هيكل السياسة

١. الهدف

تعمل هذه السياسة على توفير الإرشادات الكفيلة بمنع الدخول غير المصرح به والتدخل بالمباني والأصول المعلوماتية التابعة لجامعة الملك عبد العزيز (الجامعة). كما تقترح أيضا الإرشادات اللازمة لبناء ضوابط الحماية بهدف الحيلولة دون وقوع أية أضرار نتيجة للتهديدات المادية والمخاطر البيئية.

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 الشؤون الإدارية

- وضع وإدامة نظم للسيطرة على الدخول المادي.
- تدقيق ومراجعة الحماية المادية.
- تصميم نظم الحماية المادية، والإشراف على تركيبها، وصيانتها وتشغيلها.
- تصميم نظم السيطرة البيئية، والإشراف على تركيبها.
- مساعدة أو إبلاغ الأطراف ذات العلاقة، بخصوص أية تغييرات على واجبات الموظف أو إنهاء عقد عمله.
- الإسهام في تصميم وتطبيق والإشراف على ضوابط الحماية المادية والبيئية.

٣. 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 ضبط الدخول
- سياسة إدارة الأصول
- سياسة حماية الموظفين

٧. المالك

- مدير إدارة أمن المعلومات

٨. محور السياسة

تعمل الحماية المادية والبيئية على حماية المعلومات ومرافق نظم المعلومات من التهديدات المادية والبيئية. وتتولى جامعة الملك عبد العزيز مسئولية ضمان ضبط الدخول إلى مناطق معالجة المعلومات والبنية التحتية المساندة لها (الاتصالات، الطاقة الكهربائية، والبيئة) بهدف منع واكتشاف والحد من الدخول غير المقصود لهذه المناطق (كالدخول غير المصرح به، أو التسبب بانقطاع عملية المعالجة نفسها).

وتتطرق هذه السياسة إلى مسائل تتصل بنطاقات الحماية المادية، وضوابط الدخول المادي، وظروف العمل، وتأمين المكاتب، ومراكز البيانات، وحماية المعدات والضوابط العامة.

١. الضوابط المادية والبيئية

الهدف من السياسة	محور السياسة
منع الدخول المادي غير المصرح به، أو إتلاف مباني أو معلومات الجامعة أو التشويش عليها **[A.9.1]**	➢ يجب تقسيم المواقع المادية لمواقع معالجة المعلومات في الجامعة إلى نطاقات أمنية، بحيث يكون لكل منطقة مستويات عليا من القيود على الدخول ومتطلبات التفويض بالدخول. ➢ يجب تزويد مناطق الدخول المؤمنة بضوابط حماية مادية مشددة لتوفير حماية إضافية للأصول، ويراعى في هذه الضوابط المادية استخدام الجدران، أبواب مزودة بأقفال مُحْكمة أو مكتب أمن. ويمكن اختيار ضوابط الحماية المادية بناء على حيوية الأصول التي يجري حمايتها. ➢ يجب تحديد وتطبيق النطاق الأمني بوضوح. ➢ ضبط الدخول المادي إلى الموقع أو المبنى من خلال توفير مكتب استقبال يديره موظف استقبال، أو من خلال أي وسيلة أخرى. يكون الدخول إلى الموقع والمباني مقصورا على الموظفين المصرح لهم بذلك فقط. ➢ يجب، عند الضرورة، نشر حواجز مادية من السقف الحقيقي إلى الأرضية الحقيقية للحيلولة دون الدخول غير المصرح به والتلوث البيئي كالذي ينجم عن الحريق أو الفيضانات. ➢ يجب تزويد كافة أبواب الحريق الموجودة في النطاق الأمني بأجهزة إنذار أو إبقائها موصدة. ➢ يجب أن يتسم النطاق الأمني للمبنى أو الموقع الذي يتضمن تسهيلات معالجة المعلومات بالمتانة من الناحية المادية . ➢ يقتصر الدخول إلى المناطق ذات التصنيف الأمني المرتفع كمراكز البيانات على الأفراد الذين يتولون مسئوليات مباشرة عن تشغيل وتوفير مركز البيانات. ➢ على كافة الموظفين ارتداء ما يدل على هويتهم، بحيث تكون الوسيلة المستخدمة ظاهرة للعيان. ➢ يحظر على كافة موظفي الجامعة تبادل استخدام بطاقات الدخول الأمنية إلى مباني الجامعة فيما بينهم. ➢ يجب العمل بانتظام على مراجعة وتحديث حقوق الدخول إلى المناطق المؤمنة. ➢ ينبغي ضبط الدخول إلى المعلومات الحساسة وإلى تسهيلات معالجة البيانات، واقتصار الدخول على الموظفين المصرح لهم بذلك فقط. كما ينبغي العمل على توفير سجل لتعقب كافة عمليات الدخول وحفظ السجل بصورة آمنة. ➢ يجب على كافة زائري مرافق معالجة المعلومات في الجامعة توقيع " سجل الزوار" الموجود لدى حرس المبنى والذي يخضع للمراجعة، وسوف تقوم الجامعة بتطبيق إجراءات لضبط الزيارات. ➢ يجب فصل تسهيلات معالجة المعلومات التابعة للجامعة، والتي تقوم بمعالجة

