هيكل السياسة

١. الهدف

تهدف سياسة استمرارية العمل بجامعة الملك عبد العزيز(الجامعة) إلى تحديد الإجراءات الملائمة والتي من شأنها تقليص حالات توقف أنشطة العمل، وحماية إجراءات العمل الحساسة من الآثار التي قد تنجم عن حدوث عطل واسع في نظم المعلومات، أو وقوع الكوارث، وضمان استئناف العمل بهذه النظم دون تأخير.

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 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 إدارة الأصول
- سياسة التعامل مع حوادث حماية المعلومات

٧. المالك

- مدير إدارة أمن المعلومات

٨. محور السياسة

ينبغي عند التخطيط لاستمرارية العمل في جامعة الملك عبد العزيز، أن ينطوي على إدراج ضوابط لتحديد المخاطر والحد من آثارها، وضمان توفر المعلومات اللازمة لإجراءات العمل في الجامعة.

إدارة استمرارية العمل

الهدف من السياسة	محور السياسة
مواجهة الأعطال والإنقطاعات في أنشطة العمل وحماية إجراءات العمل الهامة من الآثار المترتبة على الأعطال الرئيسية لنظم المعلومات أو الكوارث ، وضمان استئناف العمل دون تأخير. [A.14.1]	➢ ينبغي مراعاة الجوانب المتعلقة بحماية المعلومات أثناء تخطيط وتطوير إدارة استمرارية العمل. وفيما يلي بعض العناصر الرئيسية: • تطوير إستراتيجية رسمية لاستمرارية العمل. • تطوير إطار التخطيط لاستمرارية العمل. • تحليل آثار المخاطر على العمل وإدارة المخاطر. • تطوير وتطبيق خطط استمرارية العمل. • تطوير خطة للتعافي من الكوارث واستئناف العمل. • توفير وإعادة تقييم خطط استمرارية العمل. • اختبار خطط استمرارية العمل. ➢ على لجنة مواجهة الكوارث واستمرارية العمل القيام بتحليل نصف سنوي للآثار على العمل (BIA) لتحديد إجراءات العمل الهامة ووضع الأولويات المرتبطة بها وتكلفة تعطلها. ويجب لهذا التحليل أن يغطي توفير إجراءات العمل وأهداف زمن الاستعادة (RTOs) وأهداف نقطة استعادة إجراءات العمل (RPOs). ➢ على إدارة أمن المعلومات تعميم نتائج تحليل الآثار على العمل (BIA) على قطاعات وإدارات وأقسام الجامعة وذلك بهدف تطوير تحليل للآثار على العمل يكون مخصصا لكل قطاع - إدارة أو قسم، وتحديد إجراءات العمل الهامة والمخاطر التي قد تنجم في حالة عدم توفر هذه الإجراءات. وعلى كل قطاع إدارة أو قسم تعيين منسق للجنة مواجهة الكوارث واستمرارية العمل ، يقوم من خلال تلقي الإرشادات والتوجيه من لجنة مواجهة الكوارث واستمرارية العمل، بتنسيق عملية تطوير تحليل الآثار على العمل المخصص لكل قطاع - إدارة أو قسم، وخطة استمرارية العمل المخصصة التي تنتج عن هذا التحليل. ➢ ينبغي تطوير خطط استمرارية العمل باستخدام نتائج تقييم المخاطر، والتي ستحدد النهج الكلي لاستمرارية العمل. ➢ ينبغي لعملية تقييم المخاطر أن تعمل على تحديد المخاطر وكميتها وترتيب المخاطر وفقا لمعايير وأهداف العمل في الجامعة، وان تأخذ بعين الاعتبار آثار انقطاع الخدمات، وأوقات التعطّل المسموح بها، وأولويات التعافي. ➢ يتم تطبيق خطط استمرارية العمل (خطط طوارئ)، وذلك من خلال مزيج من ضوابط المنع والاستعادة، بهدف تقليص الآثار السلبية على المديرية والتعافي من خسارة الأصول المعلوماتية إلى مستوى مقبول. وينبغي أن يعتمد التخطيط لاستمرارية العمل على المخاطر التي سبق تحديدها، والتي يمكنها التسبب بانقطاع إجراءات العمل (تعطل الأجهزة، الحرائق وغير ذلك)، والقيام بتحليل الآثار على العمل لمعرفة احتمالات وعواقب مثل هذه الانقطاعات من حيث المدة الزمنية، نطاق التلف وفترة التعافي. ➢ يمكن للمخاطر أن تؤدي إلى انقطاع إجراءات العمل (تعطل الأجهزة، الحرائق وغير ذلك)، والقيام بتحليل الآثار لمعرفة احتمالات وعواقب مثل

