هيكل السياسة

١. الهدف

تهدف هذه السياسة إلى حماية سرية وسلامة وتوافر الأصول المعلوماتية الخاصة بجامعة الملك عبد العزيز، والتي يتم بثها عبر شبكات الاتصالات، وضمان التشغيل الصحيح لهذه الأصول، تلتزم الجامعة بنشر كافة ضوابط الاتصالات/ الشبكات والتشغيل الضرورية.

٢. النطاق

تنطبق هذه السياسة على جامعة الملك عبد العزيز، وعلى كافة الأطراف المعنية بما في ذلك الشركاء، أو الشركات التابعة لها، وعلى نظم معالجة البيانات ونظم ضبط العمليات التي تحتوي على، أو تستخدم معلومات و/أو تسهيلات تعود ملكيتها للجامعة.

وتسري هذه السياسة على كافة الموظفين/ المستخدمين الذين يعملون بصورة مباشرة أو غيرة مباشرة لدى الجامعة، أو الجهات التابعة لها أو أية جهة تقوم بتنفيذ عمل نيابة عن الجامعة يتضمن استخدام الأصول المعلوماتية التابعة لها.

٣. الدور والمسئوليات

بناء على الهيكل التنظيمي للجامعة ، نورد فيما يلي قائمة بالأدوار والمسئوليات المرتبطة بهذه السياسة:

١. دور الإدارة

- دعم تنفيذ سياسات الحماية في بيئة الجامعة لحماية الأصول المعلوماتية والبرامج الحيوية للعمل .
- ضمان توافق سياسات الحماية مع المتطلبات القانونية والتعاقدية للجامعة.
- الموافقة على استخدام كافة نظم المعلومات المستخدمة في معالجة وتخزين أو طباعة المعلومات الحساسة.
- الموافقة على السياسات الجديدة أو على التعديلات التي تتم على السياسات الحالية.

٢. دور عمادة تقنية المعلومات

- توزيع وثائق حماية المعلومات، بحيث تحصل الجهات التي تحتاج إليها على نسخ منها، أو تمكينها من الحصول عليها عبر موقع على الشبكة الداخلية.
- ضمان حماية نظم المعلومات/ البنية التحتية وفقا للآليات التقنية التي حددها فريق تصميم النظم/ التطبيقات.
- مراقبة حماية النظم/ التطبيقات/ الشبكة.

٣. دور إدارة أمن المعلومات

- تحديد وإدامة سياسات حماية المعلومات.
- إعداد كتيبات حماية المعلومات اللازمة لتعزيز مستوى حماية المعلومات في الجامعة ، وتحديث هذه الكتيبات بشكل دوري .
- تطبيق الضوابط الملائمة لحماية سرية وسلامة وأصالة المعلومات الحساسة.

٤. دور المستخدم

- الالتزام بسياسات الحماية وإرشادات وإجراءات حماية البيانات الحساسة.
- إبلاغ مدير أمن المعلومات عن نقاط الضعف التي تؤثر بالفعل، أو هناك شكوك بأنها قد تؤثر على سرية وسلامة وتوافر البيانات والمعلومات الحساسة.
- استخدام وتوظيف المعلومات في الأغراض التي تنسجم مع أهداف الجامعة.

٥. دور الإدارة القانونية

- ضمان توافق سياسات حماية المعلومات مع المتطلبات القانونية والتعاقدية الحالية.
- تقديم المشورة القانونية الوافية التي تحتاج إليها الإدارات الأخرى لتقديم خدماتها بما يتوافق تماما مع القوانين والتشريعات السارية.
- اتخاذ الإجراءات اللازمة فيما يتعلق بمقاضاة المشتبه بهم.

