبط معلومات نظم الأتمتة. • تطبيق التغييرات وتركب برامج إصلاح النظم (Patching) على النظم/ التطبيقات/ الشبكة وفقا لإجراءات إدارة التغيير وإجراءات إدارة برامج إصلاح النظم (Patch)
وحدة المشروع	• المشاركة في تحديد الأدوار والمسئوليات الأمنية المطلوبة لاتفاقيات مستوى الخد واتفاقيات تبادل المعلومات. • إدارة العلاقة مع الطرف الثالث.
مالك الأصل	• تحديد حقوق دخول مستخدمي المعلومات إلى الأصول المعلوماتية الموجودة على نظم المعلومات.
المستخدم / الموظف	• الالتزام بسياسات، وإرشادات وإجراءات أمن المعلومات المتعلقة بحماية المعلومات. • إبلاغ عمادة تقنية المعلومات بالحوادث الأمنية الفعلية أو تلك التي تثير الشكوك.

9. الإطار العام للسياسة أمن الاتصالات

9.1 إدارة ضوابط الشبكة

- تتولى عمادة تقنية المعلومات والتعليم عن بعد وضع وتطبيق تدابير احتياطية من أجل:
  أ. ضمان سرية ومصداقية المعلومات الحساسة التي يتم تبادلها عبر الشبكات العمومية.
  ب. حماية نظم السيطرة والأتمتة والتطبيقات المربوطة.
  ج. الحفاظ على توافر خدمات الشبكات والحاسبات الآلية المربوطة بها.

- يحظر على كافة أعضاء الهيئة التدريسية والموظفين، والطلاب في الجامعة والمقاولين والاستشاريين والزوار ربط أي جهاز (حاسب شخصي، حاسب نقال، جهاز شبكة، مودم، أو غير ذلك) بشبكة الجامعة دون الحصول على إذن أو موافقة من عمادة تقنية المعلومات والتعليم عن بعد طبقا للإجراءات المعتمدة.

9.2 حماية خدمات الشبكة

- تتولى عمادة تقنية المعلومات والتعليم عن بعد توفير الحماية كلا البنية التحتية لشبكة الجامعة من خلال تطبيق التدابير والخصائص الأمنيّة المناسبة للشبكات. ونورد من بين هذه الخصائص ما يلي، وذلك على سبيل المثال لا الحصر:
  أ. التقنية المستخدمة في توفير الأمن لخدمات الشبكة، كالمصادقة والتشفير وآليات التحكم بوصلات الشبكة.
  ب. الخصائص الفنية (Parameters) للشبكة والمطلوبة للربط الآمن مع خدمات الشبكة وفقا للقواعد الأمنيّة وقواعد الربط بالشبكة، ومنها الجدران النارية، الشبكة الخاصة الافتراضية (VPN)، ونظم كشف التسلل/ نظم منع التسلل.
  ج. إجراءات استخدام خدمات الشبكة لوضع القيود على الوصول إلى خدمات أو تطبيقات الشبكة، أينما كان هناك ضرورة للقيام بذلك.

9.3 تقسيم الشبكات

- يتعين تقسيم شبكة نظم معلومات الخاصة بالجامعة إلى قطاعات، ومناطق، ومجالات منطقية وفقاً للمعايير التالية، والتي نوردها على سبيل المثال لا الحصر:
  أ. متطلبات الدخول (مثل: الإدارة، هيئة التدريس، الموظفين، تقنية المعلومات، الطلاب).
  ب. تكلفة استخدام التقنية الملائمة، والآثار المترتبة على الأداء.
  ج. قيمة وتصنيف المعلومات المخزنة أو التي يتم معالجتها في الشبكة (الحرجة، والحساسة).
  د. مستوى الثقة (مثال: موثوق، إنترنت، المنطقة غير المؤمّنة DMZ).
  هـ. خطوط العمل (مثل: خدمات، دعم).
- يتعين فصل الشبكة الداخلية عن الشبكة الخارجية باستخدام ضوابط محيطية أمنية مختلفة خاصة بكل شبكة من الشبكات.

9.4 سياسات وإجراءات تبادل المعلومات

- يجب وضع ضوابط رسمية تعتمد على أهمية المعلومات، وذلك لحماية تبادل المعلومات عبر وسائل الاتصالات. كما يجب العمل على توفير حماية مناسبة لعمليات تبادل المعلومات السرية.
- على كافة المستخدمين إنشاء، وتخزين، وتعديل، ونسخ، وحذف، أو إتلاف البيانات (الإلكترونية أو المطبوعة) بشكل يتوافق مع سياسات الجامعة، ويؤدي إلى ضبط، وحماية سرية، ومصداقية وتوافر مثل هذه البيانات.
- يتعين على مالكي المعلومات ضمان استخدام واتباع آليات ملائمة لحماية عملية تبادل المعلومات الخاصة بهم.
- يجب وضع وإدامة سياسات وإجراءات ومعايير رسمية تكفل حماية الوسائط المادية أثناء نقلها إلى خارج مباني الجامعة، من الدخول غير المصرح به أو إساءة الاستخدام أو تعرضها للتلف.

9.5 اتفاقيات تبادل المعلومات

- قبيل تبادل الأصول المعلوماتية مع أطراف خارجية، يجب أن يتم التوصل مع هذه الأطراف إلى اتفاقية مستوى خدمة رسمية تنطوي على ضوابط أمنية كافية. وتتضمن هذه الاتفاقية ما يلي وذلك على سبيل المثال لا الحصر:
  أ. مسئوليات الإدارة
  ب. التبادل اليدوي والإلكتروني
  ج. حساسية معلومات العمل التي يجري تبادلها
  د. متطلبات الحماية
  هـ. متطلبات الإبلاغ
  و. معايير التجميع والإرسال
  ز. تحديد الجهة الناقلة
  ح. المسئوليات والالتزامات
  ط. مُلكية البيانات والبرامج
  ي. مسئوليات وتدابير الحماية
  ك. متطلبات التشفير

9.6 تبادل الرسائل الإلكترونية

- يجب وضع ضوابط لحماية عمليات تبادل الرسائل الإلكترونية من الدخول غير المصرح به، أو التعديل أو حجب الخدمة.

9.7 اتفاقيات الحفاظ على السرية

- يجب العمل على تحديد المتطلبات المتعلقة بالتزامات السرية أو عدم الإفشاء (تلك المتعلقة بأعضاء هيئة التدريس وموظفي الجامعة وأي طرف ثالث) ومراجعتها بانتظام. ومن هنا فإنه يتعين على عمادة تقنية المعلومات والتعليم عن بعد بالتعاون مع شؤون الموظفين وإدارة الخدمات القانونية القيام بما يلي:
  أ. تحديد المعلومات التي ستتم حمايتها ومستوى السرية المطلوب.
  ب. بيان المدة الزمنية المتوقعة للالتزام.
  ج. تحديد شروط إعادة أو إتلاف المعلومات بعد انتهاء الالتزام.
  د. تحديد المسئوليات والمتطلبات المتعلقة بالمفوضين بالتوقيع بغية الحيلولة دون نشر المعلومات دون تفويض.
  هـ. نشر العقوبات التي ستطبق في حالة عدم احترام المستخدم للالتزام.

- يجب على اتفاقيات السرية أو عدم الإفشاء، أن تتضمن شروطا قانونية قابلة للتطبيق لتلبية متطلبات حماية الأصول المعلوماتية في الجامعة.

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