الهدف من السياسة	محور السياسة
	هذه الانقطاعات من حيث المدة الزمنية، نطاق التلف وفترة التعافي. ➢ في ذلك خسارة الموظفين أو المباني أو الأجهزة أو الخدمات الرئيسية. على الجامعة وفي سياق خطط استمرارية العمل، وضع خطط طوارئ، تكون قابلة للتطبيق بخصوص النظم الموجودة لديها، بحيث تسمح هذه الخطط بإدامة القدرات التشغيلية أو استعادتها في حالة حدوث طارئ بما ➢ على الجامعة تطبيق إجراءات تسمح باستعادة عمليات العمل وتوفير المعلومات ضمن المدى الزمني المطلوب. ➢ تتولى لجنة مواجهة الكوارث واستمرارية العمل مسئولية ضمان أن خطة استمرارية العمل التي تم تطويرها قد أسفرت عن تحديد موارد مالية، وتنظيمية، وفنية وبيئية كافية لتلبية متطلبات حماية المعلومات. ➢ على لجنة مواجهة الكوارث واستمرارية العمل توفير منهج كامل لاستمرارية العمل وبما يتماشى مع نتائج تحليل استمرارية العمل وتقييم المخاطر. ➢ ينبغي حفظ نسخ من خطط استمرارية العمل والوثائق الأخرى ذات الصلة في موقع بعيد وعلى مسافة كافية لتجنبيها أي تلف من أية كوارث قد تلحق بالموقع الرئيسي. وعلى لجنة مواجهة الكوارث واستمرارية العمل ضمان تحديث هذه النسخ وتزويدها بمستويات من الحماية بنفس مستوى الحماية المطبقة في الموقع الرئيسي. ➢ يجب تحديد العناصر التي تعتبر حيوية لاستمرارية الخدمة، وأن تتضمن خطط استمرارية العمل ترتيبات لإتاحة استئناف الخدمات بسرعة في حالة حدوث عطل. وفيما يلي بعض هذه التدابير: • توفير إمدادات احتياطية للطاقة الكهربائية. • ازدواجية المُعالجات والتخزين على الإنترنت (online). • توجيه تلقائي للاتصالات. • التحول إلى خدمات مشغل بديل للإنترنت. • ازدواجية مراكز عمليات الشبكة. • صيانة بموجب عقد لضمان تنفيذ عمليات الإصلاح دون تأخير. ➢ على لجنة مواجهة الكوارث واستمرارية العمل مراجعة خطط استمرارية العمل وتحديثها كل عام. ➢ ينبغي تطوير خطط استمرارية العمل لإدامة أو استعادة عمليات العمل ضمن المدة الزمنية المطلوبة، وذلك في أعقاب تعطل إجراءات العمل الهامة أو إخفاقها كليا. وعلى إجراءات التخطيط لاستمرارية العمل مراعاة ما يلي : • تحديد كافة مسئوليات وإجراءات الطوارئ والاتفاق عليها. • تحديد الحد المقبول لخسارة المعلومات والخدمات. • تطبيق إجراءات الطوارئ للسماح بالاستعادة والاسترجاع ضمن المدى الزمني المطلوب. ويبغي إعطاء عناية خاصة للأطراف الخارجية التي يعتمد عليها العمل والعقود، كموردي الأجهزة وعقود الصيانة.