الهدف من السياسة	محور السياسة
	بيانات حساسة، ماديا عن تلك التي تدار من قبل أطراف ثالثة. ➢ يجب تركيب وسائل مراقبة في مرافق معالجة المعلومات والعمل على مراقبتها. ➢ يجب تركيب نظام مناسب لكشف المتطفلين بحيث يغطي الأبواب الخارجية، والنوافذ التي يمكن الدخول من خلالها، والعمل على اختبار هذا النظام بصورة منتظمة. ➢ يجب وضع وسائل ومعدات الدعم (أجهزة نسخ الوثائق والفاكس) في مكان ملائم ضمن المنطقة المؤمنة لتجنب طلبات الدخول التي قد تؤدي إلى تعريض المعلومات إلى الخطر. ➢ يجب تخزين المواد الخطرة والقابلة للاحتراق بشكل آمن على مسافة آمنة من المناطق المؤمنة. ➢ توضع الأجهزة البديلة (Fallback) ووسائط الحفظ الاحتياطي على مسافة آمنة للحيلولة دون تعرضها للتلف في حالة وقوع كارثة في المبنى الرئيسي. ➢ يجب تصميم الضوابط البيئية وتطبيقها بهدف الحد من الضرر الذي تتسبب به الحرائق، الفيضانات، الهزات الأرضية، التفجيرات، الاضطرابات، والأشكال الأخرى من الكوارث الطبيعية أو تلك التي يتسبب بها البشر. ➢ تتولى الجامعة توفير مستوى من الحماية المادية والبيئية للبنية الفنية بما يكفل تقليص احتمالات وقوع مخاطر بيئية. ➢ ينبغي لتصميم الضوابط البيئية أن يراعي تشريعات ومعايير الصحة والسلامة ذات الصلة، وان يأخذ بعين الاعتبار التهديدات الأمنية التي تمثلها المباني المجاورة. ➢ تعمل الجامعة على ضمان ما يلي : • عدم تواجد مرافق معالجة المعلومات في منطقة غير مستقرة من الناحية البيئية. • عدم تواجد مرافق معالجة المعلومات بالقرب من أية مرافق خطيرة (معامل كيمياء، وغيرها). • تلبية معدّات اكتشاف ومكافحة الحريق المتطلبات المحددة من قبل الجهة المصنعة. ➢ تقوم الجامعة بمراعاة السلامة الشخصية للموظفين بوصفها على قمة الأولويات، واتخاذ الخطوات اللازمة لضمان توفر السلامة في مكان العمل. وتتولى الجامعة بالتعاون مع القطاعات/ الإدارات المختصة الأخرى، تطوير إجراءات طوارئ ملائمة للتعامل مع تشكيلة من التهديدات. ويتوجب توثيق وتوفير واختبار إجراءات الطوارئ بصورة دورية في كل مرفق من المرافق وبخصوص كل تهديد من التهديدات الهامة. ➢ يجب أن تتضمن مرافق الجامعة معدّات طوارئ (مثل مصابيح احتياطية، معدات مكافحة الحريق) لتحقيق مستوى كاف من السلامة بخصوص العاملين في

الهدف من السياسة	محور السياسة
	المرافق. وينبغي تفقد هذه المعدات سنويا لضمان قدرتها على العمل. ➢ يجب توفير ضوابط وإرشادات لتعزيز حماية المناطق المؤمنة. وينطبق ذلك على الموظفين بالإضافة إلى المقاولين والأطراف الثالثة التي تعمل في هذه المناطق. ➢ يجب أن تخضع الأعمال التي تتم في المناطق المؤمنة من قبل طرف ثالث أو من قبل الموردّين للإشراف. ➢ يجب القيام بعمليات مراقبة في موقع الجامعة لضمان سلامة القوة العاملة وتجنب فقدان الممتلكات. ➢ يمنح موظفي خدمات الإسناد التابعين لطرف ثالث حق الدخول إلى المناطق المؤمنة عند الحاجة، وشروط حصولهم على التفويض اللازم والإشراف عليهم.

