سياسة أمن المعلومات

في

الجامعة الإسلامية

بالمدينة المنورة

١٤٤٣ هـ

جدول المحتويات

١. مقدمة ٢

٢. تحديد هيكل السياسة ٢

٣. سياسات أمن المعلومات ٣

٣,١ سياسة أمن معلومات الجامعة الإسلامية بالمدينة المنورة ٣
٣,٢ التوعية بأمن المعلومات ٧
٣,٣ سياسة إدارة الوصول المنطقي ١٠
٣,٤ الحماية من الشفرات الخبيثة ١٧
٣,٥ الاستخدام المقبول لأنظمة المعلومات ٢١
٣,٦ التعامل مع الوسائط الإلكترونية ٢٦
٣,٧ أمن الوثائق ٢٩
٣,٨ الغش والتبليغ عن المخالفات ٣١
٣,٩ إدارة حوادث أمن المعلومات ٣٤
٣,١٠ أمن الموظفين ٣٧
٣,١١ إدارة أصول المعلومات ٤٠
٣,١٢ إدارة مخاطر أمن المعلومات ٤٣
٣,١٣ إدارة سياسات أمن المعلومات ٤٥
٣,١٤ الأمن المادي والبيئي ٤٧
٣,١٥ النسخ الاحتياطية والاسترجاع في حالة الكوارث ٥١
٣,١٦ شراء وتطوير أنظمة المعلومات ٥٤
٣,١٧ إدارة التغيير ٥٨
٣,١٨ مراقبة أمن المعلومات ٦١
٣,١٩ الالتزام بالسياسات والإجراءات المحددة ٦٤
٣,٢٠ إدارة الخدمات المقدمة من طرف ثالث ٦٦
٣,٢١ إدارة استمرارية النشاط ٦٨

مقدمة

تقدم هذه الوثيقة سياسات أمن المعلومات الخاصة بالجامعة الإسلامية بالمدينة المنورة. وقد أعدت الوثيقة مع الأخذ بعين الاعتبار المعايير الدولية لأمن المعلومات وأفضل الممارسات المطبقة بهذا الصدد.

تنطبق هذه السياسة على جميع الموظفين، والطلاب، والموردين، وشركاء العمل، وموظفي المقاولين، والوحدات الوظيفية لدى الجامعة الإسلامية بالمدينة المنورة سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.

في حال تعذر على أي شخص فهم أي جزء من هذه الوثيقة، فعليه استشارة إدارة أمن المعومات لدى عمادة تقنية المعلومات في الجامعة الإسلامية بالمدينة المنورة.

١. تحديد هيكل السياسة

تشتمل وثيقة السياسة على العناصر التالية:

- **الغرض**: وصف موجز للغرض من السياسة.
- **مجال تطبيق السياسة**: تحدد الإدارات والجهات المختلفة الداخلية والخارجية وكذلك الأشخاص الذين تنطبق عليهم هذه السياسة.
- **المسئول التنفيذي**: تحديد الشخص الذي يضطلع بالصلاحية والمسئولية النهائية عن أي تغييرات أو تحديثات تجري على السياسة. يجب اعتماد أي تغييرات أو تحديثات على السياسة من قبل المسئول التنفيذي عن السياسة.
- **راعي وثيقة السياسة**: الشخص المسئول عن إبقاء وحفظ السياسة وتبليغها وتحديثها بناءً على توجيهات المسئول التنفيذي عن السياسة.
- **إلزامية التنفيذ**: تحدد تبعات ونتائج أية مخالفة لهذه السياسة.
- **قيود سياسة أمن المعلومات**: يشتمل هذا القسم وصف لجزئية القيود/الضوابط المتعلقة بالسياسة المحددة.
- **تاريخ نفاذ السياسة**: يحدد هذا القسم التاريخ الذي يسري فيه تطبيق السياسة، ومتى يجب إتباعها.

٢. سياسات أمن المعلومات

٢,١ سياسة أمن معلومات الجامعة الإسلامية بالمدينة المنورة

٢,١,١ الغرض

الغرض من هذه السياسة هو تأكيد وبيان التزام إدارة الجامعة ونيتها دعم أهداف ومبادئ امن المعلومات بما يتوافق مع إجراءات العمل الموجودة في الجامعة وعرض الأهداف الرئيسية لتأسيس ضوابط لأمن المعلومات مبنية على المخاطر التي قد تتعرض لها الجامعة الإسلامية بالمدينة المنورة.

٢,١,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.

٢,١,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة، فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١,٦ قيود سياسة أمن المعلومات

٢,١,٦,١ الأهداف الرئيسية لأمن المعلومات لدى الجامعة الإسلامية بالمدينة المنورة

٢,١,٦,١,١ تعتبر الجامعة الإسلامية أمن المعلومات هدفاً رئيسياً من أهداف العمل لديها.

٢,١,٦,١,٢ تلتزم إدارة ومنسوبو الجامعة الإسلامية بالمدينة المنورة بالتقيد الصارم لسياسات وممارسات أمن المعومات لديها. وينبغي على جميع منسوبي الجامعة والأطراف الثالثة ذات العلاقة الالتزام بسياسات وإجراءات ومعايير أمن المعلومات.

٢,١,٦,١,٣ تؤدي مخالفة سياسات وإجراءات ومعايير أمن المعلومات إلى إجراءات تأديبية من قبل الإدارة قد تصل إلى إنهاء الخدمات وفقاً لأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر – نظام العمل والعمال، ونظام مكافحة جرائم المعلومات، ونظام التعاملات الإلكترونية، وغيرها.

٢,١,٦,١,٤ يجب أن يقتصر استخدام أنظمة المعلومات لدى الجامعة على أغراض العمل المصرح بها فقط، وعلى موظفين محدودين وفقاً لسياسة الاستخدام المقبول لأنظمة المعلومات.

٢,١,٦,١,٥ يتعين على الجامعة أن تتأكد من تكوين وعي كاف بأمن المعلومات بين الإدارة والموظفين والطلاب والأطراف الثالثة ذات العلاقة وذلك وفقاً لمتطلبات الوعي المحددة الخاصة بهم.

٢,١,٦,١,٦ ينبغي أن يتم التحكم على نحو كاف بالوصول الآلي و الفعلي إلى أنظمة المعلومات لدى الجامعة، وذلك وفقاً للمخاطر التي تنطوي عليها تلك الأنظمة ومدى حساسيتها للجهه.

٢,١,٦,١,٧ يجب حماية أنظمة المعلومات لدى الجامعة من الهجمات البرمجية الخبيثة (مثل الفيروسات، الديدان، أحصنة طروادة "التروجانات"، قنابل البريد الإلكتروني، إلخ).

٢,١,٦,١,٨ على الجامعة أن تتأكد من أنه يتم اكتشاف وضبط وإدارة المخاطر التي تتعرض لها أنظمة المعلومات من الأطراف الثالثة.

٢,١,٦,١,٩ على الجامعة أن تتأكد من توفير الأمن لمعلومات عملائها على نحو كاف، كما أن عليها أن تستخدم تدابير وحلول أمنية كافية للتعامل مع المخاطر الناشئة عن وصول عملائها إلى أنظمة المعلومات لديها.

٢,١,٦,١,١٠ يجب حماية وسائط مناولة المعلومات مثل (منافذ USB والأقراص الصلبة المتنقلة) من التلف وسرقة المعلومات والدخول غير المصرح به إليها.

٢,١,٦,١,١١ يجب التبليغ ومتابعة والتحري عن جميع حوادث أمن المعلومات ونقاط الضعف في الأنظمة الأمنية لدى الجامعة ومعالجتها بشكل فاعل.

٢,١,٦,١,١٢ يتوجب على الجامعة أن تتأكد من تحديد جميع أنظمة المعلومات لديها وتعيينها إلى مسئولي أنظمة المعلومات الذين يضطلعون بالمسئولية النهائية عن أمن المعلومات في أنظمة المعلومات التابعة لهم.

٢,١,٦,١,١٣ يتوجب على الجامعة أن تصنف أنظمة المعلومات لديها بناءً على درجة أهميتها في دعم أهداف الجامعة وأثرها على الجامعة في حالة انتهاك سرية أو تكامل أو توافر أنظمة المعلومات.

٢,١,٦,١,١٤ يجب تحديد وتصنيف الوثائق الحساسة لدى الجامعة وحمايتها على نحو كاف من التلف والسرقة والوصول غير المصرح به إليها.

٢,١,٦,١,١٥ يجب أن تضمن الجامعة سرية المعلومات الشخصية في أنظمتها المعلوماتية بما يتوافق مع احتياجاتها الأمنية والأنظمة واللوائح المتعلقة بهذا الصدد.