الهدف من السياسة	محور السياسة
	• توثيق واضح ودقيق لكافة الإجراءات والعمليات المتفق عليها. • التدريب المناسب للموظفين على إجراءات وعمليات الطوارئ المتفق عليها، بما في ذلك إدارة الأزمات. • اختبار وتحديث الخطط . ➢ تعمل خطط استمرارية العمل على تناول نقاط الضعف في الجامعة، وبالتالي فإنها قد تتضمن معلومات حساسة تتطلب توفير حماية ملائمة. ➢ تقوم لجنة مواجهة الكوارث واستمرارية العمل بتوفير إطار عمل منفرد لخطط استمرارية العمل لضمان توافق وانسجام كافة خطط استمرارية العمل مع بعضها بحيث يمكن وضع الأولويات المتعلقة بالاختبار والصيانة وحماية المعلومات. ➢ على إطار خطط استمرارية العمل في الجامعة أن يتضمن ما يلي: • الظروف اللازم توافرها لتفعيل الخطط (على سبيل المثال : كيفية تقييم الموقف، من هي الأطراف المشاركة) قبل تفعيل كل خطة من هذه الخطط. • إجراءات الطوارئ التي توضح الإجراءات الفورية التي ينبغي اتخاذها في أعقاب وقوع حادثة تمثل خطرا على إجراءات العمل و/أو الحياة البشرية. وينبغي لهذه الإجراءات أن تتضمن ترتيبات للتعامل مع الوسائط (للحد من/ تقليص الخسائر) والاتصال الفعال مع الهيئات العامة (كالشرطة، الدفاع المدني، والجهات الأمنية ذات الاختصاص). • إجراءات توفير البدائل (Fallback) بهدف نقل أنشطة العمل أو خدمات الدعم إلى مواقع مؤقتة والعمل على إعادة تشغيل إجراءات العمل ضمن الوقت الزمني المحدد. • إجراءات استئناف عمليات العمل الاعتيادية. • جدول الصيانة والذي يوضح كيفية ومتى يتم اختبار الخطة، وإجراءات صيانتها. • يعتبر تدريب الأفراد على استمرارية العمل ضروريا للاستئناف الفعال للعمليات واستعادتها. • مسئوليات الأفراد، بحيث يتم توضيح من يكون مسئولا عن أي جزئية من الخطة. وينبغي ترشيح بدلاء حسب الحاجة، بالإضافة إلى توفير معلومات الاتصال كأرقام الهواتف وعناوين هؤلاء الأفراد. • الأصول الحيوية والموارد اللازمة لتنفيذ إجراءات الطوارئ والبدائل واستئناف العمل. • يتولى مالك العمل (المسئول عن العمل) ذي العلاقة مسئولية إجراءات الطوارئ ، خطط التحول اليدوي للبدائل، وخطط الاستئناف . ➢ ينبغي القيام باختبار خطط استمرارية العمل بصورة منتظمة وذلك لضمان أن أعضاء فريق الاستعادة والموظفين الآخرين ذوي العلاقة على دراية بالخطط. ويجب أن يعمل الجدول الزمني لاختبار خطط استمرارية على

الهدف من السياسة	محور السياسة
	توضيح كيفية ومتى يتم اختبار كل جزئية من الخطة. ➢ ينبغي لخطة استمرارية العمل أن تعتمد على استخدام أساليب مختلفة بهدف توفير ضمانات بأن الخطة (الخطط) سوف تعمل في الواقع. وفما يلي بعض هذه الأساليب : • اختبار سطح الطاولة (Table-top) بخصوص كافة السيناريوهات (مناقشة ترتيبات استعادة العمل باستخدام أمثلة على تعطل الخدمة). • المحاكاة (وعلى وجه الخصوص لتدريب الأفراد على الأدوار المعينة لكل منهم في أعقاب وقوع حادثة / كارثة). • اختبار الاستعادة الفنية (ضمان إمكانية استعادة نظم المعلومات بفعالية). • اختبار الاستعادة في موقع بديل (تشغيل إجراءات العمل بالتوازي مع عمليات الاستعادة بعيدا عن الموقع الرئيسي). • اختبار مرافق وخدمات المورّدين (ضمان أن الخدمات والمنتجات المقدمة من قبل جهات خارجية سوف تلبي الالتزامات التعاقدية). • إجراء تجربة متكاملة (التأكد من أنه يمكن لموظفي ، ومعدات، ومرافق، وعمليات الجامعة مواجهة الأعطال). ➢ ينبغي تدوين نتائج اختبارات استمرارية العمل واتخاذ الإجراءات الكفيلة بتحسين الخطط عند الضرورة. ➢ تعتبر عملية الإبلاغ عن وضعية التخطيط لاستمرارية العمل والتطورات عليها من العناصر الهامة لاستحداث برنامج فعال لاستمرارية العمل في الجامعة. ويتوجب على إدارة أمن المعلومات إفادة قطاعات - ادارات واقسام الجامعة عن ذلك كل ستة شهور أو في أعقاب تنفيذ كل اختبار من اختبارات استمرارية العمل.

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.