٤. الالتزام

يعتبر التقيُّد بهذه الوثيقة إلزامي، وعلى كافة القطاعات – الإدارات – المكلفين بجامعة الملك عبد العزيز متابعة مدى الالتزام بها ضمن أقسامهم. ويكون الالتزام بنص السياسة العامة خاضعا للمراجعة الدورية من قبل مدير أمن المعلومات ، وسوف يتمخض أي انتهاك لهذه السياسة عن قيام لجنة أمن المعلومات بعمادة تقنية المعلومات بالتنسيق مع الجهات المعنية بالجامعة أو الجهات الأمنية ذات الاختصاص باتخاذ إجراءات تصحيحية. ويكون مستوى الإجراءات التأديبية المطبقة متلائما مع مستوى الانتهاك الذي تحدده التحقيقات. وتتضمن هذه الإجراءات، على سبيل المثال، لا الحصر:

- حجب امتيازات الدخول إلى الأصول المعلوماتية.
- جزاءات قد تكون مالية أو إنهاء عقد خدمة الموظف، أو تنزيل مستواه الوظيفي إلى المستوى الذي تراه الإدارة والموارد البشرية والقسم القانوني مناسبا.

٥. معايير الاستثناء

تهدف هذا السياسة إلى معالجة موضوع متطلبات حماية المعلومات. وعند الحاجة، يمكن التقدم بطلبات الحصول على استثناءات، بصورة رسمية، إلى إدارة أمن المعلومات، مع توضيح مسوغات الاستثناء، والمزايا التي قد تنجم عنه. على أن يتم الموافقة عليها من لجنة امن المعلومات بعمادة تقنية المعلومات.

تمتد فترة الاستثناء من السياسة، لمدة عام واحد كحد أقصى، ومن الممكن أن تتم إعادة مراجعته واعتماده مرة أخرى. وعند الضرورة يتم الموافقة على منح الاستثناء لثلاث فترات متعاقبة كحد أقصى. على أن لا يتم منح استثناء بشأن أي سياسة لمدة تزيد عن ٣ فترات متعاقبة.

٦. السياسات ذات العلاقة

- سياسة الالتزام
- سياسة ضبط الدخول
- سياسة إدارة الأصول
- سياسة التعامل مع الحوادث الحماية

٧. المالك

- مدير إدارة أمن المعلومات

٨. محور السياسة

تعتبر إدارة الاتصالات والعمليات من الوظائف الهامة والتي تؤثر بشكل ملحوظ على حماية المعلومات. ونظرا لمستويات الدخول الواسعة إلى نظم المعلومات على هذا المستوى، فإنه لا بد من توفر إجراءات تشغيل موثّقة ومفصلة، بما في ذلك تحقيق مستوى ملائم من الفصل بين الواجبات (الصلاحيات).

ينبغي توفير الحماية لكافة معدات وأجهزة الاتصالات، بما في ذلك نظم الحاسوب وأجهزة الشبكة التابعة لجامعة الملك عبد العزيز، بهدف الحفاظ على سرية، وسلامة وتوافر كافة تسهيلات معالجة المعلومات.

١. إجراءات التشغيل

الهدف من السياسة	محور السياسة
ضمان التشغيل الصحيح والآمن لتسهيلات معالجة المعلومات **[A.10.1]**	➢ تلتزم الجامعة بوضع وتطوير عمليات، وإجراءات وإرشادات ومعايير بناء على متطلبات التشغيل. ➢ على جامعة الملك عبد العزيز تطوير تدابير تقنية وتقنيات ملائمة لحماية سرية وسلامة المعلومات والنظم الحساسة في الجامعة عند الربط مع الشبكات غير الموثوقة. ➢ عند تنفيذ أية تغييرات ضرورية على الأصول التي تخص الجامعة، يتوجب الالتزام بإجراءات إدارة التغيير الموثقة المعمول بها في الجامعة. ➢ ينبغي القيام باختبار أي تغيير مهما كان نوعه وتنفيذه في بيئة الاختبار قبل التفويض بتطبيقه في بيئة الإنتاج. ➢ عند تطبيق أو نقل البرامج المطورة حديثا أو تلك التي تم تحديثها، من بيئة التطوير إلى بيئة الإنتاج، يجب الالتزام بإجراءات تكون موثقة توثيقا جيدا ومُعدّة خصيصا لها الغرض. ➢ يجب تطبيق مبدأ الفصل بين الواجبات الوظيفية في الجامعة حيثما أمكن ذلك، وذلك للحد من إساءة استخدام النظم بسبب الإهمال أو عن قصد. ➢ في حالة عدم انطباق مبدأ الفصل بين الواجبات، يتوجب استخدام ضوابط أخرى بدلا عن ذلك، كأن يتم مراقبة الأنشطة والصيانة ومراجعة أنشطة التعديل على النظم. ➢ يجب عدم استخدام البيانات الفعلية (البيانات الحقيقية) لتنفيذ الاختبارات سواء في بيئة الإنتاج أو الاختبار. ➢ تتولى الجامعة تطوير وإعداد إجراءات مناسبة موثقة لأنشطة النظام ذات الصلة بمعالجة المعلومات وتسهيلات الاتصالات.