٢,١,٦,١,١٦ يجب على الجامعة تحديد وتطبيق والحفاظ على ضوابط أمن معلومات كافية لأنظمة المعلومات لديها بما يتواكب مع تصنيف المخاطر وأفضل الممارسات المطبقة بهذا الخصوص.

٢,١,٦,١,١٧ يجب أن تحد الجامعة من فرص الإساءة، أو سوء الاستخدام، أو تدمير أنظمتها المعلوماتية وذلك من خلال التأكد من نزاهة الموظفين الحاصلين على إمكانية الدخول إلى أنظمة المعلومات.

٢,١,٦,١,١٨ يجب أن تقوم الجامعة بالعمل على التوافق مع جميع الأنظمة واللوائح السعودية (والعالمية إذا كان ضرورياً) التي تنطبق على أنظمة المعلومات.

٢,١,٦,١,١٩ يتعين على الجامعة الأخذ في اعتبارها بشكل استباقي متطلبات أمن المعلومات أثناء مرحلة شراء/تطوير أنظمة المعلومات بما يتوافق مع سياسات وإجراءات ومعايير أمن المعلومات لديها، وأفضل الممارسات المتبعة بهذا الصدد.

٢,١,٦,١,٢٠ ينبغي أن يتم التحكم بالتغييرات التي تتم على أنظمة المعلومات الرئيسية من خلال سياسة إدارة التغيير للحد من أثر الحوادث المتعلقة بالتغيير في أنظمة المعلومات.

٢,١,٦,١,٢١ يتم مراقبة حالة أمن المعلومات ضمن أنظمة المعلومات التابعة للجامعة من خلال تخطيط ونشر أساليب كافية لمراقبة أمن المعلومات بما يتواكب مع المخاطر ذات العلاقة ومدى حساسية أنظمة المعلومات.

٢,١,٦,١,٢٢ على الجامعة أن تقوم بتقييم أمن المعلومات الخاص بأنظمتها المعلوماتية لتحديد نقاط الضعف والتهديدات والمخاطر التي تحيط بأمن المعلومات لديها، ومن ثم اتخاذ الإجراءات العلاجية المناسبة وبالسرعة الواجبة.

٢,١,٦,١,٢٣ يتعين على الجامعة أن تقوم بتخطيط وإجراء مراجعات وتدقيق مستقل لأمن المعلومات لديها بما يتوافق مع المخاطر ذات العلاقة وحساسية أنظمة المعلومات. ويتوجب عليها اتخاذ الإجراءات المناسبة وفي الأوقات الواجبة لمعالجة الملاحظات التي تم تحديدها أثناء عملية التدقيق والمراجعة.

٢,١,٦,١,٢٤ على الجامعة التأكد من حماية عملياتها وخدماتها الحساسة في الوقت المناسب من آثار الإخفاقات الرئيسية أو الكوارث لأنظمة المعلومات، وذلك من خلال خطة رسمية للحفاظ على استمرارية العمل واستمرارية توفر الخدمات و استخدام وحدات إضافية مسانده.

٢,١,٦,١,٢٥ يلتزم منسوبو الجامعة والأطراف الثالثة ذات العلاقة بتحديد والتبليغ عند ملاحظتهم لأي غش أو ممارسات أوأنشطة غير سليمة. كما تلتزم الجامعة بمنع النشاطات التي تنطوي على غش و تقوم باتخاذ إجراءات سريعة وفاعلة حيال تلك الحوادث المبلغ عنها.

٢,١,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتباراً من تاريخ (اعتمادها)

٢,٢ التوعية بأمن المعلومات

٢,٢,١ الغرض

الغرض من هذه السياسة هو تزويد المستخدمين لدى الجامعة.بالتوعية المناسبة فيما يتعلق بأمن المعلومات وبتهديدات أمن المعلومات، وسياسات وإجراءات ومعايير أمن المعلومات لدى الجامعة بناءً على الاحتياجات المحددة.

٢,٢,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.
يشمل مجال تطبيق هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٢,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,٢,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٢,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة، فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٢,٦ قيود سياسة أمن المعلومات

٢,٢,٦,١ برنامج التوعية

٢,٢,٦,١,١ يتعين على الجامعة نشر التوعية الفاعلة بأمن المعلومات بين منسوبيها والأطراف الثالثة ذات العلاقة وعملائها، وذلك من خلال تطوير خطة رسمية للتوعية الأمنية وفقاً لإجراءات تطوير برنامج التوعية بأمن المعلومات.

٢,٢,٦,١,٢ تساعد خطة التوعية الأمنية في التخطيط الفاعل لمبادرات أمن المعلومات لدى الحهه أو الجامعة.

٢,٢,٦,١,٣ يجب أن تحدد خطة التوعية بمخاطر أمن المعلومات الأطراف المستهدفة ورسائل أمن المعلومات التي سيتم تبليغها وقنوات الاتصال وجدول تنفيذ أنشطة التوعية بأمن المعلومات.

٢,٢,٦,١,٤ على عميد تقنية المعلومات ومدير إدارة أمن المعلومات الاضطلاع بمسؤولية تطوير وإعداد وتنفيذ وابقاء خطة التوعية بأمن المعلومات.

٢,٢,٦,١,٥ ينبغي على جميع منسوبي الجامعة والأطراف الثالثة إن احتاج الأمر أن يحضروا فعاليات وأنشطة التوعية المتعلقة بأمن المعلومات للتأكد من تحقيق مستوى مقبول من الالتزام الأمني بسياسات أمن المعلومات لدى الجامعة.

٢,٢,٦,١,٦ يجب أن يتم نشر نسخة محدثة من الوثائق الرسمية لسياسات وأحكام وشروط الخدمة وسياسات الخصوصية المتعلقة بأمن المعلومات لدى الجامعة، والتي يتم تطبيقها على العملاء والأطراف الخارجية. ينبغي نشر هذه الوثيقة في مكان واضح ومرئي ضمن الموقع الإلكتروني للجامعة.

٢,٢,٦,١,٧ ينبغي على الجامعة تطبيق إجراءات محددة وقابلة للقياس للتأكد من فهم العملاء والموظفين لمسئولياتهم والتزاماتهم نحو أمن المعلومات.

٢,٢,٦,٢ التوعية بمخاطر الخدمات المقدمة عبر الإنترنت

٢,٢,٦,٢,١ يجب تشجيع مستخدمي خدمات الإنترنت المقدمة من الجامعة على حماية أنظمة الحاسوب الخاصة بهم وأي أجهزة مستخدمين نهائيين أخرى لديهم و التي تستخدم لتنفيذ العمليات. و يجب تأمين هذه الحماية من خلال استخدام برامج أمنية متكاملة وحديثة وقابلة للتطبيق مثل برامج مكافحة الفيروسات، برامج مكافحة التجسس، برامج مكافحة الرسائل الاقتحامية، وتقنيات برامج الحماية (جدار الحماية).

٢,٢,٦,٢,٢ يجب أن تقدم الجامعة برنامجاً للتوعية الأمنية يهدف إلى تعليم عملاء الجامعة بشأن سرية أسم المستخدم وكلمة المرور الخاصة بكل عميل والتهديدات الأمنية والتدابير المضادة، خصوصاً فيما يتعلق بالعمليات التي تجرى عبر الإنترنت.

٢,٢,٦,٢,٣ كجزء من برنامج التوعية بأمن المعلومات الذي تقدمه الجامعة لموظفيها وعملائها، فإن على الجامعة أن ترفع من وعي موظفيها وعملائها بشأن عمليات الاصطياد الإلكتروني و طرق اعتراض البيانات وطرق الخداع الأخرى. كما يجب توعية الموظفين والعملاء بالدور المناط بهم في هذا الصدد (ويشمل ذلك التبليغ عن الأمر فوراً إلى الجامعة) إذا اشتبهوا بوجود مثل هذه الحوادث.

٢,٢,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,٣ سياسة إدارة الوصول المنطقي

٢,٣,١ الغرض

الغرض من هذه السياسة هو التحكم بالوصول المنطقي إلى أنظمة المعلومات لدى الجامعة مما يكفل دقة وسرية وتوفر المعلومات.

٢,٣,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٣,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,٣,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٣,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة، فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٣,٦ قيود سياسة أمن المعلومات

٢,٣,٦,١ التحكم بالوصول

٢,٣,٦,١,١ يجب أن يسمح لجميع المستخدمين لدى الجامعة بالوصول إلى أنظمة المعلومات والعمليات اللازمة لتأدية مهام أعمالهم فقط.

