هيكل السياسة

١. الهدف

تهدف سياسة الالتزام هذه إلى تزويد موظفي جامعة الملك عبد العزيز (الجامعة) بما يلزم لتجنب أي انتهاك لسياسات حماية المعلومات، والقوانين والأنظمة والالتزامات التعاقدية أو أية متطلبات تتعلق بالحماية.

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 وتوفير 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 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

- كافة سياسات حماية المعلومات

٧. المالك

- مدير إدارة أمن المعلومات

٨. محور السياسة

ينبغي تطبيق كافة الضوابط اللازمة لضمان التزام كافة الموظفين والمقاولين والاستشاريين بسياسات حماية المعلومات، والقوانين والأنظمة والالتزامات التعاقدية أو أية متطلبات تتعلق بالحماية في جامعة الملك عبد العزيز.

١. المتطلبات القانونية

الهدف من السياسة	محور السياسة
تجنب انتهاك أي قانون، أو تشريع أو نظام أو التزام تعاقد أو أية متطلبات ذات صلة بالحماية **[A.15.1]**	➢ تقوم الجامعة بتحديد وتحليل المتطلبات التنظيمية الخارجية على صعيد تأثيرها على وظائف تقنية المعلومات، واتخاذ التدابير الملائمة للالتزام بها . ➢ تقوم الجامعة بتحديد وتوثيق المتطلبات التشريعية والتنظيمية والتعاقدية ذات الصلة. ➢ يتوجب على الجامعة التأكد من التزام تصميم وإدارة تشغيل واستخدام نظم المعلومات والتسهيلات ذات الصلة بكافة المتطلبات القانونية والتنظيمية أو المتطلبات التعاقدية ذات الصلة بحماية المعلومات. ➢ يجب أن يتضمن دليل الحماية الخاص بكل نظام من نظم المعلومات توثيقا للمتطلبات التشريعية والتنظيمية والتعاقدية. ➢ يجب وضع هيكل للإدارة والضبط وذلك لضمان الالتزام بهذه السياسة والقوانين والنظم الأخرى ذات الصلة والتي تتوافق مع متطلبات الجامعة. ➢ ينبغي عدم نقل المعلومات الشخصية أو إطلاع أية جهة أخرى عليها، عندما يمكن اللجوء إلى استخدام البيانات الإحصائية كبديل عن ذلك. ➢ يجب وضع وتوثيق إجراءات لتصنيف وحماية السجلات من إساءة الاستخدام أو الضياع أو التلف أو التزوير. ➢ يتوجب على الجامعة تفهم أهمية حقوق الملكية الفكرية المرتبطة بنظم المعلومات لديها. ومن هذه الحقوق : • البرامج • حقوق تأليف وطباعة الوثائق • حقوق التصميم • العلامات التجارية • براءات الاختراعات • الرموز البرمجية(Source Code) والرخص. ➢ تتمثل حقوق الملكية الفكرية الخاصة بالجامعة بما يلي: • المخرجات التي تقوم الجامعة بإنشائها داخليا دون وجود عميل خارجي راعي لهذه المخرجات. • المخرجات التي يتم إنشاؤها بصورة مشتركة من قبل الجامعة وطرف ثالث، حيث يوافق الطرفان بموجب عقد (تفاهم مكتوب) على أن حقوق الملكية الفكرية تخص الجامعة. ➢ على الجامعة الالتزام بما يلي: • متطلبات حقوق التأليف والطبع المرتبطة بالمواد والبرامج والتصاميم