٢. إدارة تسليم خدمات الطرف الثالث

الهدف من السياسة	محور السياسة
تطبيق وتوفير المستويات الملائمة من حماية المعلومات وتسليم الخدمات بما يتماشى مع اتفاقيات تسليم خدمات الطرف الثالث **[A.10.2]**	➢ ينبغي عدم تمكين أي طرف ثالث من الدخول إلا إلى المرافق والبيانات اللازمة لتنفيذ مهام محددة ومتفق عليها ➢ عدم تمكين أي طرف ثالث من الدخول، إلا بعد قيامه بتوقيع اتفاقية عدم الإفشاء. هذا وينبغي لاتفاقية عدم الإفشاء الموقعة بين الجامعة والطرف الثالث أن تتوافق مع سياسة الالتزام القانوني في الجامعة. ➢ على موظفي عمادة تقنية المعلومات تحديث قائمة المقاولين التي بحوزتهم، وكذلك الخدمات التي تقوم بها أطراف ثالثة (Outsourced) والجهات المستهدفة باتفاقيات مستوى الخدمة وتفاصيل الاتصال بهم. ➢ يجب أن تقوم العمادة بتكليف موظف معين أو فريق عمل من العمادة للقيام بمهمة إدارة العلاقات مع الطرف الثالث. ➢ على الجامعة توفير رقابة كلية كافية وتواجد في كافة الجوانب الأمنية فيما يتعلق بالمعلومات الحساسة أو الهامة، أو مرافق معالجة المعلومات التي يتم دخولها أو معالجتها أو إدارتها من قبل طرف ثالث. ➢ تتبع الجامعة إجراءات رسمية عند ربط الأصول المعلوماتية بطرف ثالث. ➢ تقوم الجامعة بعمليات تدقيق عشوائية لدخول الطرف الثالث بهدف اكتشاف أية انتهاكات للحماية أو إساءة استخدام، وتقييم الاحتياجات. ➢ تقوم الجامعة بانتظام بمراقبة ومراجعة الخدمات والتقارير والسجلات التي يوفرها الطرف الثالث. ➢ يجب على الطرف الثالث تصنيف أية وثائق يتم إنشاؤها من قبله وتتعلق بالمهمة التي يؤديها لدى الجامعة اعتمادا على أهمية الوثيقة ووفقا لسياسة تصنيف المعلومات الخاصة بالجامعة. ➢ يجب أن يكون لدى موظفي الطرف الثالث العاملين لدى الجامعة تفهما ووعيا بسياسة حماية المعلومات الخاصة بالجامعة.

٣. التخطيط للنظام

الهدف من السياسة	محور السياسة
تقليص مخاطر تعطل النظم **[A.10.3]**	➢ يتوجب على الجامعة مراعاة متطلبات أداء النظم الجديدة والسعة في مرحلة التخطيط والقبول. ➢ يجب على معايير القبول أن تتطرق إلى ضمانة المورّد بأن تركيب النظام الجديد لن يؤثر سلبا على النظم القائمة

الهدف من السياسة	محور السياسة
	➢ يجب على الجامعة تحديد متطلبات السعة لكافة الأنشطة الجديدة أو القائمة. ➢ ينبغي القيام بمراقبة وضبط استخدام المصادر والخروج بتوقعات بخصوص متطلبات السعة مستقبلا لضمان استمرارية أداء النظام حسبما هو مطلوب. ➢ تتولى الجامعة مسئولية التحقق من أن متطلبات ومعايير قبول النظم الجديدة محددة بشكل واضح ومعتمدة وموثقة وخضعت للاختبار. ➢ يجب عدم ترحيل النظم الجديدة، والتحديثات، والإصدارات الجديدة إلى بيئة الإنتاج إلا بعد الحصول على الموافقة الرسمية على ذلك. ➢ في حالة حدوث تطورات رئيسية، تقوم الجامعة أثناء عملية التطوير بالتشاور مع الجهة المسئولة عن التشغيل ومع المستخدمين، وذلك لضمان الفعالية التشغيلية للتطويرات المقترحة. وينبغي القيام باختبارات وعمليات تدقيق مناسبة للتأكد من تلبية كافة معايير القبول.

