هيكل السياسة

١. الهدف

تهدف هذه السياسة إلى تأكيد وبيان التزام الإدارة ونيتها في دعم أهداف ومبادئ حماية المعلومات بما يتوافق مع إجراءات العمل 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.

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

بناء على أفضل الممارسات ومنها معيار (ISO27001:2005) وبما يتوافق مع توصياته، فقد تم تطوير السياسات التالية في سياق برنامج شمولي لحماية المعلومات يهدف إلى دعم سياسة حماية المعلومات هذه، والموقف الأمني الكلي لجامعة الملك عبد العزيز:

- سياسة إدارة المخاطر
- تنظيم سياسة حماية المعلومات
- سياسة إدارة الأصول
- سياسة حماية الموظفين
- سياسة الحماية المادية والبيئية
- سياسة إدارة الاتصالات والعمليات
- سياسة ضبط الدخول
- سياسة اقتناء وتطوير نظم المعلومات
- سياسة التعامل مع حوادث حماية المعلومات
- سياسة التخطيط لاستمرارية العمل
- سياسة الالتزام

تمثل هذه الوثيقة كل من سياسة تقنية المعلومات وسياسة حماية المعلومات، وقد طورت بشكل كلي لأغراض تقنية المعلومات بالجامعة. وترتكز الوثيقة على المعايير العالمية لتقنية المعلومات وعلى أفضل الممارسات (ISO 27001 و COBIT) في هذا المجال. وقد بذلت الجامعة مستويات احترافية من العناية والتركيز لضمان جودة وكفاية المعلومات الواردة بهذه الوثيقة.

٧. المالك

- عمادة تقنية المعلومات

٨. محور السياسة

تهدف هذه السياسة إلى تأكيد وبيان التزام الإدارة ونيتها في دعم أهداف ومبادئ حماية المعلومات بما يتوافق مع إجراءات العمل بجامعة الملك عبد العزيز (الجامعة).

الهدف من السياسة	محور السياسة
قيام الإدارة بتوجيه حماية المعلومات ودعمها وفقا لمتطلبات العمل والقوانين والأنظمة ذات الصلة **[A.5.1]**	➢ يلتزم موظفي الجامعة بالمحافظة على حماية الأصول المعلوماتية الموجودة بحوزتهم وذلك بهدف ضمان الالتزام بالمتطلبات القانونية والتعاقدية. ويتوجب على إدارة الجامعة إدراك مسئوليتها نحو دعم أهداف حماية المعلومات ضمن البيئة. ➢ تلتزم الجامعة بتبني معايير عالمية وأفضل الممارسات المعتمدة، إضافة إلى تبني المتطلبات التنظيمية والتشريعية عند إعداد سياسة حماية المعلومات الخاصة بالجامعة وذلك بهدف ضمان : • عدم الدخول إلى المعلومات إلا من قبل الأفراد المصرح لهم بذلك، والذي لديهم تفويض رسمي معتمد بذلك. • تطبيق الضوابط الملائمة لحماية كافة المعلومات السرية. • عدم تغيير و/أو تحديث المعلومات إلا من قبل الأفراد المصرح لهم بذلك، والذي لديهم تفويض رسمي معتمد بذلك. • ديمومة توفر المعلومات لكافة الأفراد المصرح لهم بذلك، والذي لديهم تفويض رسمي معتمد للدخول إلى هذه المعلومات. • أن كافة الأفراد الذين حصلوا على أي نوع من التفويض بالدخول إلى المعلومات يتحملون كامل المسئولية عن الاستخدام المناسب لهذه المعلومات. • تقوم إدارة الجامعة بتحديد واعتماد إطار منظم لحماية المعلومات وفقا لمتطلبات العمل. وتلتزم الإدارة بتوفير التوجيه والدعم اللازمين لتطبيق هذا الإطار. ➢ أن كافة موظفي الجامعة على إدراك تام، ويقرون بمسئوليتهم فيما يتعلق بالالتزام بسياسات وإجراءات ومعايير حماية المعلومات. ➢ تقوم إدارة أمن المعلومات بمراجعة وتحديث سياسات وإجراءات ومعايير حماية المعلومات كل عام. ➢ تقوم إدارة أمن المعلومات بإجراء قياس سنوي لفعالية الضوابط المطبقة بهدف تجنب حوادث انتهاك حماية المعلومات وتقليص الآثار الناتجة عن ذلك، بالإضافة إلى مقارنة مستوى نضج الحماية في الجامعة مع مؤسسات أخرى مماثلة. ➢ توافق سياسات وإجراءات ومعايير حماية المعلومات ذات الصلة مع المتطلبات

الهدف من السياسة	محور السياسة
	القانونية والتنظيمية والمعايير العالمية. ➢ تقوم إدارة أمن المعلومات بالتعاون مع الإدارة بضمان التحقيق الفعّال لأهداف وغايات حماية المعلومات والأنشطة الأخرى ذات الصلة. ➢ على كافة الدوائر الأخرى وبدعم من إدارة أمن المعلومات ضمان توفر مستويات مقبولة من الحماية للأصول المعلوماتية الموجودة لديهم.

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.