هيكل السياسة

١. الهدف

تهدف هذه الوثيقة إلى وضع إطار للتعامل مع حوادث حماية المعلومات بفعالية ودون تأخير. وتعرّف حادثة حماية المعلومات بأنها انتهاك مشكوك به أو مؤكد، لسلامة وتوافر وسرية معلومات جامعة الملك عبد العزيز (الجامعة)، بما يتسبب أو يكون قد تسبب بالتأثير على أمن 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.

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

٧. المالك

- مدير إدارة أمن المعلومات

٨. محور السياسة

يجب مراعاة الجوانب المتعلقة بحماية أمن المعلومات على مدار فترة عملية تطوير أو/و اقتناء نظم المعلومات الجديدة في جامعة الملك عبد العزيز (الجامعة).

١. الإبلاغ عن الحوادث المرتبطة بحماية المعلومات

الهدف من السياسة	محور السياسة
ضمان الإبلاغ عن حوادث أمن المعلومات المرتبطة بنظم المعلومات بأسلوب يسمح باتخاذ إجراءات تصحيحية دون تأخير	➢ يتوجب إبلاغ الموظفين ذوي العلاقة عن كافة حوادث أمن المعلومات المؤكدة أو المحتملة، والذين سيعملون بدورهم على المساعدة في اتخاذ إجراءات تصحيحية. ➢ ينبغي العمل فورا على إبلاغ فريق التعامل مع حوادث أمن المعلومات بكافة الحوادث التي يشك بوجودها.

الهدف من السياسة	محور السياسة
[A.13.1]	➢ تتولى الجامعة تبنى إجراءات مناسبة تحدد خطوات التعامل مع أي حوادث تتعلق بأمن المعلومات. ➢ على كافة موظفي الجامعة إدراك مسئولياتهم فيما يتعلق بالإبلاغ عن أية أحداث ذات صلة بأمن المعلومات يكون لها آثار معروفة أو محتملة على أمن المعلومات.

٢. إدارة الحوادث المرتبطة بحماية المعلومات

الهدف من السياسة	محور السياسة
ضمان تطبيق نهج متجانس وفعّال على إدارة حماية المعلومات [A.13.2]	➢ تتولى إدارة أمن المعلومات مسئولية تطوير وتطبيق إجراءات للقيام بالأنشطة الروتينية للتحقق من الكشف عن الحوادث، والإبلاغ عن حوادث أمن المعلومات، وضبط الأضرار ومعالجتها، والحيلولة دون إلحاق أضرار مستقبلية بموارد الجامعة. ➢ على فريق الاستجابة لحوادث أمن المعلومات البت فيما إذا كان سيتم تصنيف الأحداث، كحوادث أمنية وتحديد أفضل الطرق للتعامل معها. ➢ ينبغي أن لا يسمح بدخول إلا الموظفين المحددين والمفوضين بدخول النظم المتأثرة خلال الحادثة، ويجب توثيق كافة الإجراءات العلاجية بحيث يتم توفير أكبر قدر من التفاصيل. ➢ يتم الإبلاغ عن أحداث أمن المعلومات إلى جهة اتصال مركزية ضمن فريق التعامل مع الحادثة في أقرب فرصة ممكنة، وإتباع إجراءات الاستجابة إلى الحوادث وتحويلها إلى الجهات العليا (تصعيدها). ➢ تعمل جهة الاتصال المركزية على تنسيق كافة جهود إدارة وحل الحوادث ذات الصلة. كما تقوم بتشكيل وقيادة "فريق الاستجابة للحادثة " والذي يتكون من موظفين آخرين من الجامعة لمواجهة واحتواء الأضرار الذي تسببت بها الحادثة ومعالجة هذه الحادثة. ➢ على جهة الاتصال المركزية، تسجيل الحادثة، وتخصيص سجل لها يمكن من خلاله تعقبها والرجوع إليها مستقبلا. ➢ تتولى جهة الاتصال المركزية مسئولية تعقب وضع الحادثة والمتابعة مع الأشخاص ذوي العلاقة والتعامل مع الاستفسارات المتعلقة بالتطورات على الحادثة. ➢ يمكن لجهة الاتصال المركزية إحالة الحادثة إلى مستويات أعلى في الجامعة، وذلك اعتمادا على مدى جدية الآثار المترتبة جراء هذه الحادثة. ➢ يجب علي جهة الاتصال المركزية، وبناء على البيانات التي وردت من الجهة التي أبلغت عن الحادثة، القيام بتحليل الحادثة، على أن تقوم بطلب معلومات إضافية من تلك الجهة فيما لو استدعى الأمر ذلك. ➢ يجب أن تكون إجراءات الإبلاغ سريعة وتنطوي على بدائل. ➢ يتم إدراج إجراءات إحالة المواضيع العالقة إلى مستويات أعلى (Escalation) ضمن عملية التعامل مع حوادث أمن المعلومات ، بحيث يكون المستخدمون وموظفو الدعم على دراية بالجهات الأخرى التي يمكنهم إبلاغها بالحادثة ، وذلك في حالة عدم تلقي رد من المجموعة خلال فترة زمنية محددة. ➢ يتوجب على إدارة أمن المعلومات، وبناء على البيانات المتوفرة ودرجة أهمية وحيوية الحادثة، إرسال تحذيرات بخصوص الحادثة، إلى الإدارات التي قد تتأثر