٤. ضوابط الحماية من الكودات الضارة والمتنقلة

الهدف من السياسة	محور السياسة
حماية سلامة البرامج والمعلومات **[A.10.4]**	➢ ينبغي أن تعمل الجامعة على تحديد وتطبيق آلية ملائمة لمنع واكتشاف البرامج الضارة ومعالجة النظم المتأثرة بصورة ملائمة، ودون أي تأخير. ➢ ينبغي تطبيق برنامج مركزي للحماية من الفيروسات على المستويات المختلفة في البنية التحتية للشبكة والنظام وذلك في سياق نهج متعدد الطبقات (Layard) للحد من دخول الكودات الضارة إلى بيئة الجامعة. ➢ ينبغي أن يعمل الخادم المركزي للحماية من الفيروسات تلقائيا على تحديث تواقيع الفيروسات من مزود الخدمة، وكذلك القيام بهذه المهمة عند توفر تحديث للتوقيع أو لمحرك الفيروس. ➢ يجب اتخاذ كافة التدابير الممكنة والعملية الكفيلة بتوفير الوقاية من إدخال البرامج الضارة إلى نظم المعلومات وشبكة الجامعة. ➢ ينبغي تهيئة برنامج الحماية من البرامج الضارة بحيث يقوم تلقائيا بمسح أمني لسواقات (drives) وسائط التخزين النقالة وذاكرة الفلاش عند ربطها. ➢ على الجامعة القيام بوضع وتطبيق إجراءات ملائمة للعمل بانتظام على جمع المعلومات، كالتسجيل في القوائم البريدية و/أو زيارة مواقع الويب التي توفر معلومات عن البرامج الضارة الجديدة. ➢ على الجامعة منع تركيب البرمجيات غير المصرح بها أو غير القانونية على أي نظام للمعلومات.

الهدف من السياسة	محور السياسة
	➢ على الجامعة توفير الحماية الفعالة ومنع المستخدمين من تغيير تهيئة أو إزالة أو تعطيل أو العبث بأي برنامج لمنع / اكتشاف البرامج الضارة قد يكون تم تركيبه على الأجهزة المستخدمة من قبلهم. ➢ على المستخدمين استيعاب مسئوليتهم فيما يتعلق بإبلاغ عمادة تقنية المعلومات عن أية مواضيع بخصوص أية كودات ضارة يشك في وجودها. ➢ ينبغي تفقد كافة الوسائط المتبادلة بين الدوائر والمؤسسات بحثا عن البرامج الضارة قبل استخدامها أو تبادلها. ➢ ينبغي تهيئة برنامج الحماية من البرامج الضارة بحيث يقوم تلقائيا بمسح أمني لكافة الحواسيب الشخصية، الخوادم، الحواسيب النقالة وأية مكونات أخرى من مكونات بنية النظم في الجامعة لاكتشاف الكودات الضارة المحتملة. ➢ يتولى إداري النظام مسئولية مراقبة برامج الحماية من الفيروسات بصورة منتظمة، وذلك لضمان التعامل دون تأخير مع الحوادث المتعلقة بالفيروسات.

