هيكل السياسة

١. الهدف

تهدف هذه السياسة إلى توفير إطار إداري لتنفيذ وضبط تطبيق أمن 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 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 إدارة الشؤون الإدارية

- تنفيذ عمليات تدقيق وفرز الموظفين.
- إصدار القوانين العامة الخاصة بالتوظيف.
- المساعدة في توعية المستخدمين وتدريبهم.
- التعاون مع، أو إبلاغ الأطراف ذات العلاقة، وذلك في حالة حدوث تغيير على واجبات الموظف، أو إنهاء عقد خدمته.
- عقد برامج تعريف لكافة الموظفين الجدد فيما يتعلق الهيكل التنظيمي والأدوار والمسئوليات.

٦. 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 المخاطر
- سياسة حماية المعلومات

٧. المالك

- مدير إدارة أمن المعلومات

٨. محور السياسة

في سبيل تطبيق ضوابط الحماية المناسبة، ينبغي تحديد المسئوليات والأدوار الخاصة بحماية المعلومات على نطاق جامعة الملك عبد العزيز (الجامعة).

هذا وتتوافق كافة الضوابط التي تم التطرق إليها في هذه السياسة مع أفضل الممارسات الدولية ومعيار الآيزو ٢٧٠٠١.

١. التنظيم الداخلي

الهدف من السياسة	محور السياسة
إدارة حماية المعلومات في المؤسسة **[A.6.1]**	➢ يتوجب على الإدارة تحديد أهداف وغايات حماية المعلومات في الجامعة. ➢ يتوجب على الإدارة تقديم التوجيه والدعم الواضح للمبادرات الخاصة بالحماية. ➢ تتولى الإدارة العمل على تحديد إطار واضح لإدارة حماية المعلومات، وكذلك الأدوار والمسئوليات والمؤهلات للموظفين الذين لهم صلة بالحماية، وإدارة الموارد وتطبيق الحماية. ➢ تقوم الإدارة بتطوير واعتماد سياسة حماية المعلومات، وضمان مراقبة عملية تطبيقها. ➢ يجب العمل على توفير التنسيق فيما بين الإدارات المختلفة بخصوص الأدوار المرتبطة بالحماية ووظائف العمل. ➢ يجب تحديد وتوثيق منهجيات تقييم المخاطر التي تغطي متطلبات واحتياجات العمل في الجامعة. ➢ يجب العمل على تحديد وتوثيق مسئوليات حماية المعلومات بوضوح، وذلك طبقا لوثيقة الهيكل التنظيمي لحماية المعلومات. ➢ يجب العمل على تحديد الأصول وإجراءات الحماية المرتبطة بكل نظام بصورة جيدة. ➢ يجب أن تعمل الجامعة على تحديد إجراءات رسمية لإدارة التفويض بخصوص تسهيلات معالجة المعلومات الجديدة. ➢ يحظر استخدام تسهيلات معالجة المعلومات الشخصية أو الخاصة في الجامعة، دون الحصول على موافقة خطية. ➢ يجب أن تتضمن اتفاقيات السرية أو عدم الإفشاء على شروط قانونية قابلة للتطبيق بخصوص متطلبات حماية الأصول المعلوماتية السري في الجامعة. ➢ يجب العمل على تحديد المتطلبات المتعلقة باتفاقيات السرية أو عدم الإفشاء، والقيام بإعادة دراستها بصورة منتظمة. ومن هنا فإنه يتعين على الجامعة القيام بما يلي: • تحديد المعلومات التي ستتم حمايتها ومستوى السرية المطلوبة. • بيان المدة الزمنية المتوقعة للالتزام .

الهدف من السياسة	محور السياسة
	• تحديد شروط إعادة أو إتلاف المعلومات بعد انتهاء الالتزام. • تحديد المسئوليات والمتطلبات المتعلقة بالمفوضين بالتوقيع بغية الحيلولة دون نشر المعلومات دون تفويض. • نشر العقوبات التي ستطبق في حالة عدم احترام المستخدم للالتزام. ➢ على إدارة أمن المعلومات تحديد الهيئات الخارجية الرئيسية، وتطوير وإدامة اتصالات رسمية مع الهيئات التي يتم تحديدها. ➢ تتولى الجامعة وضع إجراءات كافية تحدد متى ومن قبل من سيتم الاتصال بالهيئات (كجهات تطبيق القانون، والدفاع المدني، والهيئات الإشرافية)، وكيفية الإبلاغ عن حوادث انتهاك حماية المعلومات دون تأخير في حالة وجود شك بانتهاك القوانين. ➢ يجب مراجعة السياسات، والإجراءات، والمعايير الفنية بصورة مستقلة ومنتظمة أو عند حدوث تغييرات على بيئة أو وثائق حماية المعلومات. ➢ يجب تدوين نتائج المراجعة المستقلة ورفعها إلى الإدارة، والعمل على حفظ هذه السجلات.

٢. الأطراف الخارجية

الهدف من السياسة	محور السياسة
إدامة حماية معلومات وتسهيلات معالجة المعلومات التي يتم دخولها ومعالجتها وإرسالها إلى ، أو تتم إدارتها من قبل جهة خارجية **[A.6.2]**	➢ يتوجب بحث كافة متطلبات الحماية قبل منح المستخدمين الخارجيين حق الدخول إلى الأصول المعلوماتية للجامعة. ➢ عند الحاجة للسماح لهيئة خارجية بالدخول إلى تسهيلات معالجة المعلومات، ينبغي القيام بعملية تقييم للمخاطر، وذلك للتعرف فيما إذا كانت هناك حاجة لضوابط محددة ➢ يجب عدم منح الأطراف الخارجية حق الدخول إلى معلومات الجامعة قبل تطبيق ضوابط الحماية الملائمة، ويجب فيما لو كان ذلك ممكنا إبرام عقد مع الطرف الثالث يحدد أحكام وشروط الربط أو الدخول وترتيبات العمل. ➢ يجب الاحتفاظ بسجل دقيق وحديث بعمليات دخول الأطراف الخارجية إلى تسهيلات معالجة المعلومات. ➢ يجب تضمين كافة متطلبات الحماية ذات الصلة في اتفاقيات الطرف الثالث، المتعلقة بالدخول إلى، أو معالجة، أو نقل، أو إدارة المعلومات أو تسهيلات معالجة المعلومات في الجامعة. ➢ على الجامعة الإشراف على دخول الطرف الثالث لتسهيلات معالجة المعلومات الخاصة بالجامعة.

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.