هيكل السياسة

١. الهدف

يجب توفير الحماية الكافية لكافة الأصول التابعة لجامعة الملك عبد العزيز (الجامعة)، وللموظفين دور هام فيما يتعلق بحماية المعلومات يمكن تحقيقه من خلال بيان متطلبات حماية الأصول التابعة للمديرية من الاستغلال، إساءة الاستخدام أو الإتلاف المتعمد من قبل الموظفين أو المقاولين أو الاستشاريين.

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 مالك الأصل المعلوماتي

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

٢. 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.

٣. 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.

٤. 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.

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.

٦. 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 حماية المعلوماتي
- سياسة التعامل مع حوادث حماية المعلومات

٧. المالك

- مدير إدارة أمن المعلومات

٨. محور السياسة

تتولى جامعة الملك عبد العزيز وضع إجراءات رسمية لتوظيف، واستقالة وإنهاء عقود عمل الموظفين، بحيث تقوم، ومن خلال برنامج تعريف الموظف بالجامعة، بإعداد وعقد دورات توعية بأهمية حماية المعلومات لكافة الموظفين.

١. ما قبل التوظيف

الهدف من السياسة	محور السياسة
ضمان أن الموظفين والمقاولين والمستخدمين التابعين لطرف ثالث على دراية بمسئولياتهم، وبأنهم مناسبون للأدوار التي يجري النظر في توظيفهم للقيام بها، والتقليل من مخاطر السرقة، أو إساءة استخدام التسهيلات **[A.8.1]**	➢ على كافة الموظفين إدراك مسئوليتهم فيما يتعلق بحماية كافة الأصول التي تملكها جامعة الملك عبد العزيز و/ أو تلك التي تكون في عهدتها. ➢ على كافة الموظفين إبلاغ مديرهم المباشر بأية تهديدات أو هجمات حقيقية أو محتملة ضمن بيئة الجامعة. ➢ يتولى مدراء كافة القطاعات - الإدارات مسئولية تحديد مجموعة المهارات اللازمة لتفعيل دور الموظفين ضمن الإدارات التابعة لهم. ➢ على مدراء كافة القطاعات - الإدارات التنسيق مع إدارة الشؤون الإدارية التأكد من أن إجراءات توظيف كافة الموظفين تنسجم وتتوافق مع السياسات والإجراءات المعمول بها في الجامعة. ➢ تقوم إدارة الشؤون الإدارية أو أي طرف ثالث مناسب، بإجراء تدقيق على المرشحين للوظائف، أو للتعاقد أو للعمل كطرف ثالث مع الجامعة. ➢ في الحالات التي يتم فيها توفير الموظفين من قبل وكالة توظيف، فإنه ينبغي للعقد الموقع مع هذه الوكالة بيان مسئوليات الوكالة فيما يتعلق بالتدقيق على خلفية الموظفين. ➢ تقوم إدارة الشؤون الإدارية بإعداد مواد تعريفية مناسبة تعطى للموظفين الجدد، وتعمل هذه المواد كدليل فيما يتعلق بالمناصب التي سيشغلونها، وبالضوابط والتدابير المتعلقة بأي من هذه المناصب. ➢ يتوجب على كافة الموظفين، التوقيع على إقرار خطي مفاده بأنهم قد قاموا بقراءة وقبول سياسة حماية المعلومات في الجامعة. ➢ يتوجب على كافة الموظفين، الالتزام بمسئوليات حماية المعلومات، وإدراج هذه المسئوليات في دليل الموظف الذي تصدره الجامعة. ➢ ينبغي إدراج مسئوليات محددة تتعلق بحماية المعلومات في كافة العقود المبرمة مع المقاولين (بما في ذلك الاستشاريين، أو أي طرف لا يكون موظفا ويقوم بأداء عمل في الجامعة) والذين سوف يتم تمكينهم من الدخول إلى معلومات سرية أو تخص الجامعة أو تكون ذات طبيعة حساسة. ➢ تعمل إدارة الشؤون الإدارية بالتنسيق مع مدراء كافة القطاعات والإدارات، على توثيق الأدوار والمسئوليات ضمن الوصف الوظيفي بما يلبي متطلبات سياسة حماية