٢. حماية الأصول

الهدف من السياسة	محور السياسة
الحيلولة دون فقدان أو تلف أو سرقة أصول الجامعة أو تعريضها للخطر أو التسبب في توقف أنشطة المؤسسة **[A.9.2]**	➢ يجب عزل تسهيلات معالجة المعلومات التابعة للجامعة، والتي تقوم بمعالجة بيانات حساسة، بهدف إضافة ضوابط احتياطية. ➢ يجب العمل على مراقبة كافة الظروف المحيطة (كالحرارة والرطوبة)، والتي قد تؤثر على عمل تسهيلات معالجة المعلومات الحساسة في الجامعة . ➢ يجب توفير الحماية الكافية لخطوط الاتصال والمعدات الخاصة بالجامعة، وذلك لضمان توافر وسرية الموارد. ➢ يجب العمل على إحْكَام ضبط عمليات نقل المعلومات ووسائط تخزين البرامج والأجهزة وأية أصول مادية أخرى. وأن لا يسمح إلا للموظفين الحاصلين على تفويض بأخذ ممتلكات الجامعة خارج المباني، وفي هذه الحالة فإن مسئولية حماية هذه الممتلكات وضبط عملية استخدام تقع على عاتقهم. وسوف تتولى الجامعة مسئولية تطوير وتوفير الإجراءات اللازمة لضبط الممتلكات التي تخصها. ➢ تتولى الجامعة توفير حماية من الطاقة الكهربائية لدعم سلامة للموظفين وضمان توافر نظم المعلومات التابعة للجامعة. كما يجب تهيئة كافة التطبيقات الحيوية بحيث يمكن التحول على الفور إلى مصدر بديل للطاقة، في حالة انقطاع التيار الكهربائي. ➢ ينبغي فصل خطوط الطاقة الكهربائية عن كابلات شبكة نقل البيانات حسب الأصول، وذلك للحيلولة دون حدوث تداخل أو تشويش. ➢ يجب عزل وحماية الكابلات الخاصة بشبكة نقل البيانات، لحمايتها من عمليات الاعتراض من قبل غير المخولين، أو من التلف، وذلك من خلال استخدام القنوات (Conduit) أو تجنب تمرير هذه الكابلات عبر المناطق العامة.

الهدف من السياسة	محور السياسة
	➢ يجب الإشراف على أعمال الصيانة الوقائية والتصحيحية التي تتم من قبل موظفي المورد داخل الجامعة ، والحصول على موافقة رسمية بخصوصها. ➢ يجب صيانة معدات الجامعة حسب الأصول لضمان توافرها ودقتها. ➢ على إدارة أمن المعلومات التأكد من تطبيق الإجراءات المناسبة بخصوص وضع المعدات خارج المبنى، وفقا لمتطلبات السلامة الخاصة بالأصل المعلوماتي. ➢ يجب تزويد مناطق التخزين التابعة للجامعة والواقعة خارج المباني، بنفس المستوى من الحماية الموجودة في موقع المعالجة الرئيسي، وأن يتم تطبيق ضوابط حماية مادية وبيئية لحماية البيانات. ➢ يجب عدم ترك المعدات والوسائط ، التي يتم نقلها خارج المبنى، في الأماكن العامة دون إشراف. ➢ يجب تزويد معدات الجامعة والتي يتم استخدامها خارج الموقع مناطق التخزين التابعة للجامعة والواقعة خارج المباني، بنفس مستويات حماية المعدات الموجودة في موقع المعالجة الرئيسي، مع أخذ المخاطر التي تواكب العمل في خارج المبنى بعين الاعتبار. ➢ يجب إتلاف أجهزة التخزين التابعة للجامعة، والتي تحتوي على معلومات حساسة يدويا، وذلك عوضا عن القيام بعملية الـ "حذف" القياسية. ➢ يجب التخلص من الوثائق الحساسة والوسائط والمعدات التابعة للجامعة بطريقة معتمدة تعمل على حماية سرية المعلومات المطبوعة أو المخزّنة. ➢ يجب تقييم المخاطر المتعلقة بأدوات التخزين التالفة التي تحتوي على بيانات حساسة لتحديد فيما إذا كان سيتم إتلاف أو صلاح أو التخلص من المعدّة. ➢ يجب الحصول على تخويل خطي بخصوص المعدّات، والمعلومات، والبرمجيات التي يتم نقلها إلى خارج الجامعة ➢ على الجامعة الاحتفاظ بسجل دقيق وحديث بكافة المعدّات التي تم نقلها إلى خارج المبنى.

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.