هيكل السياسة

١. الهدف

تهدف هذه السياسة إلى مراعاة وتطبيق معايير حماية المعلومات خلال كامل دورة اقتناء، وتطوير وصيانة نظم المعلومات بجامعة الملك عبد العزيز (الجامعة).

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 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.

٢. 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. 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
- ضبط الدخول
- سياسة إدارة الأصول
- سياسة إدارة الاتصالات والعمليات

٧. المالك

- مدير إدارة أمن المعلومات

٨. محور السياسة

يجب مراعاة حماية المعلومات بجامعة الملك عبد العزيز ، خلال عملية تطوير أو/ و اقتناء النظم الجديدة.

١. تحليل ومواصفات متطلبات الحماية

الهدف من السياسة	محور السياسة
التأكد من أن الحماية تمثل جزء لا يتجزأ من نظم المعلومات **[A.12.1]**	➢ ينبغي تحليل متطلبات الحماية بخصوص نظم المعلومات الجديدة أو التحسينات على النظم الحالية، واستحداث الضوابط الضرورية عبر إتباع إجراءات رسمية. ➢ تتولى الجامعة ضمان أن كافة عمليات تطوير نظم المعلومات أو اقتنائها تتم وفقا للمتطلبات، والمعاير والإجراءات الموثقة. ➢ تتولى الجامعة ضمان تحديد وتوثيق وتطبيق ومراقبة ضوابط حماية مخصصة لمخاطر معينة بخصوص كافة النظم الحيوية التي تدعم العمل بالجامعة. ➢ تتولى إدارة تقنية المعلومات بدعم من إدارة أمن المعلومات، ومن مالك الأصل المعلوماتي، مسئولية تنفيذ الإجراءات المحددة. ➢ تقوم الجامعة بإجراء تقييم للتهديدات والمخاطر خلال مرحلة المتطلبات عند تطوير أو تطبيق إجراءات رئيسية أو اقتناء نظام حماية معلومات وذلك بهدف:

الهدف من السياسة	محور السياسة
	• تحديد متطلبات الحماية الضرورية لحماية نظم المعلومات. • تخصيص تصنيف حماية للمعلومات ولنظم المعلومات. ➢ تلتزم الجامعة بضمان توفر الضوابط الكافية للحد من مخاطر فقدان أو أخطاء أو إساءة استخدام المعلومات في نظم المعلومات. ➢ على الجامعة ضمان التوثيق الكافي لكافة خطة حماية النظام وبأنه يتم إدامة هذه الخطط بخصوص كل نظام من نظم المعلومات.

٢. معالجة التطبيقات

الهدف من السياسة	محور السياسة
الحيلولة دون حدوث الأخطاء في المعلومات أو فقدانها أو تعديلها بدون تفويض أو إساءة استخدامها في التطبيقات [A.12.2]	➢ يجب تطبيق عمليات تحقق ومصادقة ملائمة على التطبيقات ونظم قواعد البيانات للتأكد من صحة وسلامة مدخلات ومخرجات بيانات نظم المعلومات. وفي حالة البيانات الحساسة، ينبغي تطبيق ضوابط إضافية حسب الحاجة. ➢ يجب تصميم ضوابط المعالجة ضمن نظم التطبيقات وقواعد البيانات، وذلك للكشف عن عدم دقة المعلومات سواء أكان ذلك بسبب أخطاء المعالجة أو الأعمال المتعمدة. ➢ يجب تصميم ضوابط سلامة المعلومات (Integrity) ضمن التطبيقات، وذلك لضمان أصالة الرسالة، وحمايتها من التعديل في التطبيقات. ➢ يجب تصميم ضوابط المخرجات ضمن التطبيقات، للتحقق من صحة وسلامة معالجة البيانات المخزنة. ➢ تخضع عملية إجراء التغييرات على الوثائق والموارد الخاصة بالبيانات المدخلة لإجراءات التفويض. ➢ يجب تحديد وتوثيق مسئوليات كافة الموظفين القائمين على إجراءات إدخال وإخراج البيانات. ➢ عند استلام التطبيق لمعلومات نتيجة لتحميل الملفات، فلا بد من إجراء عمليات التحقق والمصادقة الضرورية للتحقق من ملاءمة نوع الملف وحجمه. ➢ يجب وضع آلية ومعايير لتسجيل الأعطال للتعامل مع الأعطال التي يتم الإبلاغ عنها. وينبغي العمل على مراقبة البيئة باستمرار بحثا عن أية أحداث سلبية.