٢,٣,٦,١,٢ يجب ضبط إعدادات الوصول لأنظمة المعلومات عند تطبيق و إعداد الأنظمة و ذلك باستخدام خاصية مجموعات المستخدمين والتي تحدد امتيازات الوصول لكل مجموعه و يجب أن لا يتم تعيين امتيازات وصول مستقلة للمستخدمين الأفراد، وإنما يتم منحهم إمكانية الوصول من خلال عضويتهم في مجموعات المستخدمين المحددة مسبقاً.

٢,٣,٦,١,٣ على كل مستخدم من مستخدمي أنظمة المعلومات الحصول على تفويض من المسئول عن نظام المعلومات كي يتسنى له الدخول إلى أنظمة معلومات الجامعة.

٢,٣,٦,١,٤ يسمح بالدخول إلى أنظمة المعلومات وتفعيل حسابات المستخدمين لكل من الموظفين، المقاولين، الاستشاريين، العاملين المؤقتين، أو موظفي الموردين في حالة قيام الشخص بتأدية الخدمات لمصلحة الجامعة فقط. (فضلاً راجع القسم الفرعي بعنوان "وصول الأطراف الثالثة إلى أنظمة معلومات الجامعة ضمن هذه السياسة للاطلاع على المزيد من الضوابط الواجب إتباعها عند منح إمكانية الدخول إلى الأطراف الثالثة).

٢,٣,٦,٢ اسم المستخدم وكلمة المرور

٢,٣,٦,٢,١ يجب أن يتم تخزين وتوزيع كافة أسماء المستخدمين وكلمات المرور إلى الأنظمة بشكل آمن.

٢,٣,٦,٢,٢ يجب أن يكون لكل مستخدم من مستخدمي أي نظام معلوماتي اسم مستخدم فريد وكلمة مرور خاصة به.

٢,٣,٦,٢,٣ يجب عدم استخدام أسماء المستخدمين المشتركة و الأسماء الشائعة و العامة.

٢,٣,٦,٢,٤ لا يسمح للمستخدم بمشاركة اسم المستخدم وكلمة المرور الخاصين به مع أشخاص آخرين تحت أي ظرف من الظروف. وعلى المستخدم أن يتحمل المسؤولية المباشرة كاملة عن كافة الأنشطة التي تتم من خلال حساب المستخدم الخاص به على أي من الأنظمة المسموح له استخدامها.

٢,٣,٦,٢,٥ يجب عدم إعادة إصدار نفس اسم المستخدم لمستخدمين آخرين.

٢,٣,٦,٢,٦ يجب أن تكون معايير تحديد اسم المستخدم لا تعطي أي انطباع حول مستوى المستخدم أو امتيازاته أو حقوق الدخول التي يتمتع بها، مثل (verifier) أو (Releaser).

٢,٣,٦,٢,٧ ينبغي على جميع المستخدمين بمن فيهم مدراء الأنظمة الالتزام بالأحكام والشروط المتعلقة باستخدام وإدارة كلمات المرور الخاصة بهم، ويجب تطبيق المعايير التالية من قبل كل نظام:

- أدنى طول مسموح به لكلمة المرور يتكون من (١٠ خانات).
- تشتمل كلمة المرور (بحد أدنى على رقم واحد، مع حرف هجائي واحد، واستخدام أحرف كبيره وصغيره ورمز واحد إن سمحت اعدادت النظام باستخدام الرموز).
- تاريخ كلمة المرور (آخر أربع كلمات مرور).
- انتهاء صلاحية كلمة المرور (مع أول تسجيل دخول باستخدام كلمة المرور، وبعد ذلك بحد أقصى لمدة ١٨٠ يوماً منذ آخر تغيير لكلمة المرور) وينصح أن يتم تغييرها كل ٩٠ يوم.
- يتم الاستخدام لمرة واحدة فقط لكلمة المرور الأولية، وبعد ذلك يقوم نظام المعلومات بإجبار المستخدم على تغيير كلمة المرور في أول تسجيل دخول.
- يتم تطبيق تشفير كلمة المرور.
- لا يتم عرض كلمة المرور في الحقل المخصص لإدخال كلمة المرور.
- عند استحداث حساب لمستخدم، يجب أن يتم إصدار كلمة مرور عشوائية لاستخدامها في تسجيل الدخول لأول مرة فقط، ويجوز إبلاغ المستخدم بها شفوياً.
- تعتبر المعايير السابقة هي الحد الأدنى الذي يجب تطبيقه ولكن يمكن أن يتم تطبيق معايير أشد صرامة بناء على حساسية الأنظمة المستخدمة.

٢,٣,٦,٢,٨ يجب تحديد ميزات حجب اسم المستخدم وانتهاء صلاحية كلمة المرور بناءً على متطلبات النظام، وتصنيفه، وأهميته (كونه من الأنظمة الحرجة) ، والآثار الجانبية في حال الانتهاك.

٢,٣,٦,٣ إدارة امتيازات الدخول للأنظمة

٢,٣,٦,٣,١ يجب حصر جميع الحسابات ذات المزايا العالية (مثل حسابات مدراء الأنظمة أو الحسابات الأساسية (root accounts)). على عدد قليل من الأشخاص المصرح لهم باستخدام هذه الحسابات.

٢,٣,٦,٣,٢ يجب عدم منح أي امتيازات لحسابات مستخدمي تقنية المعلومات كمدير نظام محلي أو بعيد أو مدير نطاق إلا في حال وجود مبرر لذلك.

٢,٣,٦,٣,٣ يجب إتباع مبدأ الفصل في الامتيازات عند تعيين امتيازات الوصول لأنظمة المعلومات لمستخدمي تقنية المعلومات.

٢,٣,٦,٣,٤ يجب عدم منح موظفي عمليات تقنية المعلومات إمكانية الوصول إلى بيئة تطوير الأنظمة.

٢,٣,٦,٣,٥ يجب عدم منح موظفي تطوير الأنظمة إمكانية الوصول إلى بيئة عمليات تقنية المعلومات.

٢,٣,٦,٣,٦ عندما يتعذر الفصل في المهام أو عندما لا يكون ذلك ممكناً من الناحية العملية، يجب أن تتضمن العملية ضوابط تعويضية مثل مراقبة الأنشطة، إبقاء ومراجعة سجل الفحص والمراجعة audit trail والإشراف الإداري.

٢,٣,٦,٤ تغيير وصول المستخدم

٢,٣,٦,٤,١ يجب التأكد من أنه يتم الإلغاء الفوريً لجميع حسابات المستخدمين بمجرد إنهاء أو انتهاء عقودهم، أو تغيير وظائفهم، أو عندما لم يعد لمستخدم معين حاجة عملية للوصول إلى نظام المعلومات.

٢,٣,٦,٤,٢ في حالة انتهاء أو إنهاء عقد الموظف أو انتقاله، يجب على إدارة شؤون هيئة التدريس والموظفين أن تقوم فوراً بإشعار عمادة تقنية المعلومات من خلال البريد الإلكتروني وتزويدهم بتفاصيل قرار تغيير الوظيفة أو الانتقال وتاريخ النفاذ.

- في حالة إنهاء أو انتهاء عقد الموظف، يتم إيقاف وصول ذلك الموظف إلى أنظمة المعلومات إلا إذا تمت الموافقة على طلب التمديد المؤقت لوصول الموظف المعني إلى الأنظمة وحُدّد تاريخ لاحق لإيقاف ذلك الوصول. و يجب الانتظار حتى يحين الموعد/ التاريخ المحدد قبل أن يوقف وصول المستخدم إلى الأنظمة.
- في حال إعطاء الموظف المنتهي عقده الموافقة على استخدام بريده الإلكتروني الخاص بالجامعة فإنه يتم إعداد حساب المستخدم بحيث لا يملك أي صلاحيات أخرى.
- في حال انتقال الموظف، يتم إزالة جميع إمكانيات الوصول الحالية للموظف، ومن ثم يحدد الوصول الجديد وفقاً للوظيفة الجديدة.

٢,٣,٦,٥ مراجعة حقوق وصول المستخدم

٢,٣,٦,٥,١ تقوم الجامعة بإجراء مراجعة دورية تتعلق بالمخاطر المترتبة عن حقوق وصول المستخدمين للأنظمة.

٢,٣,٦,٥,٢ يتأكد مسئول أمن المعلومات من أن جميع حقوق وصول المستخدمين قد تمت مراجعتها من قبل المسئولين عن الأنظمة المعلوماتية للتأكد من:

- مطابقتها لأوصاف وظائف المستخدمين.

