هيكل السياسة

١. الهدف

تهدف هذه السياسة إلى تمكين إدارة تقنية المعلومات بجامعة الملك عبد العزيز (الجامعة) ، من إدارة مخاطر حماية المعلومات بهدف تحديد المناطق التي تعاني من نقاط ضعف في الحماية أو من تهديدات واتخاذ الإجراءات العلاجية المناسبة.

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.

٣. دور مالك الأصل المعلوماتي

- يتولى مسئولية توفير الحماية المناسبة، وإدارة وتداول الأصول المعلوماتية الحيوية التي تم تكليفه بملكيتها.
- تحديد حقوق دخول المستخدمين إلى الأصول المعلوماتية.

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 إدارة الأصول
- سياسة ضبط الدخول
- سياسة التخطيط لاستمرارية العمل
- سياسة حماية الموظفين

٧. المالك

- مدير إدارة أمن المعلومات

٨. محور السياسة

تتولى الجامعة وضع وتطبيق إدارة للمخاطر، وذلك بهدف ضمان توفر حماية بتكلفة معقولة، للأصول واستمرارية إجراءات العمل، على أن تتم إدارة المخاطر بخصوص كافة الأصول التي تخص الجامعة أو تتواجد بعهدتها. وبناء على النتائج التي تتمخض عنها عملية إدارة المخاطر، تتولى الجامعة تطوير تدابير حماية لتقليص و/أو الحد من آثار كافة المخاطر.

١. منهجية تقييم المخاطر

الهدف من السياسة	محور السياسة
تحديد وتحليل وتقييم المخاطر التي تواجه الجامعة	➢ تعمل منهجية المخاطر على أخذ العناصر التالية بعين الاعتبار: • تحديد الأصول، وتحديد أيها يعتبر أكثر حيوية. • تحديد وتقسيم وتقييم التهديدات. • تقييم مدى ضعف الأصول الحيوية في مواجهة بعض التهديدات. • تحديد الخطر (كان يتم تحديد الآثار المتوقعة لنوع معين من الهجمات على نوع معين من الأصول). • تحديد طرق تقليص هذه المخاطر. • ترتيب تدابير تقليص المخاطر وفقا للأولوية واعتمادا على إستراتيجية.

٢. توثيق إدارة المخاطر

الهدف من السياسة	محور السياسة
إدراك الفرصة المحتملة أثناء إدارة الآثار السلبية	➢ لكي يكون بوسع الجامعة إدارة أي خطر حسب الأصول فإنه لا بد من القيام بعمليات التوثيق الملائمة. ➢ يجب مراجعة واعتماد عملية إدارة الخطر والتوثيق من قبل مدير أمن المعلومات. ➢ يجب على مالكي الأصول، الاحتفاظ بسجلات للمخاطر التي تؤثر على المسئوليات التي يتولونها. وينبغي تمرير المعلومات التي تتضمنها هذه السجلات إلى مدير أمن المعلومات، والذي سيعمل بدوره على وضع وتوفير سجل الجامعة. ➢ تعتبر كافة الوثائق الخاصة بإدارة مستويات الخطر معلومات سرية، وتسلم إلى إدارة امن المعلومات والتي تحتفظ بهذه الوثائق لديها.

٣. تقييم المخاطر

الهدف من السياسة	محور السياسة
إجراء تقييم للمخاطر بخصوص كافة أصول الجامعة	➢ يجب القيام بعملية تقييم مخاطر على كامل البنية التحتية الموجودة أو الجديدة، وذلك وفقا لمنهجية إدارة المخاطر. ➢ يجب تضمين عملية تقييم المخاطر في التعاملات الجارية أو في العمليات التقنية. ➢ يتم إجراء عملية تقييم مخاطر للعقود الجديدة والحالية، وفي حالة إجراء أية تغييرات على هذه العقود. ➢ تحدد المخاطر على أساس التهديدات ونقاط الضعف الموجودة في الأصول الرئيسية للجامعة .