٣. ضوابط التشفير

الهدف من السياسة	محور السياسة
حماية سرية وأصالة وسلامة المعلومات عبر استخدام وسائل التشفير [A.12.3]	➢ يجب تطبيق ضوابط التشفير حسب الحاجة على تطبيقات العمل الحيوية التي يتم الدخول إليها عبر الإنترنت، أو على أية نظم قد تتواجد عليها معلومات حساسة. ➢ يجب توفر حماية كافية للبيانات التي تبث عبر الإنترنت وذلك باستخدام تقنيات تشفير مناسبة. ➢ يجب تبنى أساليب آمنة لإدارة المفتاح (Key Management)، عند استخدام منهجيات التشفير في الجامعة.

الهدف من السياسة	محور السياسة
	➢ تتم عمليات الاستيراد والتصدير واستخدام منهجيات التشفير بما يتوافق مع القوانين والنظم ذات الصلة. ➢ يجب استخدام شهادات رقمية تعتمد على بنية المفتاح العام في حالة التطبيقات الهامة في الجامعة وذلك بناء على متطلبات العمل. ➢ يجب على المستخدمين توخي الحذر عند توقيع أو تشفير أو توقيع وتشفير الرسائل، وذلك اعتمادا على أهمية الرسائل في الجامعة.

٤. ضبط ملفات النظم

الهدف من السياسة	محور السياسة
ضمان حماية ملفات النظم [A.12.4]	➢ يجب تطبيق الإجراءات الكفيلة بضبط تركيب البرامج على النظم العاملة، والحد من مخاطر انقطاع خدمة المعلومات أو إلحاق الضرر بها. ➢ يجب تحصين حماية كافية لنظم المعلومات من خلال التهيئة الآمنة وبما يتماشى مع معايير أفضل الممارسات العالمية. ➢ يجب تطبيق ضوابط لنقاط الاتصال والربط (End-point) للحد من استخدام أجهزة النظم وملحقاتها. ➢ يكون إداريو النظم في الجامعة هم وحدهم المفوضون بالقيام بتحديث برامج التشغيل، والتطبيقات ومكتبات البرامج. ➢ يجب عدم تشغيل نظم المعلومات الموجودة في بيئة التطوير، في البيئة التشغيلية (الحية). ➢ تتولى الجامعة مسئولية ضمان توثيق وإدامة إجراءات التهيئة (Configuration) في الجامعة بشكل كاف. ➢ عند اتخاذ أي قرار بالتحديث إلى إصدار جديد، فإنه ينبغي أن يتم أخذ حاجة العمل إلى التغيير ومراعاة متطلبات الحماية. ➢ يحب توثيق إجراءات تشغيل النظم بوضوح، وإدامة سجل للأنشطة يبين بالتفصيل كافة أنواع الأنشطة. وينبغي العمل على مراقبة هذا السجل بصورة دورية بما يتوافق مع السياسات والإجراءات المعتمدة في الجامعة. ➢ تلتزم الجامعة بضمان تصنيف وضبط وإدامة كافة الرموز البرمجية (Source Code) بصورة مركزية. ➢ يجب ضبط وتوثيق عملية الدخول إلى الرموز البرمجية والتهيئة، واقتصارها على الموظفين المصرح لهم بذلك.

٥. حماية عمليات التطوير والدعم

الهدف من السياسة	محور السياسة
إدامة حماية برامج ومعلومات نظم التطبيق	➢ تلتزم الجامعة بضمان توثيق وتنفيذ إجراءات رسمية لضبط التغيير. ➢ يجب القيام باختبار كافة التغييرات أو البرامج الجديدة المركبة في بيئة مخصصة