- الاستمرار في الحفاظ على متطلبات الفصل بين المهام.
- الاستمرار في إتباع مبدأ "الحاجة إلى المعرفة"

٢,٣,٦,٥,٣ ينبغي على مدراء الأنظمة إجراء مراجعات دورية للنظام لاكتشاف الحسابات غير المستخدمة، حيث يتعين تعطيل تلك الحسابات ومن ثم إزالتها من النظام.

٢,٣,٦,٥,٤ عند اكتشاف أي سوء استخدام لحقوق الوصول المميزة، فإن على مدير النظام تقييد تلك الامتيازات وإشعار مسئول أمن المعلومات لاتخاذ الإجراء اللازم حيال ذلك.

٢,٣,٦,٦ سياسة المكتب النظيف والشاشة النظيفة

٢,٣,٦,٦,١ يجب عدم ترك أجهزة الحاسوب المحولة وأجهزة سطح المكتب ووحدات الحاسوب الطرفية والطابعات مفتوحة في حالة عدم التواجد بجوارها، وإنما يجب تحصينها بشاشات محمية بكلمات مرور .

٢,٣,٦,٦,٢ يجب تحصين أجهزة تصوير المستندات وأجهزة الفاكس بكلمات مرور.

٢,٣,٦,٦,٣ يجب رفع المعلومات الحساسة والمصنفة عند طباعتها فوراً من الطابعات.

٢,٣,٦,٧ وصول الأطراف الثالثة إلى أنظمة معلومات الجامعة

٢,٣,٦,٧,١ على مدير إدارة أمن المعلومات إجراء تقييم لتحديد المخاطر المحتملة لأنظمة المعلومات لدى الجامعة، والناشئة عن وصول أطراف أخرى إليها.

٢,٣,٦,٧,٢ يجب الأخذ بعين الاعتبار أن يتضمن التقييم المذكور المعايير التالية:

- نوع ومستوى الوصول الذي سيتم منحه للطرف الآخر.
- تصنيف مخاطر أنظمة المعلومات التي سيتم السماح بالوصول إليها.
- الأسباب التي على أساسها يتم منح الوصول لأنظمة المعلومات.
- المعلومات المرجعية عن الطرف الآخر.
- توفر وفاعلية الضوابط الواجب تطبيقها لتنظيم ومراقبة وصول الطرف الآخر.

٢,٣,٦,٧,٣ يتم منح إمكانية وصول الطرف الآخر لأنظمة المعلومات لدى الجامعة بناءً على عقد رسمي بين الجامعة و الطرف المذكور.

٢,٣,٦,٧,٤ يجب أن يتضمن العقد الشروط التالية كحد أدنى:

- الشروط والأحكام التي يتم منح الوصول بموجبها.
- مستوى الأمن الطبيعي والمنطقي الذي سيقدمه (الطرف الثالث) للحفاظ على سرية وتكامل وسلامة معلومات/ بيانات الجامعة التي يتم معالجتها.
- مسؤوليات موظفي المقاولين أو الاستشاريين أو الموردين.

٢,٣,٦,٧,٥ يجب الحصول على تصريح لوصول جميع موظفي الطرف الثالث إلى أنظمة المعلومات لدى الجامعة من قبل مدراء الإدارات المعنية. يجب أن يتضمن التصريح إيضاح مبررات الوصول وفترة الوصول المطلوبة و قائمة أنظمة المعلومات التي سيتم منح الوصول إليها والمعلومات الأخرى المرتطة بذلك. وعلى مدير أمن المعلومات مراجعة الطلب قبل تنفيذه.

٢,٣,٦,٧,٦ يجب أن يتم تحديد تاريخ انتهاء لاسم المستخدم لموظفي المقاول والاستشاري وجميع موظفي الطرف الثالث الآخرين مع مراعاة أن لا يتجاوز تاريخ انتهاء المشروع المتعاقد عليه.

٢,٣,٦,٨ الوصول عن بعد

٢,٣,٦,٨,١ يمنح الوصول عن بعد لشبكة الجامعة باستخدام إجراءات تسجيل دخول المستخدمين.

٢,٣,٦,٨,٢ يمنح الوصول عن بعد على أساس الحاجة ولأغراض العمل فقط.

٢,٣,٦,٨,٣ تمنح الجامعة إمكانية الوصول عن بعد فقط للاحتياجات التشغيلية الضرورية وتوثق مبررات هذا الوصول.

٢,٣,٦,٨,٤ يجب على المستخدمين الحاصلين على إمكانية الوصول عن بعد التأكد من أن أجهزة الحاسب الآلي أو محطة العمل المملوكة من قبل الجامعة أو الشخصية، الموصولة عن بعد مع شبكة الجامعة تتصف بما يلي:

- غير موصولة مع أية شبكة أخرى في نفس الوقت باستثناء الشبكات الشخصية الخاضعة للسيطرة الكاملة من قبل ذلك المستخدم.
- تتضمن أحدث برامج مكافحة الفيروسات والتجسس والجدار الحماية.

٢,٣,٦,٨,٥ يجب أن تتحكم الجامعة بجميع حالات الوصول عن بعد عبر عدد محدود من النقاط المدارة للتحكم بالوصول.

٢,٣,٦,٨,٦ يتحمل المستخدم المسئولية عن أن أية تبعات أو آثار سلبية ناشئة عن إساءة استخدام الوصول.

٢,٣,٦,٨,٧ يجب أن يتم اعتماد جميع وصلات الدخول عن بعد من قبل إدارة أمن المعلومات.

٢,٣,٦,٨,٨ يجب تسجيل كافة أنشطة الدخول عن بعد بما في ذلك عنوان بروتوكول الإنترنت واسم المستخدم الخاص بالدخول.

٢,٣,٦,٨,٩ يجب مراقبة النشاطات المجراة عبر الحساب. في حالة عدم استخدام الحساب لمدة ثلاثة أشهر يجب إنهاؤه وإيقافه. وإذا تم طلب الوصول مرة أخرى، فعلى المستخدم أن يطلب حساباً جديداً.

٢,٣,٦,٨,١٠ يجب أن يكون للوصول عن بعد آليات قوية للتحقق من الهوية مثل التحقق باستخدام كلمة مرور تستخدم لمرة واحدة أو مفاتيح عامة/ خاصة مع مقاطع قوية لكلمة المرور.

٢,٣,٦,٨,١١ يجب عدم منح الأطراف الثالثة إمكانية الوصول عن بعد إلى أنظمة معلومات الجامعة إلا إذا كان هناك مبرر عملي قوي لذلك. وإذا ما تم منح الغير إمكانية الوصول عن بعد إلى أنظمة / شبكات معلومات الجامعة، يجب مراعاة ما يلي:

- أن يكون دخول الغير محدوداً فقط على شبكة / نظام معلومات محدد مطلوب لتأدية المسئوليات المناطة بتلك الأطراف.
- أن تتم مراقبة سجلات وأنشطة الوصول عن كثب من قبل إدارة أمن المعلومات.

٢,٣,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,٤ الحماية من الشفرات الخبيثة

٢,٤,١ الغرض

الغرض من هذه السياسة هو حماية أنظمة المعلومات لدى الجامعة من البرامج الخبيثة (مثل الفيروسات، ديدان الحاسب الآلي، أحصنة طروادة، قنابل البريد الإلكتروني، إلخ).

٢,٤,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٤,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,٤,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٤,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة، فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٤,٦ قيود سياسة أمن المعلومات

٢,٤,٦,١ استخدام حلول مكافحة الفيروسات المتعارف عليها دولياً

٢,٤,٦,١,١ يجب أن يكون لدى الجامعة آلية محددة وواضحة للكشف عن الفيروسات والشفرات الخبيثة ومنعها وعلاج واستعادة الأنظمة المصابة بطريقة مناسبة وبالسرعة الواجبة.

٢,٤,٦,١,٢ يجب أن يكون لدى الجامعة برنامج مكافحة فيروسات متعارف عليه دولياً ومدار لديها بصورة مركزية ومركب ومفعّل في جميع الأوقات في كافة أنظمتها المعلوماتية، وكذلك في الأنظمة أو البنية التحتية الخاصة بأطراف أخرى والموصولة مع شبكة الجامعة.

٢,٤,٦,٢ اكتشاف ومنع الفيروسات / الشفرات الخبيثة من التأثير على أنظمة المعلومات لدى الجامعة.

٢,٤,٦,٢,١ يجب أن يتم فحص كافة الأجهزة المملوكة وغير المملوكة من قبل الجامعة للفيروسات/ الشفرات الخبيثة قبل وصلها مع شبكة الجامعة.