٥. النسخ الاحتياطي للمعلومات

الهدف من السياسة	محور السياسة
المحافظة على سلامة وتوافر المعلومات وتسهيلات معالجة المعلومات **[A.10.5]**	➢ على إدارة أمن المعلومات، ومن خلال التعاون عن كثب مع مالكي النظم والبيانات والتنسيق معهم، تحديد متطلبات الحفظ الاحتياطي واستعادة البيانات لكافة نظم الجامعة وبما يراعي الجوانب القانونية والتنظيمية، وتوصيات الموردين والعوامل الأخرى ذات الصلة. ➢ يجب إجراء حفظ احتياطي، وفقا للإجراءات التي يوصي بها المورد/ المطبّق، لكافة برامج التطبيقات ونظم التشغيل، والبيانات (بما في ذلك قواعد البيانات)، ومعلومات التهيئة الخاصة بالمستخدم (أينما انطبق ذلك). ➢ يجب الحصول على التفويض المناسب للقيام باستعادة البيانات من النسخ الاحتياطية، وأن تتم عملية الاستعادة وفقا لإجراءات الحفظ الاحتياطي للبيانات واستعادتها. ➢ وجوب تفقد واختبار كافة نسخ الحفظ الاحتياطي على فترات منتظمة، وذلك لضمان سلامة وفعالية البيانات، وذلك من خلال القيام باستعادة بعض البيانات على أساس انتقائي. ➢ عنونة النسخ الاحتياطية وترقيمها تلقائيا حسب الأصول من قبل نظام الحفظ الاحتياطي أو يدويا من قبل الإداري الذي يقوم بعملية الحفظ. ➢ يجب استخدام جهة موثوقة عند نقل وسائط التخزين إلى مكان محدد "خارج

الهدف من السياسة	محور السياسة
	الموقع". وفي مثل هذه الحالة تقوم الجهة الناقلة بتوقيع اتفاقية عدم إفشاء مع الجامعة واستخدام مغلفات مختومة وموقعة. ➢ ينبغي توفير وتحديث سجلات الحفظ الاحتياطي. ➢ يجب مراجعة سجلات الحفظ الاحتياطي من قبل إداري النظام ذي العلاقة لضمان تنفيذ عملية الحفظ حسب الأصول. ➢ العمل على تشفير نسخ الحفظ الاحتياطي التي تتضمن معلومات حساسة، فيما لو كان ذلك ممكنا. ➢ يقوم إداري النظام باختيار وسائط حفظ احتياطي ملائمة بناء على أهمية وحيوية البيانات ومدة الحفظ. ➢ على إداري النظام تفهّم مسئوليته عن الإبلاغ عن أية أوضاع قد تؤدي إلى التأثير على سلامة البيانات المحفوظة أو على سريتها أو توافرها لأي سبب كان.

٦. إدارة حماية الشبكة

الهدف من السياسة	محور السياسة
ضمان حماية المعلومات في الشبكات وحماية البنية التحتية المساندة **[A.10.6]**	➢ على جامعة الملك عبد العزيز وضع وتطبيق تدابير احتياطية بخصوص : • حماية سرية وسلامة وتوافر البيانات التي يتم تمريرها عبر الشبكات العمومية أو الشبكات اللاسلكية. • حماية النظم والتطبيقات المربوطة • توافر خدمات الشبكة والحواسيب المربوطة. ➢ يجب الفصل بين مسئولية تشغيل الشبكة ومسئولية تشغيل الحواسيب، لتجنب حدوث تداخل. ➢ يجب تسجيل ومراقبة أنشطة الدخول والخروج إلى ومن الشبكة بهدف تسجيل أية أعمال تتعلق بالحماية. ➢ على الجامعة تطبيق تدابير وخصائص حماية ملائمة للشبكة لحماية البنية التحتية لتقنية المعلومات. ➢ يتم وضع اتفاقية خدمات الشبكة، بخصوص خدمات الشبكة التي يتم توفيرها داخليا أو من خلال أطراف ثالثة، على أن تتضمن خصائص الحماية ومتطلبات الإدارة ومستويات الخدمة.