الهدف من السياسة	محور السياسة
[A.12.5]	للاختبار. ➢ يجب عزل بيئة الإنتاج عن بيئة التطوير والاختبار. ➢ تلتزم الجامعة بضمان اختبار وتدوين وتحديث وإدامة كافة التغييرات على نظم المعلومات. ➢ يتم تنفيذ التغييرات في أوقات ملائمة، بحيث لا تؤثر سلبا على إجراءات العمل في الجامعة. ➢ يجب وضع كافة الضوابط الضرورية للحد من تسرب المعلومات من الأجهزة التي تقوم بمعالجة المعلومات الحساسة، بحيث تتوافق تدابير الحماية مع سياسة إدارة الأصول. ➢ يجب التخطيط لمتطلبات سعة النظام قبل إدخال تطبيقات عمل حساسة جديدة، وأن تتم مراجعتها عند التحديث. وينبغي اتخاذ تدابير احتياطية ملائمة لتجنب أية إشكالات تتعلق بتوافر التطبيقات أو النظم الحالية. ➢ يجب وضع معايير واضحة لقبول التحديثات على النظم أو الإصدارات الجديدة. ➢ يتم التخطيط لاختبارات القبول وتنفيذها وفقا للخطة. ➢ تكون العملية المستدامة لتوثيق إدارة التغيير وتحليل الآثار على العمل بخصوص التعديلات على التطبيقات، جزء لا يتجزأ من دورة تطوير النظام.

٦. إدارة نقاط الضعف الفنية في الحماية

الهدف من السياسة	محور السياسة
تقليص المخاطر الناجمة من استغلال نقاط الضعف الفنية **[A.12.6]**	➢ تتولى الجامعة القيام بإجراءات استباقية لتحديد وتقليص نقاط الضعف في بيئة التقنية الخاصة بها، قبل قيام جهة ما باستغلال هذه النقاط. ➢ تتولى إدارة أمن المعلومات مسئولية اتخاذ الخطوات الاحتياطية لتوفير الحماية للبنية التحتية في الجامعة. ➢ يجب اختبار برامج إصلاح النظم (Patches) الجديدة وتقييمها في بيئة الاختبار، وذلك قبل تركيبها على نظم الإنتاج. ➢ على الموظفين الذين يتولون مسئولية إدارة نقاط الضعف التأكد مما يلي : • استخدام أدوات المسح الأمني وفقا لأسس محددة في التعرف على نقاط ضعف الحماية التي يمكن أن يتم استغلالها من قبل أشخاص يقومون بعمليات مسح غير مصرح بها باستخدام نفس الأدوات. • يجب استخدام أدوات متعددة تعتمد على تقنيات مختلفة في تحديد أكبر قدر ممكن من نقاط الضعف. • يجب القيام بمسح للأصول المربوطة بكل من الشبكة الداخلية وبشبكة الإنترنت. • يجب إبلاغ مالك المعلومات بالآثار المحتملة لأنشطة المسح في البيئة المستهدفة وقبوله لها، وذلك قبل بدء المسح. • يجب العمل على مراقبة موارد الطرف الثالث فيما يتعلق بمعلومات نقاط الضعف الفنية (مثل التنبيهات الخاصة بالحماية، برامج إصلاح النظم

الهدف من السياسة	محور السياسة
	(Patches)، الحلول المؤقتة، وتحديثات برامج الحماية من الفيروسات لمعرفة مدى انطباقها على الجامعة. ومع الإبلاغ عن نقاط الضعف من قبل موارد الأطراف الثالثة هذه، فإنه يتوجب على الموظفين الذين يقومون بمسئوليات إدارة نقاط الضعف مقارنة كل نقطة من نقاط الضعف هذه بما لديهم من نقاط ضعف ، وذلك لمعرفة مدى أمكانية تعرض مصادر تقنية المعلومات لديهم لهذه النقاط. • عند قيام أحد الموردين بإصدار برنامج إصلاح لأحد ضوابط الحماية، فإنه ينبغي معاملة عملية إصدار برنامج الإصلاح على أنها إبلاغ ضمني عن وجود نقطة ضعف في الحماية، وبالتالي العمل على الحد من المخاطر التي قد تترتب عليها. • يتم تركيب برامج الإصلاح على كافة الأجهزة المربوطة بالشبكات الحكومية التي تحتوي على نظم تشغيل وتطبيقات يعرف عنها احتوائها على نقاط ضعف في الحماية، وذلك بهدف التعامل مع هذه النقاط. • في حالة عدم إمكانية تركيب برامج الإصلاح على جهاز مربوط بالشبكة، فإن يتم الحد من نقطة الضعف من خلال استخدام ضوابط حماية بديلة تكون مقبولة.

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.