٢,٤,٦,٢,٢ يجب تطبيق تقنية مكافحة الفيروسات في النقاط التي يمكن للفيروس/ الشفرة الخبيثة أن تدخل منها إلى شبكة الجامعة.

٢,٤,٦,٢,٣ يجب نشر تعريفات وتحديثات برامج مكافحة الفيروسات عبر وسائل آلية بشكل يومي أو بمجرد حدوثها.

٢,٤,٦,٢,٤ يجب إعداد أنظمة المعلومات بحيث تمنع المستخدمين من تعطيل عمل أدوات مكافحة الفيروسات.

٢,٤,٦,٢,٥ يجب أن تشتمل برامج الحماية من الفيروسات/ الشفرات الخبيثة على آلية التثبيت/ التركيب الإلزامي لبرامج مكافحة الفيروسات في أي أنظمة معلومات (أجهزة الحاسب الآلي ، الخادم، أجهزة الاتصالات المتنقلة، إلخ) موصولة مع شبكة الجامعة، إذا لم تكن مثبتة فعلياً فيها.

٢,٤,٦,٢,٦ يتم تطبيق التدابير الفنية التالية:

- يجب أن يتم- إعداد- برنامج مكافحة الفيروسات للتأكد بأن عميل مكافحة الفيروسات (agent) يعمل في جميع الأوقات على أجهزة المستخدمين (أجهزة سطح المكتب، أجهزة الحاسب الآلي المحمول، أجهزة الاتصالات المتنقلة، إلخ) وذلك من خلال كشف حالة العميل كل ٥ دقائق. وإذا تم اكتشاف تعذر الوصول إلى العميل (agent) فيما كان يمكن الوصول إلى أجهزة المستخدمين (أجهزة سطح المكتب، أجهزة الحاسب الآلي المحمول، أجهزة الاتصالات المتنقلة، إلخ)، فإن ذلك يعني أن عميل مكافحة الفيروسات لا يعمل.
- يجب أن يقوم خادم مكافحة الفيروسات بإغلاق كافة منافذ الدخول إلى الشبكة (أجهزة سطح المكتب، أجهزة الحاسب الآلي المحمول، أجهزة الاتصالات المتنقلة، إلخ) إلى أن يعمل العميل مرة أخرى.
- يجب أن يتم مسح الأجهزة بشكل أسبوعي آليا وفي أوقات محددة

٢,٤,٦,٢,٧ يتم ضبط إعدادات برنامج مكافحة الفيروسات لفحص كافة سواقات الوسائط القابلة للإزالة وذاكرات الفلاش الموصولة مع أنظمة المعلومات.

٢,٤,٦,٢,٨ يتم فحص مرفقات البريد الإلكتروني أو الملفات المشتركة المجهولة الهوية للتأكد من خلوها من الفيروسات/ الشفرات الخبيثة قبل فتحها أو الدخول إليها.

٢,٤,٦,٢,٩ يتم ضبط إعدادات برنامج الحماية من الفيروسات/ الشفرات الخبيثة بحيث يقوم بإجراء فحص آلي بشكل دوري لجميع أجهزة الحاسوب، والخوادم، والأجهزة المحمولة وجميع المكونات الأخرى للبنية الهيكلية لأنظمة المعلومات على فترات منتظمة، للكشف عن احتمالات وجود أي فيروسات/ شفرات خبيثة.

٢,٤,٦,٢,١٠ يتم ضبط إعدادات سجل الدخول إلى برنامج مكافحة الفيروسات بحيث يتم رصد أقصى حد ممكن من التفاصيل. ويجب عدم السماح بالحذف النهائي لتلك السجلات.

٢,٤,٦,٢,١١ يتم عمل نسخ احتياطية من سجلات مكافحة الفيروسات، كي يتم توفيرها لأي تحريات مطلوبة في حالة وجود أية حوادث هجمات للفيروسات/ الشفرات الخبيثة.

٢,٤,٦,٢,١٢ يكون مدير إدارة أمن المعلومات مسئولاً عن بقاء البنية التحتية للكشف عن الفيروسات/ الشفرات الخبيثة فاعلة وأنها لم يتم ولا يمكن إبطالها في أي نقطة دخول ممكنة.

٢,٤,٦,٣ مسئوليات المستخدم

٢,٤,٦,٣,١ يتعين على المستخدم توخي الحذر عند تحميل (إنزال) الملفات من الإنترنت.

٢,٤,٦,٣,٢ يجب أن لا يفتح المستخدم أو يحمل أو ينفذ أي ملفات يستقبلها أو مرفقات بريد إلكتروني يتلقاها من مصدر غير معروف أو مشبوه أو غير موثوق به.

٢,٤,٦,٣,٣ يجب منع المستخدمين من تغيير الإعدادات، أو حذف، أو إبطال، أو العبث بأي برنامج مخصص لمكافحة أو الكشف عن الفيروسات/ الشفرات الخبيثة يكون قد تم تركيبه على أي نظام معلومات مستخدم من قبلهم.

٢,٤,٦,٣,٤ ينبغي على المستخدمين تبليغ إدارة تقنية المعلومات فوراً عن جميع حوادث الفيروسات/ الشفرات الخبيثة (المكتشفة من خلال برنامج مكافحة الفيروسات/ الشفرات الخبيثة المركبة في أجهزتهم) وعن أي سلوك غير اعتيادي / غير طبيعي للنظام (مثل بطء الاستجابة أو تأخر زمن الاستجابة أو غير ذلك).

٢,٤,٦,٣,٥ على المستخدمين أن يتأكدوا من أن الوسائط الإلكترونية المتبادلة مع الإدارات أو المؤسسات الأخرى قد تم فحصها تحسباً لوجود فيروسات / برامج خبيثة وذلك قبل استخدامها في الأنظمة التي لديهم.

٢,٤,٦,٤ إزالة الفيروسات/ الشفرات الخبيثة من أنظمة معلومات الجامعة

٢,٤,٦,٤,١ يجب القيام فوراً بإزالة أي فيروسات/ شفرات خبيثة مكتشفة في أنظمة معلومات الجامعة. ويجب عدم السماح بوصل أنظمة المعلمات التي لم يتم إزالة / تعطيل الفيروسات/ الشفرات الخبيثة المكتشفة فيها مع شبكة الجامعة.

٢,٤,٦,٤,٢ يتم عمل إعدادات برنامج الفيروسات بحيث يزيل آلياً جميع الفيروسات/ الشفرات الخبيثة المكتشفة في أنظمة المعلومات.

٢,٤,٦,٤,٣ يتم التعامل مع جميع هجمات الفيروسات/ الشفرات طبقاً لإجراءات إزالة الفيروسات/ الشفرات الخبيثة من أنظمة المعلومات لدى الجامعة.

٢,٤,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,٥ الاستخدام المقبول لأنظمة المعلومات

٢,٥,١ الغرض

الغرض من هذه السياسة هو وضع قواعد الاستخدام المقبول لأنظمة المعلومات لدى الجامعة.

٢,٥,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٥,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,٥,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٥,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة، فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٥,٦ قيود سياسة أمن المعلومات

٢,٥,٦,١ الاستخدامات العامة

٢,٥,٦,١,١ يسمح للمستخدمين باستخدام مصادر المعلومات لدى الجامعة فقط لأغراض العمل المصرح لهم القيام بها. ويمنع منعاً باتاً أي استخدام غير مصرح به لأنظمة ومصادر المعلومات لدى الجامعة كالاستخدام الشخصي أو بالنيابة عن أي طرف ثالث (مثل عميل شخصي، أحد أفراد الأسرة، أغراض سياسية أو خيرية أو مدرسية أو خلافه)، وسيتعرض المستخدم الذي يخالف ذلك للإجراءات التأديبية و/أو القانونية المناسبة.

٢,٥,٦,١,٢ تؤول ملكية كافة بيانات الحاسب الآلي التي تم إنشاؤها أو استلامها أو إرسالها باستخدام أنظمة المعلومات لدى الجامعة لملكية الجامعة ولا تعتبر مملوكة من قبل المستخدم. وتحتفظ الجامعة بحقها بفحص كافة البيانات لأي سبب ودون إخطار، ومثال ذلك عندما تكون هناك شبهات بمخالفة هذه القواعد أو أية سياسات وإجراءات لدى الجامعة.

٢,٥,٦,١,٣ ينبغي على منسوبي الجامعة و المستخدمين من طرف ثالث الذين يستخدمون أو الذين لديهم إمكانية الوصول إلى معلومات الجامعة أن يكونوا على دراية بالحدود الحالية لاستخدامهم لأنظمة المعلومات لدى الجامعة، وهم مسئولون عن استخدامهم لأنظمة المعلومات وأي استخدام يتم تحت مسئوليتهم.