٧. إدارة الوسائط

الهدف من السياسة	محور السياسة
الحيلولة دون الإفشاء غير المصرح به، أو التعديل، أو إزالة أو إتلاف الأصول أو تعطيل أنشطة العمل **[A.10.7]**	➢ على مالكي الأصول المعلوماتية التأكد من إدارة وضبط الوسائط وفقا للسياسات والإجراءات المعمول بها في الجامعة. ➢ يجب تخزين كافة الوسائط ضمن بيئة آمنة ومحمية وفقا للمواصفات التي توفرها الجهات الصانعة لهذه الوسائط. ➢ يجب تخزين المعلومات الموجودة على وسائط، والتي تحتاج إليها الجامعة لفترة زمنية تزيد عن فترة صلاحية وسائط التخزين (وفقا للمواصفات التي توفرها الجهة المصنعة) في مكان أخر للحد من فقدان المعلومات بسبب تدهور حالة وسائط التخزين. ➢ تحفظ المعلومات الشخصية على الوسائط النقالة فقط عندما تكون هناك حاجة ماسة لذلك، وينبغي أن تكون مشفرة. ➢ يجب تفعيل محركات الوسائط القابلة للنقل فقط في حالة وجود حاجة حقيقية لها تكون مرتبطة بالعمل. ➢ يجب تسجيل كافة الوسائط القابلة للنقل ضمن سجل يتم تحديثه لتقليص فرص فقدان البيانات. ➢ ينبغي أن يتم إعادة تهيئة الوسائط القابلة للنقل والتي يمكن إعادة الكتابة عليها، وذلك للحيلولة دون الكشف عن المعلومات عن غير قصد خلال عمليات تبادلها بين الموظفين أو الأطراف الأخرى. ➢ يجب التخلص بصورة ملائمة من كافة الوسائط وفقا لإجراءات تصنيف، وعنونة وتداول المعلومات، ومدة الاحتفاظ بها أو الانتهاء من استخدامها. ➢ يُحتفظ بسجل حديث بخصوص كافة وسائط التخزين التي تم التخلص منها وذل بهدف توفير إمكانية تعقب التعديلات عليها. ➢ على مالكي الأصول المعلوماتية التأكد من حماية الوسائط المادية أثناء النقل من خلال تطبيق الضوابط الملائمة. ➢ يجب أن تقوم كافة الأطراف بتسجيل وتعقب للوسائط المادية أثناء النقل حسب الأصول، وان تقوم الجهة المستلمة للوسائط بإبلاغ الجهة المرسلة عن استلام الوسائط المادية بحالة جيدة. ➢ يجب حماية الوسائط أثناء النقل من الدخول غير المصرح به أو إساءة الاستخدام أو التلف.

٨. إجراءات تبادل المعلومات

الهدف من السياسة	محور السياسة
توفير حماية المعلومات والبرامج التي يتم تبادلها في المؤسسة أو مع الجهات الخارجية **[A.10.8]**	➢ يتوجب على الجامعة حماية وضبط تبادل الأصول المعلوماتية والبرامج الحيوية، وذلك للحيلولة دون خسارة أو تعديل أو إتلاف أو إساءة استخدام المعلومات. ➢ على مالكي المعلومات ضمان توفر استخدام آليات ملائمة لحماية عملية تبادل المعلومات. ➢ يجب وضع اتفاقيات رسمية بخصوص تبادل الأصول المعلوماتية الخاصة بالتعاملات الهامة أو البرامج مع جهات خارجية. ➢ قبيل تبادل الأصول المعلوماتية مع أطراف خارجية يجب أن يتم التوصل إلى اتفاقيات رسمية بخصوص ذلك. ➢ يجب، وحيثما أمكن، تبني وتطبيق وسائل التشفير لحماية سرية، وسلامة وأصالة المعلومات ذات الطبيعة الحساسة. ➢ يجب عدم ترك المعلومات الحساسة أو الحيوية التي تخص الجامعة على أجهزة التصوير والطباعة أو الفاكس، نظرا لإمكانية الوصول إلى هذه الأجهزة من قبل موظفين غير مصرح لهم بذلك. ➢ يجب وضع وتوفير سياسات، وإجراءات ومعايير رسمية لحماية الوسائط أثناء النقل خارج مباني الجامعة من الدخول غير المصرح به أو إساءة الاستخدام أو التلف. ➢ استخدام نظام متفق عليه لعنونة المعلومات ذات الطبيعة الحساسة أو الحرجة، وبما يضمن فهم محتويات العنوان على الفور من قبل الموظفين، وحماية البيانات طبقا للأصول. ➢ استخدام نظام ملائم ومفهوم للعنونة في الجامعة. ➢ يجب وضع ضوابط لحماية تبادل الرسائل الإلكترونية من الدخول غير المصرح به، أو التعديل أو حجب الخدمة. ➢ قد يتواجد لدى الأطراف الثالثة، التي تتلقى منها الجامعة معلومات حساسة، السياسات الخاصة بها فيما يختص بتداول ومعالجة مثل هذه البيانات. وعلى المستخدمين ضمان الالتزام بالسياسات ذات العلاقة قبل تداول أو معالجة المعلومات التي تخص مثل هذه الأطراف. ➢ على كافة المستخدمين القيام بإنشاء وتخزين وتعديل ونسخ وحذف أو إتلاف البيانات (الإلكترونية أو المطبوعة) مع مراعاة سياسة الجامعة التي تعمل ضبط وتوفير الحماية لسرية وسلامة وتوافر هذه البيانات.