الهدف من السياسة	محور السياسة
	بمثل هذه الحوادث. ➢ في أعقاب التعافي التام من آثار الحادثة، ينبغي وضع آليات مراقبة إضافية لفترة محددة من الزمن، وذلك للتأكد من أنه قد تمت معالجة الحادثة بشكل كامل. ➢ تقوم الجامعة بإجراء تحقيق واف في جذور أسباب كل حادثة من حوادث انتهاك أمن المعلومات ، ويعمل على اتخاذ إجراءات مناسبة بهدف: • تحذير، تأديب، أو مقاضاة المسئولين عن الحادثة. • تحديث ضوابط الحماية الحالية أو استحداث ضوابط جديدة بهدف الحيلولة دون تكرار وقوع نفس الحادثة. • تحديث سجل حوادث الحماية لضمان دقة عملية الإبلاغ. ➢ على إدارة أمن المعلومات العمل بانتظام على مراجعة وتحديث خطط الاستجابة للحوادث. ➢ تقوم الجامعة بتبني آليات فعالة لقياس الحوادث وآثارها. وعلى إدارة أمن المعلومات، وبناء على المعلومات التي توفرت جراء وقوع الحادثة القيام بالتغييرات الضرورية (إذا ما استدعى الأمر ذلك) على سياسات الحماية، ورفع مستوى الضوابط أينما احتيج إلى ذلك، بهدف الحد من تكرار وقوع الحادثة، والأضرار الناجمة عنها، والتكلفة المترتبة على وقوعها. ➢ يقوم فريق الاستجابة للحوادث على تكييف وتعديل الخطة/الخطط السابقة للتوصل إلى خطة معالجة نهائية تخصص قدر الإمكان للحادثة المعينة، وذلك ضمن الإطار الزمني المتاح. ➢ تخضع إجراءات التعافي من حادثة انتهاك أمن المعلومات لضوابط رسمية. ➢ تقوم إدارة أمن المعلومات وإدارة تقنية المعلومات بوضع وتوثيق وإدامة قواعد لجمع وتقديم الأدلة المنصوص عليها ضمن الاختصاص ➢ فيما لو تطلبت إحدى الحوادث الحصول على بعض المعلومات لتسهيل سير التحقيق، فيجب عند ذلك الالتزام بالقواعد بدقة بالغة، والتعامل بحذر مع عملية جمع الأدلة للتحقيقات المحتملة. ➢ يجب الاتصال على الفور بإدارة أمن المعلومات وعمادة تقنية المعلومات للحصول على توجيهات وإجراء التحقيقات، وإتباع إجراءات صارمة في عند جمع الأدلة الجنائية. ➢ يجب تأمين وحفظ الأدلة المتعلقة بالحادثة حسب الأصول، حيث أنها تمثل دليلا على اكتشاف أي اختراق. ➢ تتولى الجامعة توفير برنامج وخطة موثقة للتعامل مع الحوادث بحيث تغطيان الأنواع الرئيسية من الحوادث. وينبغي إخضاع أية خطة للتعامل مع الحوادث للاختبار، لمعرفة مدى فعاليتها، وذلك بإتباع الوسائل المناسبة مثل التدريب الذي يعتمد على المحاكاة (Simulation). ➢ يجب على إدارة أمن المعلومات الاحتفاظ بسجل يوثق تاريخ الحادثة. ➢ تقوم إدارة أمن المعلومات بجمع معلومات ما بعد الحادثة.

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.