٢,٥,٦,٢ حقوق الملكية الفكرية والترخيص

٢,٥,٦,٢,١ الجامعة تقدر وتحترم حقوق الملكية الفكرية (التي تشمل حقوق النسخ، وحقوق التصميم، وحقوق براءة الاختراع وتراخيص الشفرات المصدرية للبرامج والوثائق) المرتبطة بأنظمة المعلومات لديها.

٢,٥,٦,٢,٢ يمنع انتهاك أي حقوق لأي شخص أو شركة محمية بحقوق النسخ أو براءة الاختراع أو حقوق الملكية الفكرية الأخرى، أو الأنظمة واللوائح المشابهة، بما في ذلك، ودون حصر، تركيب البرامج غير المصرح بها أو غير القانونية على أنظمة الجامعة، أو الأنظمة الأخرى غير التابعة إلى الجامعة لكنها موصولة مع بيئة تقنية المعلومات لدى الجامعة.

٢,٥,٦,٢,٣ يجب أن تحتفظ عمادة تقنية المعلومات بمعلومات مناسبة عن التراخيص والأحكام والشروط المتعلقة بأنظمة المعلومات الهامة التي لديها.

٢,٥,٦,٢,٤ يمنع منعاً باتاً استخدام برمجيات أو حقوق ملكية فكرية غير مرخصة.

٢,٥,٦,٣ الاستخدام غير المقبول للأنظمة والشبكة

٢,٥,٦,٣,١ يمنع إدخال برامج خبيثة (مثل الفيروسات، الديدان الإلكترونية، أحصنة طروادة، إلخ) إلى أنظمة المعلومات لدى الجامعة.

٢,٥,٦,٣,٢ يمنع إدخال البرامج المجانية أو المشتركة في شبكة الجامعة سواء تم تحميلها من الإنترنت أو تم الحصول عليها من وسائط أخرى، دون تفويض من عميد تقنية المعلومات.

٢,٥,٦,٣,٣ يمنع استخدام أنظمة المعلومات لدى الجامعة لتخزين، معالجة، تحميل، أو إرسال البيانات التي يمكن أن تعتبر منحازة (سياسياً، دينياً، عنصرياً، عرقياً، حزبيا إلخ) أو تنطوي على مضايقة.

٢,٥,٦,٣,٤ يمنع تقديم عروض أو منتجات أو بنود أو خدمات تنطوي على الغش والخداع باستخدام موارد الأنظمة لدى الجامعة.

٢,٥,٦,٣,٥ يمنع الكشف عن كلمات المرور التي يستخدمها الآخرون للدخول إلى حساباتهم أو السماح باستخدام تلك الحسابات من قبل أطراف أخرى.

٢,٥,٦,٣,٦ يمنع إجراء مسح للمنافذ أو مسح أمني لشبكة معلومات الجامعة أو نظام معلوماتها إلا إذا كان ذلك مصرحاً به من قبل مدير أمن المعلومات وتم إرسال إشعارات مسبقة بذلك للأشخاص المعنيين.

٢,٥,٦,٣,٧ يمنع تنفيذ أي شكل من أشكال مراقبة الشبكة والتي يتم خلالها اعتراض البيانات التي لا تعني الجهاز المضيف لحساب الموظف، إلا إذا كان هذا النشاط جزءاً من الوظيفة/ المهمة المصرح بها للموظف.

٢,٥,٦,٣,٨ يمنع التحايل أو الالتفاف حول تعريف هوية المستخدم أو أمن أي مضيف أو شبكة أو حاسوب.

٢,٥,٦,٣,٩ يمنع استخدام أي برنامج/ لغة/ أمر، أو إرسال الرسائل من أي نوع، بغرض التداخل مع أو تعطيل طرفيه أي مستخدم، من خلال أية وسائل، محلياً أو عبر الإنترنت/ الإنترانت/ الإكسترانت.

٢,٥,٦,٣,١٠ يمنع تزويد معلومات تتعلق بموظفي الجامعة أو قوائم بأسمائهم إلى أي أطراف خارج الجامعة دون تفويض من الجهات المعنية داخل الجامعة.

٢,٥,٦,٣,١١ يجب تغيير كلمات المرور على مستوى نظام المعلومات كل نصف سنة مع إمكانية تقليل المدة وفقاً لحساسية كل نظام.

٢,٥,٦,٤ استخدام البريد الإلكتروني والاتصالات

٢,٥,٦,٤,١ يمنع إرسال أية رسائل بريد إلكتروني غير مطلوبة (طوعية unsolicited) بما في ذلك إرسال "البريد غير النافع Junk" أو المواد الإعلانية الأخرى إلى الأشخاص الذي لم يطلبوا تلك المواد بصفة محددة (رسائل البريد الإلكتروني الاقتحامية).

٢,٥,٦,٤,٢ تمنع المضايقة عبر البريد الإلكتروني أو الهاتف أو الفاكس، سواء من حيث اللغة أو بتكرار أو حجم الرسائل.

٢,٥,٦,٤,٣ يمنع منعاً باتاً الاستخدام غير المصرح به أو تزوير معلومات ترويسة البريد الإلكتروني أو محتوياتها.

٢,٥,٦,٤,٤ يمنع إنشاء أو تحرير "الرسائل التسلسلية chain letters" أو "Ponzi" أو برامج "هرمية pyramid schemes" من أي نوع.

٢,٥,٦,٤,٥ يمنع منعاً باتاً التسجيل والتراسل مع المجموعات الإخبارية والمدونات (الرسائل الاقتحامية للمجموعات الإخبارية).

٢,٥,٦,٤,٦ يجب أن لا يتوقع منسوبو الجامعة أية خصوصية لأي شيء يقومون بتخزينه أو إرساله أو استلامه عبر نظام البريد الإلكتروني للجامعة. ويجوز للجامعة مراقبة الرسائل دون سابق إشعار.

٢,٥,٦,٥ إبداء العناية الواجبة

٢,٥,٦,٥,١ يكون كل مستخدم مسئولاً عن منع الوصول غير المصرح به، بما في ذلك المشاهدة، إلى مصادر المعلومات الواقعة تحت مسئوليته أو تحكمه (مثل المعلومات المتوفرة في الأجهزة المحمولة، أجهزة سطح المكتب، طرفيات الدخول، الطابعات، أو وسائط الأشرطة، إلخ).

٢,٥,٦,٥,٢ يكون كل مستخدم مسئولاً عن إبلاغ إدارة أمن المعلومات بأي سلوك يشتبه بأنه ناتج عن الفيروسات أو أي أنشطة مشبوهة في أنظمتهم.

٢,٥,٦,٦ سياسة استخدام الإنترنت

٢,٥,٦,٦,١ على مستخدمي الإنترنت من خلال شبكة الجامعة ألا يتوقعوا أية خصوصية للمعلومات المخزنة والمعالجة والمرسلة باستخدام نظام المعلومات لدى الجامعة. وينبغي على الجامعة وضع آلية للتحكم ومراقبة استخدام الإنترنت بما في ذلك حجب الوصول إلى فئات معينة من المواقع الإلكترونية (مثل المواقع الإباحية). ويكون الحجب بالتوازي مع استخدام ضوابط أخرى فنية وإجرائية مثل تسجيل الأنشطة التي يقوم بها المستخدم. ويمكن مراقبة هذه السجلات للتأكد من عدم إساءة استخدام الإنترنت. وستتعقب هذه السجلات استخدام الإنترنت وتراقب محتوى وطبيعة المواقع التي يدخلها المستخدمون.

٢,٥,٦,٦,٢ لن تقف الجامعة مكتوفة الأيدي نحو إساءة استخدام الإنترنت، وخصوصاً الأنشطة التي قد تعرضها للملاحقة القضائية أو إجراءات قانونية (ويشمل ذلك الإباحية، ومضايقة الأشخاص). وستتخذ الجامعة الإجراءات التأديبية المناسبة والتي قد تصل إلى فصل المخالف، في حالة قيام المستخدم بأي أنشطة غير قانونية، فإن الجامعة تحتفظ بحقها بالتبليغ عن هذه الأنشطة إلى السلطات التنظيمية أو الحكومية أو القانونية ذات العلاقة.

٢,٥,٦,٦,٣ تقوم الجامعة بحجب فئات محددة من المواقع الإلكترونية بناءً على قوائم أو قواعد بيانات معينة. وهذه القوائم أو قواعد البيانات ليست دقيقة وحديثة دائماً. وإذا ما تم الدخول إلى أي موقع إلكتروني غير قانوني أو لا يتعلق بالعمل، فإن ذلك لا يعني أن الجامعة قد صرحت بالدخول إليه أو اعتبرته مقبولاً. بالتالي، فعلى المستخدمين عدم زيارة مثل تلك المواقع الإلكترونية التي قد تعتبر غير قانونية أو غير أخلاقية أو تتنافى مع مبادئ الجامعة.