٤. تقليص المخاطر

الهدف من السياسة	محور السياسة
تقليص المخاطر من خلال تطبيق تدابر حماية معقولة من الناحية المالية	➢ ينبغي لإجراءات تقليص المخاطر مراعاة ما يلي: • اختيار التدابير الاحتياطية التي من شأنها الحد من مستوى التعرض للخطر. • تخصيص وترتيب يقوم على الأولوية فيما يتعلق بتطبيق تدابير الحماية. • تخصيص المسئوليات المالية والفنية لتطبيق وسائل الحماية. • تطبيق وسائل الحماية وتوثيقها.

٥. قبول الخطر والمخاطر المتبقية

الهدف من السياسة	محور السياسة
ضمان قبول الخطر من خلال إتباع إجراءات رسمية	➢ تقوم الجامعة بإتباع إجراءات رسمية بخصوص البت في قبول الخطر الموجود و/أو الخطر المتبقي، والإقرار ببقاء بعض المخاطر حتى في أعقاب تطبيق تدابير احتياطية معقولة من الناحية المالية. ➢ في حالة كون مستوى الخطر المتبقي غير مقبول، فإنه ينبغي تطبيق تدابير احتياطية إضافية للحد من مستويات التعرض للخطر إلى حدود مقبولة.

٦. التدريب على إدارة المخاطر والتوعية اللازمة

الهدف من السياسة	محور السياسة
ضمان أن كافة الأشخاص ذوي الصلة على دراية بإدارة المخاطر	➢ تقوم إدارة أمن المعلومات بإجراء تدريب على إدارة المخاطر والتوعية بها لضمان تفهم كافة موظفي عمادة تقنية المعلومات والكادر الوظيفي لضوابط ومتطلبات إدارة المخاطر، والعمل على تطبيقها.

٧. مراقبة ومراجعة إدارة المخاطر

الهدف من السياسة	محور السياسة
مراقبة تطبيق إدارة المخاطر	➢ يجب القيام سنويا بإجراء برامج تدقيق داخلي لمراقبة تطبيق هذه السياسة. وسيعمل التدقيق على تقييم: • ما إذا كانت هناك خططا لإدارة المخاطر بخصوص جزئية العمل التي يتم تدقيقها. • ما إذا كانت خطط العمل تتكامل بشكل مناسب مع وثائق التخطيط الأخرى، وأن هذه الخطط تتميز بالحداثة وتتم مراجعتها بانتظام. • يعمل التدقيق الداخلي، ومن خلال الإجراءات الاعتيادية المتعلقة بإعداد التقارير في أعقاب عمليات التدقيق، على رفع تقرير بخصوص مسائل إدارة المخاطر إلى الإدارة والجهات الأخرى ذات العلاقة.

٨. إعادة تقييم المخاطر

الهدف من السياسة	محور السياسة
تحديث إدارة المخاطر بالتغييرات الجديدة	➢ يجب إعادة تقييم المخاطر وتحديثها كما يلي: • كل عامين على الأقل اعتبار من تاريخ التقييم السابق. • بعد توصل التدقيق لنتائج هامة. • كلما تعرضت البنية التحتية لعمليات تحسين أو تعديل كبيرة. • في أعقاب وقوع حادثة تؤدي إلى انتهاك سياسة صريحة أو ضمنية للحماية ، وتعريض سلامة وتوافر وسرية الأصل للخطر.

٩. الإدارة المستقلة للمخاطر

الهدف من السياسة	محور السياسة
ضمان تقييم إدارة المخاطر من قبل طرف مستقل	➢ تجرى الإدارة المستقلة للمخاطر من قبل جهات منفصلة ليس لها صلة بالجهات التي تتولى مسئولية تطوير وتشغيل المعلومات. ➢ يجب إجراء العمليات المستقلة (مثل التقييم المستقل للمخاطر، المراجعة المستقلة للرموز البرمجية، المصادقة المستقلة على اختبارات الحماية، اختبار اختراق مستقل والمسح الأمني لنقاط الضعف) من قبل أفراد مستقلين،أو مقاولين أو موردين بهدف تطبيق معايير تقييم صارمة على المعلومات.

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.