الهدف من السياسة	محور السياسة
	المعلومات. ➢ يتضمن الوصف الوظيفي مسئوليات محددة فيما يتعلق بحماية المعلومات وبما يتماشى مع الدور الذي يقوم به الموظف. ➢ على كافة القطاعات والإدارات أن يكونوا على دراية بالظروف الشخصية لموظفيهم وإبقاء أعينهم مفتوحة لملاحظة أية تغيرات سلوكية قد تؤدي إلى حدوث انتهاك لحماية المعلومات. ➢ يجب أن تعمل أحكام وشروط التوظيف على تحديد مسئوليات الموظف تجاه حماية المعلومات من خلال اتفاقية الحفاظ على السرية. ➢ على كافة الموظفين والمقاولين والأطراف الثالثة المتعاملة مع الجامعة توقيع شروط وأحكام التوظيف/ المهمة وذلك كمؤشر على قبولهم بها. ➢ على كافة الموظفين التوقيع على اتفاقية عدم الإفشاء. وبالإضافة إلى ما ورد بسياسات وإجراءات ومعايير وإرشادات الجامعة، فإنه ينبغي لهذه الاتفاقية أن تعمل تحديدا على مطالبة الموظف بوجوب الالتزام بكافة السياسات والإجراءات والمعايير والإرشادات ذات الصلة. ➢ ينبغي أن يطلب من الموظفين التابعين للمقاولين أو للوكالات المتعاقد معها من الذين يقوم الموظفون التابعون لهم بزيارة المناطق الحساسة، التوقيع على اتفاقية الحفاظ على السرية.

٢. أثناء التوظيف

الهدف من السياسة	محور السياسة
ضمان أن الموظفين والمقاولين والمستخدمين التابعين لطرف ثالث على وعي بالتهديدات والمسائل التي تتعرض لها المعلومات، وبمسئولياتهم، والتزاماتهم، وبأنهم مؤهلون لدعم سياسة الحماية في الجامعة أثناء أدائهم لمهام عملهم الاعتيادية، وتقليص الأخطاء البشرية **[A.8.2]**	➢ يتلقى كافة الموظفين، وكذلك المقاولين والمستخدمين التابعين لأطراف ثالثة -فيما إذا دعت الحاجة – تدريبا في مجال التوعية بأهمية حماية المعلومات، بالإضافة إلى تزويدهم على أساس منتظم بالتحديثات التي تتم على السياسات والإجراءات ويكون لها صلة بمسئولياتهم الوظيفية. ➢ تقوم الجامعة بالتأكد من أن كافة الموظفين على دراية بمتطلبات حماية المعلومات، وبأنهم يتم تدريبهم على متطلبات وإجراءات الحماية المرتبطة بأعمالهم. ➢ يجب أن يتلقى كافة الموظفين تدريبا حديثا، بما لا يقل عن مرة واحدة في السنة، وذلك لوضعهم بصورة المستجدات على سياسة حماية المعلومات في الجامعة. ➢ تتولى الجامعة، وبهدف ردع الآخرين، إيقاع إجراءات تأديبية رسمية بالموظفين الذين يصرون على انتهاك سياسات حماية المعلومات. ➢ ينبغي للإجراءات التأديبية أن تنطوي على معاملة الموظفين، الذين يشك في قيامهم بانتهاك الحماية، بصورة صحيحة ومنصفة. ➢ تعمل الجامعة على اتخاذ تدابير احتياطية للفصل بين واجبات الموظف بهدف تقليص فرص التعديل غير المصرح به للمعلومات أو إساءة استخدامها. ➢ يجب عدم استخدام تسهيلات معالجة المعلومات لأغراض ليست لها صلة بالعمل. وفي حالة اكتشاف أية عمليات تحايل فإنه سيتم التعامل معها وفقا للإجراءات التأديبية. ➢ على كافة الموظفين والمقاولين، تفهم مسئوليتهم فيما يتعلق بسرعة إبلاغ الجامعة، عن

الهدف من السياسة	محور السياسة
	أية أحداث أو مخاطر ذات صلة بحماية المعلومات. ➢ على إدارة أمن المعلومات التأكد من التحقيق في كافة الأنشطة الاحتيالية التي يجري الإبلاغ عنها.

٣. إنهاء الخدمة أو تغيير الوظيفة

الهدف من السياسة	محور السياسة
ضمان أن عملية ترك العمل أو تغيير الوظيفة من قبل الموظفين والمقاولين والمستخدمين التابعين لطرف ثالث تجري بصورة صحيحة **[A.8.3]**	➢ تقوم الجامعة بتحديد وتخصيص مسئوليات وإجراءات إنهاء الخدمة أو تغيير طبيعة الخدمة، بشكل واضح. ➢ على كافة الموظفين والمقاولين وموظفي الطرف الثالث إعادة كافة الأصول المعلوماتية والمادية الموجودة بعهدتهم عند إنهاء الوظيفة أو العقد. ➢ ينبغي أن يتم سحب حقوق الدخول إلى المعلومات وتسهيلات معالجة المعلومات عند إنهاء خدمة الموظف أو الاتفاقية التعاقدية. ➢ على إدارة أمن المعلومات ، بالتعاون مع إدارة الشؤون الإدارية ، وفيما لو دعت الحاجة، التأكد من نقل الموظفين الذين يعملون في وظائف هامة ، أو قاموا بإعطاء إنذار بنيتهم ترك العمل في الجامعة ، إلى مناصب لا يستطيعون من خلالها إلحاق سوى الحد الأدنى من الضرر بأصول الجامعة. ويمكن أيضا، وحسب تقدير مدير الإدارة منحهم إجازة إجبارية.

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.