الهدف من السياسة	محور السياسة
	المملوكة للجامعة. • متطلبات التراخيص والتي تُقيّد استخدام المنتجات والبرامج والتصاميم والمواد الأخرى التي تحتاج إليها الجامعة. ➢ على الجامعة تطوير وتطبيق إجراءات مناسبة لضمان أن التشريعات، والأنظمة والمتطلبات التعاقدية متوافقة مع حقوق الملكية الفكرية. ➢ ينبغي إدامة الالتزام بمتطلبات حقوق التأليف والطبع والترخيص المرتبطة بالمنتج، وأن يتم التحقق من ذلك بصورة منتظمة. ➢ يجب على الجامعة الاحتفاظ بما يدل على ملكية المديرية للرخص أو لأدلة التشغيل وتوفير الحماية اللازمة لهذا الدليل. ➢ تقوم الجامعة بتبني وثيقة تحدد الأسلوب الملائم للتصرف بالبرامج أو نقلها إلى جهات أخرى. ➢ يصرح فقط بالدخول المادي والمنطقي إلى المواد المشتركة (بين الجامعة وطرف ثالث، على أساس مُحْكم واعتمادا على مبدئي "الحاجة إلى المعرفة" و"الحاجة إلى الدخول". ➢ تحمى حقوق تأليف البرامج وفقا لأحكام العقد، على أن يتم القيام بعملية توعية ملائمة للمستخدمين. ➢ يتوجب على الجامعة تطبيق ضوابط حماية للحيلولة دون تعرض المواد والبرامج التي تخص حقوق الملكية في الجامعة من أي نوع من أنواع إساءة الاستخدام. ➢ تلتزم الجامعة بعدم نسخ المواد التي تخص الطرف الثالث، أو تحويلها إلى صيغة أخرى أو أخذ مقتطفات منها من التسجيلات التجارية (الأفلام والأشرطة) بما يتعارض مع سياسة حقوق التأليف. ➢ على كافة المستخدمين الإقرار بأن إساءة استخدام المواد من قبلهم قد يؤدي إلى انتهاك حقوق الملكية الفكرية للطرف الثالث. ➢ على الجامعة وضع وتوثيق سياسة مناسبة بخصوص الاستخدام المقبول لتسهيلات معالجة المعلومات. ➢ ينبغي أن يكون كافة المستخدمين على دراية واطلاع على النطاق المحدد بوضوح للدخول المصرح به لهم، وكذلك بوجود مراقبة للكشف عن الاستخدام غير المصرح به. ➢ على جميع المستخدمين الإقرار بأن إساءة استخدام تسهيلات معالجة المعلومات من قبلهم قد يؤدي إلى انتهاك السرية على صعيد التزامات الجامعة، وبأنهم ملتزمون بسياسات الجامعة.

٢. سياسات حماية المعلومات، والمعايير والأمور التقنية

الهدف من السياسة	محور السياسة
ضمان توافق النظم سياسات ومعايير الحماية في المؤسسة **[A.15.2]**	➢ على كل إدارة ضمان التوافق التام بين السياسات والإجراءات والمعايير التي تخصها وسياسات ومعايير حماية المعلومات في الجامعة. ➢ على كافة المستخدمين تفهم مسئوليتهم والإقرار بالالتزام بسياسات ومعايير الحماية بالجامعة. ➢ تتولى الجامعة القيام بعملية تدقيق على الالتزام التقني مرتين في العام. ويتضمن التقييم على سبيل المثال لا الحصر : • تفقد نظم التشغيل. • اختبار اختراق. • تقييم نقاط الضعف التي تعاني منها الحماية. ➢ كلما أمكن ذلك، يجب إجراء اختبار الاختراق وتقييم نقاط الضعف في الحماية لتقييم فعالية الضوابط المطبقة. ➢ يجب أن لا يتم إجراء تدقيق الالتزام التقني إلا من قبل شخص مؤهل ومرخص، أو أن يتم التدقيق تحت إشراف مثل هذا الشخص.

٣. تدقيق نظم المعلومات

الهدف من السياسة	محور السياسة
زيادة فعالية عملية تدقيق نظم المعلومات/ وتقليل التشويش الذي قد ينجم عنها على النظم **[A.15.3]**	➢ ينبغي القيام بتعقب كل تدقيق من التدقيقات على حده بهدف إغلاقه، والقيام بالإبلاغ عن أي عدم انتظام يتعلق بالتدقيق إلى رئيس الإدارة ذات العلاقة وإدارة الجامعة بذلك. ➢ تكون النتائج التي يتوصل إليها التدقيق المخطط له أو العشوائي طبقا لنوع المخاطر(خطر مرتفع، خطر متوسط، أو خطر منخفض). وعلى المدققين تصنيف النتائج على أنها غير متوافقة مع الإجراء الموثّق أو أنها تمثل قصورا في النظام. ➢ على الجامعة تقييد وضبط استخدام أدوات تدقيق النظم وفقا لإرشادات محددة لهذا الغرض. ➢ ينبغي الفصل فيما بين أدوات التدقيق، كالبرامج أو ملفات البيانات، ونظم التطوير أو النظم العاملة الحية، وعدم حفظها في مكتبة الأشرطة أو في المناطق المخصصة للمستخدمين ما لم يتم تزويدها بمستويات إضافية من الحماية.

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.