٢,٥,٦,٦,٤ على المستخدم فهم الوقت الذي يقضيه في الاستخدام الشخصي للإنترنت والذي يمكن اعتباره مقبولاً. وللمستخدم استشارة إدارته لاستيضاح هذه المتطلبات.

٢,٥,٦,٦,٥ يجب عدم استخدام عناوين البريد الإلكتروني العامة أو الشخصية لإرسال رسائل إلكترونية تتضمن معلومات تتعلق بالعمل.

٢,٥,٦,٦,٦ على المستخدم ملاحظة أن رسائل البريد الإلكترونية المرسلة من أجهزة الكمبيوتر الخاصة بالعمل باستخدام حسابات البريد الإلكترونية العامة مثل ياهو وجي ميل وغيرهما يمكن أن يتم تتبعها من قبل المستلم كونها مرسلة من الجامعة. وبالتالي، فإن أية إساءة استخدام يمكن أن تعرض الجامعة إلى الإجراءات القضائية.

٢,٥,٦,٦,٧ إذا كان هناك مواقع معينة تم حجبها وكان واجباً ألا يتم حجبها (أو بالعكس)، فعلى المستخدم إشعار إدارة أمن المعلومات بذلك.

٢,٥,٦,٦,٨ إذا قام المستخدم بشكل عرضي بزيارة موقع غير لائق، أو إذا تم توجيهه آلياً إلى ذلك الموقع، فإن عليه مغادرة ذلك الموقع فوراً.

٢,٥,٦,٦,٩ على المستخدمين الامتناع عن تنزيل أي برمجيات أو أية مواد أخرى (موسيقى، صور، إلخ) لا علاقة لها بالعمل.

٢,٥,٦,٦,١٠ أثناء تنزيل المعلومات المتعلقة بالعمل، ينبغي على المستخدم التأكد من عدم مخالفة أي حقوق ملكية فكرية مما قد يعرض الجامعة لمخاطر الإجراءات القضائية.

٢,٥,٦,٦,١١ على الجامعة التأكد بأن المعلومات المتاحة على موقعها الإلكتروني قد تم التحقق منها والتأكد من صحتها بشكل ملائم.

٢,٥,٦,٦,١٢ ينبغي على المستخدم أن لا يسجل عنوان بريده الإلكتروني الخاص بالعمل على أي موقع إلكتروني لا يتعلق بالعمل.

٢,٥,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,٦ التعامل مع الوسائط الإلكترونية

٢,٦,١ الغرض

الغرض من هذه السياسة حماية الوسائط الإلكترونية لدى الجامعة مثل (أجهزة الذاكرة الموصولة على منافذ USB، الأقراص الصلبة المتنقلة، وسائط بيانات الدخل/الخرج مثل دي في دي، والأقراص الضوئية وغيرها) من الاستخدام والسرقة والوصول إليها بشكل غير مصرح به.

٢,٦,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٦,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,٦,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٦,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٦,٦ قيود سياسة أمن المعلومات

٢,٦,٦,١ تخزين الوسائط الإلكترونية

٢,٦,٦,١,١ يتم خزن الوسائط الإلكترونية في بيئة آمنة تتوفر فيها شروط السلامة.

٢,٦,٦,١,٢ يجب استخدام البطاقات لتعريف الوسائط التي تتطلب مناولة خاصة، حيث يجب وضع بطاقات على الوسائط الإلكترونية بطريقة لا تمكن الأشخاص الذين ليسوا موظفين لدى الجامعة (سواء كانوا موظفين مؤقتين أو دائمين أو على عقود) من تحديد أنظمة المعلومات الحساسة من خلال تلك البطاقات.

٢,٦,٦,١,٣ يجب تخزين المعلومات المخزنة على وسائط بيانات و التي يتطلب توفرها لفترات زمنية أطول من دورة حياة الوسائط في مكان آخر لتفادي ضياعها بسبب التلف الذي قد يصيب الوسائط.

٢,٦,٦,٢ أمن الوسائط الإلكترونية أثناء نقلها

٢,٦,٦,٢,١ على الجامعة أن تتأكد من حماية أنظمة معلومات العمل أثناء نقل الوسائط .

٢,٦,٦,٢,٢ يجب الحصول على تصريح بأية عمليات نقل لوسائط تخزين المعلومات من الجامعة من قبل المسئول عن تلك المعلومات، والاحتفاظ بسجل عمليات النقل هذه من قبل الطرف ذي العلاقة لأغراض فحص ومراجعة السجلات audit trail.

٢,٦,٦,٣ الوسائط القابلة لإعادة الاستخدام

٢,٦,٦,٣,١ يجب أن يتم المسح التام للمحتويات السابقة المحفوظة على الوسائط الإلكترونية القابلة لإعادة الاستخدام والتأكد من عدم إمكانية استرجاع تلك المحتويات.

٢,٦,٦,٣,٢ يجب فحص جميع الأجهزة المحتوية على وسائط خزن بيانات (سواقات الأقراص الصلبة الثابتة) للتأكد من إزالة أي أنظمة معلومات حساسة تتعلق بالعمل، وكذلك إزالة البرامج المرخصة عنها، وأنه يتم الكتابة فوقها بأمان أو إتلافها قبل التخلص منها أو إعادة استخدامها.

٢,٦,٦,٤ الوسائط القابلة للإزالة

٢,٦,٦,٤,١ يجب إعادة تهيئة الوسائط القابلة للفك وإعادة الكتابة التي لم تعد مستخدمة للحيلولة دون الكشف عن المعلومات التي تحتويها أثناء تبادلها بين الموظفين أو الأطراف الأخرى.

٢,٦,٦,٥ التخلص من الوسائط

٢,٦,٦,٥,١ يجب إتلاف الوسائط المادية التي تحتوي على معلومات حساسة بشكل آمن عندما لا تعود هناك حاجة لها.

٢,٦,٦,٥,٢ يتم الاحتفاظ بسجل عمليات إتلاف/ تدمير أجهزة الوسائط وتوثيق الأشخاص المسئولين عن الإتلاف.

٢,٦,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,٧ أمن الوثائق

٢,٧,١ الغرض

الغرض من هذه السياسة هو حماية المعلومات الحساسة لدى الجامعة من التلف والسرقة والدخول غير المصرح به إليها.

٢,٧,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم.
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٧,٣ المسئول التنفيذي

مدير الإدارة المسئولة في كل جهة

٢,٧,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٧,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٧,٦ قيود سياسة أمن المعلومات

٢,٧,٦,١ حماية وثائق العمل

٢,٧,٦,١,١ على الجامعة تصنيف وثائقها لحماية المعلومات من استخدامها وإلحاق الضرر بالجامعة أو تعريض أمنها وخصوصيتها للمخاطر. ويتم تصنيف الوثائق من قبل المسئول عنها ضمن إحدى الفئات التالية:

- عامة: لأية وثيقة ممكن أن تنشر أو يمكن الحصول عليها من مصدر منشور، مثل الإنترنت.
- سرية: لأية وثيقة يمكن أن تتوفر لجميع موظفي الجامعة، ولكن ليس للجمهور، مثل أدلة الهاتف، المعلومات المحصورة على جماعة معينة أو مشروع ضمن الجامعة، مثل محاضر الاجتماعات.
- سرية عالية: لأية وثيقة محدودة التوزيع لها قيمة هامة للجامعة، مثل العقود، ويمكن أن يشمل ذلك جميع المعلومات الخاصة مثل المهام الحساسة للجامعة.
- سرية قصوى: أعلى تصنيف سرية المعلومات ضمن الجامعة، والتي يمكن أن تلحق "ضرراً جسيماً" بأمن الجامعة، و/أو على المستوى الوطني إذا ما تم الكشف عنها للجمهور.
- (يجب ملاحظة أن الوثائق السرية وتلك المصنفة ذات سرية أعلى يجب أن يوضع عليها علامة بذلك).

٢,٧,٦,١,٢ يجب حفظ وثائق العمل الحساسة أو الهامة في أماكن مقفلة (يستحسن أن تكون داخل خزانات مقاومة للحريق) عندما لا تكون مطلوبة، وخصوصاً عند إخلاء المكاتب.