٩. خدمات التجارة الإلكترونية

الهدف من السياسة	محور السياسة
ضمان حماية خدمات واستخدام التجارية الإلكترونية [A.10.9]	➢ يتوجب حماية كافة البيانات المتعلقة بالتجارة الإلكترونية عبر الشبكات العمومية، من أي نزاع، أو أنشطة احتيالية، أو الإفشاء غير المصرح به أو التعديل. ➢ ينبغي حماية كافة المعلومات المتصلة بالتعاملات عبر الإنترنت من عمليات التوجيه الخاطئ، عمليات البث غير التامة، الكشف غير المصرح به، التعديل غير المصرح به للرسالة، أو عمليات النسخ أو إعادة التشغيل بدون تصريح. ➢ يتوجب حماية كافة النظم المتاحة للعموم من عمليات التعديل غير المصرح بها.

١٠. مراقبة أنشطة معالجة المعلومات

الهدف من السياسة	محور السياسة
الكشف عن أنشطة معالجة المعلومات التي تتم دون تصريح [A.10.10]	➢ يجب على إدارة أمن المعلومات، وبناء على درجة حساسية البيانات، ضمان تطبيق مستويات محددة وكافية من أنشطة تعقب التعديلات (Audit Trails)، وأن تكون مفعّلة في التطبيقات وقواعد البيانات. ➢ على إدارة أمن المعلومات التأكد من أن سجل أنشطة تعقب التعديلات الخاصة بإنشاء، وحذف وإلغاء حقوق الدخول إلى حساب المستخدم وحفظها لما لا يقل عن ٥ سنوات. ➢ على كافة خدمات تعاملات النظم تسجيل بيانات حساب المستخدم والتوقيع رقميا على مثل هذه السجلات بهدف الحيلولة دون إنكار المستخدمين للتعاملات التي نفذوها. ➢ على الجامعة التأكد من فعالية ضوابط أمن المعلومات المطبقة، وبأنه لا يتم تجاوزها. ➢ على الجامعة التأكد من أن السلوكيات غير الطبيعية واستغلال الثغرات التي يتم اكتشافها، تخضع للمراقبة والتسجيل. وحيثما أمكن يجب توفير خط حماية مرجعي (Baseline). ➢ على الجامعة التأكد من عدم السماح لكافة إداريي النظام بتعديل أو تعطيل السجلات الخاصة بالأنشطة التي يقومون بها. ➢ على الجامعة التأكد من تزامن تاريخ ووقت أنشطة تعقب التعديلات (Audit Trails) لمكونات الأنظمة المربوطة بالإنترنت لتسهيل تعقب هوية المستخدم

الهدف من السياسة	محور السياسة
	والأنشطة المباشرة (Online). ➢ لضمان دقة بيانات ملف أنشطة الحماية، ينبغي ضبط تزامن كافة ساعات الخوادم وأجهزة الشبكة . ➢ على الجامعة القيام بمراجعة أنشطة المراقبة على أساس المخاطر القائمة.

المصطلحات

الأصل	Asset	كل ما يمثل قيمة بالنسبة للمؤسسة.
التوافر	Availability	إمكانية الوصول والاستخدام من قبل جهة مفوضة.
السرية	Confidentiality	عدم إتاحة المعلومات أو إفشائها لأشخاص أو جهات أو عمليات ليس لديها تفويض.
الضبط	Control	وسائل لإدارة المخاطر، بما في ذلك السياسات، الإجراءات، الإرشادات، الممارسات أو الهياكل التنظيمية، والتي قد تكون ذات طبيعة إدارية، أو تقنية، أو قانونية. ***ملاحظة:*** *يستخدم الضبط أيضا كمرادف للحماية أو اتخاذ التدابير الاحتياطية.*
دليل الموظفين	Employee Hand Book	وثيقة تتضمن تعليمات ومعلومات يتوجب على الموظفين الالتزام بها، أو ينبغي لهم الرجوع إليها بهدف تلبية أحكام وشروط عملهم.
توجيهات	Guideline	وصف يوضح ما الذي يجب القيام به وكيفية القيام بذلك، وذلك بغية تحقيق الأهداف التي نصت عليها السياسات.
تسهيلات معالجة المعلومات	Information Processing Facilities	أي نظام لمعالجة المعلومات، أو خدمة أو بنية تحتية أو الموقع المادي الذي توجد به هذه التسهيلات.
حماية المعلومات	Information Security	الحفاظ على سرية، وسلامة، وتوفر المعلومات. وقد يتضمن خصائص أخرى الأصالة، المساءلة، عدم الإنكار، والاعتمادية.
الحادثة المتعلقة بالحماية	Information Security Event	حادثة ذات صلة بالحماية، هي واقعة محددة لنظام، خدمة أو شبكة، تشير إلى احتمال حدوث اختراق لسياسة حماية المعلومات أو الإخفاق في الحماية، أو أن تكون حالة غير معروفة من قبل قد يكون لها صلة بالحماية.
جهة تلقي بلاغات الحوادث المتعلقة بالحماية	IRC	وتتولى مسئولية تلقي وتسجيل كافة حوادث تقنية المعلومات التي يتم الإبلاغ عنها.
فريق الاستجابة لحوادث الحماية	IRT	مجموعة من العناصر البشرية المتأهبة والتي تستجيب لأية حادثة طارئة، مثل الكوارث الطبيعية أو انقطاع علميات العمل.
قائد فريق الاستجابة لحوادث حماية المعلومات	IRTL	**قائد فريق الاستجابة لحوادث حماية المعلومات**
نظام إدارة حماية المعلومات	ISMS	مجموعة من السياسات المتعلقة بإدارة حماية المعلومات

كود متنقل	Mobile Code	برنامج يتم الحصول عليه من نظام بعيد، وينقل عبر الشبكة، ومن ثم يتم تنزيله وتنفيذه على نظام محلي دون قيام الطرف المتلقي للبرنامج بتركيبه أو تنفيذه.
اتفاقية مستوى خدمة	Service-Level Agreement (SLA)	اتفاقية تم التفاوض بشأنها بين طرفين أحدهما العميل أما الطرف الثاني فهو مزود الخدمة.
السياسة	Policy	القصد الكلي والتوجه الذي تعبر الإدارة عنه رسميا.
الخطر	Risk	احتمالية حدوث واقعة مقرونة بالآثار المترتبة عن حدوثها.
تحليل المخاطر	Risk Analysis	الاستخدام المنظم للمعلومات بهدف التعرف على المصادر وتقدير حجم الخطر.
تقدير الخطر	Risk Assessment	العملية الكلية لتحليل الخطر وتقييمه.
تقييم الخطر	Risk Evaluation	عملية مقارنة الخطر الذي تم تقديره مقابل معايير محددة للمخاطر لتحديد أهمية الخطر.
إدارة المخاطر	Risk Management	أنشطة منسقة لتوجيه والتحكم بالمؤسسة فيما يتعلق بالخطر. ***ملاحظة:*** *إدارة المخاطر عادة ما تتضمن تقييم الخطر، معالجة الخطر، قبول الخطر، والإبلاغ عن الخطر.*
معالجة الخطر	Risk Treatment	عملية اختيار وتنفيذ تدابير للتخفيف من الخطر.
الطرف الثالث	Third Party	الشخص أو الجهة التي تعتبر مستقلة عن الأطراف ذات العلاقة المهتمة بالموضع مدار الاهتمام.
التهديد	Threat	سبب محتمل لحادثة غير مرغوب بها، وقد تؤدي إلى إلحاق الضرر بنظام أو بمؤسسة.
نقاط ضعف في الحماية	Vulnerability	نقطة ضعف في حماية احد الأصول أو مجموعة منها بحيث تتاح إمكانية استغلالها من قبل التهديدات.