٢,٧,٦,١,٣ يسمح فقط لموظفي الجامعة الذين يعملون بصفة دائمة والمصرح لهم القيام بمناولة ومسح وتصوير الوثائق المصنفة ذات سرية عالية، بما في ذلك جميع الوثائق المحتوية على معلومات العملاء. ولا يجب السماح للموظفين المؤقتين، والمتدربين في الإجازات الصيفية، والمقاولين، والأطراف الثالثة بالتعامل مع الوثائق ذات السرية العالية.

٢,٧,٦,١,٤ يتعين على الجامعة تطوير وتطبيق والحفاظ على آليات للتأكد من أن جميع الوثائق قد تم وضع البطاقات المتعلقة بالسرية عليها.

٢,٧,٦,١,٥ عندما لا تعود ثمة حاجة للوثائق الحساسة فيجب تقطيعها بأجهزة تقطيع الأوراق أو تحويلها إلى خام ورق أو إتلافها بطريقة تحول دون إعادة تجميعها.

٢,٧,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتباراً من تاريخ (اعتمادها)

٢,٨ الغش والتبليغ عن المخالفات

٢,٨,١ الغرض

إن الغرض من هذه السياسة هو التأكد من منع حدوث الغش والتبليغ عن الغش والأنشطة المحظورة في أنظمة المعلومات لدى الجامعة والتحقيق في تلك الأنشطة واتخاذ الإجراءات المناسبة نحوها.

٢,٨,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٨,٣ المسئول التنفيذي

مدير إدارة تقنية المعلومات

٢,٨,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٨,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٨,٦ قيود سياسة أمن المعلومات

٢,٨,٦,١ التبليغ عن الأنشطة التي تنطوي على غش

٢,٨,٦,١,١ يتعين على جميع مستخدمي أنظمة المعلومات لدى الجامعة التبليغ عند اكتشاف أي أنشطة تنطوي على غش وتحايل.

٢,٨,٦,٢ التحري عن الأنشطة التي تنطوي على غش والإجراءات المترتبة عليها

٢,٨,٦,٢,١ تعتزم الجامعة القيام بتحري وتقصي كامل عن أي تصرفات تنطوي على غش، أو اختلاس، أو مخالفات أخرى مشابهة تتعلق بأنظمة المعلومات. ويجب إجراء تحقيق موضوعي ونزيه بصرف النظر عن منصب أو وظيفة أو طول خدمة أو علاقة أي طرف لدى الجامعة، قد يكون متورطاً أو عرضة لذلك التحقيق.

٢,٨,٦,٢,٢ يجب أن تتعاون الجامعة مع وكالات تنفيذ القانون في التحقيق والتحري عن الأنشطة التي تنطوي على غش وتحايل وفقاً لأنظمة المملكة العربية السعودية.

٢,٨,٦,٢,٣ على الجامعة أن تبذل كل الجهود المعقولة، بما في ذلك التحصيل على تعويض عن الخسائر التي تسبب فيها الطرف المخالف أو الموارد الأخرى المناسبة بأمر المحكمة.

٢,٨,٦,٣ التعامل مع الأنشطة التي تنطوي على غش وتحايل

٢,٨,٦,٣,١ تلتزم الجامعة بمنع الأنشطة التي تنطوي على غش وتحايل من قبل منسوبيها وعملائها وموردیها وأصحاب المصالح الآخرين.

٢,٨,٦,٣,٢ يتم تشجيع جميع الموظفين والوكلاء والعاملين المؤقتين/ العاملين على العقود لدى الجامعة على التبليغ عن أية أنشطة يرون أنها قد تنطوي على غش وتحايل.

٢,٨,٦,٣,٣ يجب التبليغ فوراً عن جميع الأنشطة المكتشفة التي تنطوي على غش وتحايل إلى الإدارات المعنية.

٢,٨,٦,٣,٤ يجب أن تتأكد الجامعة من التحقيق والتحري عن جميع الأنشطة المبلغ عنها و التي تنطوي على غش وتحايل.

٢,٨,٦,٣,٥ يجب أن تتأكد الجامعة من الملاحقة القضائية لكافة الحالات التي تنطوي على غش وتحايل وفقاً لأنظمة ولوائح المملكة.

٢,٨,٦,٣,٦ يجب أن تتأكد إدارة الجامعة من الحفاظ على السرية المطلوبة وتقديم الحماية الضرورية (حسبما تسمح به الأنظمة واللوائح المطبقة في المملكة) لأي شخص قام بالتبليغ عن الحوادث المتعلقة بالغش والتحايل.

٢,٨,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,٩ إدارة حوادث أمن المعلومات

٢,٩,١ الغرض

الغرض من هذه السياسة هو التأكد من التبليغ عن جميع حوادث أمن المعلومات المتعلقة بأنظمة المعلومات لدى الجامعة ومتابعتها والتحقيق فيها وحلها بالسرعة الواجبة وبصورة فعالة.

٢,٩,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٩,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,٩,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٩,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٩,٦ قيود سياسة أمن المعلومات

٢,٩,٦,١ تعريف الجامعة لحوادث أمن المعلومات

٢,٩,٦,١,١ تعرف الجامعة حوادث أمن المعلومات على أنها أية أحداث غير متوقعة تؤثر على أنظمة معلومات الجامعة، حسبما يلي:

- الأحداث التي لا تشكل جزءاً من العمليات الاعتيادية لخدمات تقنية المعلومات، والتي تسبب، أو قد تسبب، تعطيل أو توقف أو هبوط في جودة تلك الخدمات.
- الأحداث التي قد تنتهك سرية أو نزاهة/ تكامل أو توفر المعلومات لدى الجامعة و/أو أنظمة المعلومات وتشمل الحوادث الأمنية المتعلقة بتقنية المعلومات، والحوادث المتعلقة بالأمن المادي وأمن الأشخاص.
- الأحداث المتعلقة بأوضاع استثنائية أو أوضاع تستدعي تدخل الإدارة العليا، ومن شأنه أن يسبب أذى أو ضرر بالغ في الممتلكات.
- الثغرات الأمنية (مَواطِن الضعف في أنظمة المعلومات، والتي قد تستغل في انتهاك سرية أو سلامة أو توفر النظام) وأخطاء البرامج (وهي أي خلل أو انحراف في سير التطبيقات البرمجية). كما تُعد أية مخالفة لسياسات وإجراءات أمن المعلومات لدى الجامعة من حوادث أمن المعلومات.

٢,٩,٦,٢ التبليغ عن حوادث أمن المعلومات

٢,٩,٦,٢,١ يتوجب على جميع موظفي الجامعة وموظفي الأطراف الثالثة المعنيين التبليغ عن حوادث أمن المعلومات إلى إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة بالسرعة اللازمة على البريد الالكتروني ***incident@iu.edu.sa***.

٢,٩,٦,٣ إدارة الحوادث للمستخدمين/ العملاء عبر الإنترنت

٢,٩,٦,٣,١ على الجامعة أن تقوم بتزويد المستخدمين و العملاء عبر الإنترنت بآلية بسيطة وسهلة الوصول إليها لاستخدامها في التبليغ عن الأنشطة المشبوهة، أو المخاوف الأمنية، أو الشكاوى، أو الحوادث. كما و أن عليها الرد على ما يقدمه المستخدمين و العملاء بالسرعة اللازمة. وفيما يلي بعض الضوابط الرئيسية التي يجب أن تضعها الجامعة:

- يجب أن يتضمن الموقع الإلكتروني أو الشبكة الداخلية الخاصة بـالجامعة على وسيلة تمكن المستخدمين و العملاء من تبليغها عن الحوادث الأمنية أو الأنشطة المشبوهة.
- يجب أن يقدم الموقع الإلكتروني أو الشبكة الداخلية الخاصة بـالجامعة رقم هاتف ليتواصل من خلاله المستخدمين و العملاء للتبليغ عن الحوادث أو الأنشطة المشبوهة.

٢,٩,٦,٣,٢ على مستخدمي/ عملاء الخدمات عبر الإنترنت/ الخدمات الإلكترونية لدى الجامعة القيام بالتبليغ عن الأنشطة المشبوهة، أو المخاوف الأمنية، أو الحوادث الأمنية عن طريق البريد الالكتروني الخاص باستقبال الحوادث ***incident@iu.edu.sa*** .

٢,٩,٦,٤ اعتبارات تتعلق بعملية إدارة الحوادث

٢,٩,٦,٤,١ يجب أن تضطلع إدارة أمن المعلومات بمسئولية تلقي وتسجيل جميع حوادث أمن المعلومات المبلغ عنها، وتقييم مدى صحة هذه الحوادث، وتصنيفها بناءً على أولويتها وأثرها على النشاط، ومن ثم معالجتها، أو التبليغ عن الحوادث التي تم التحقق منها إلى الشخص المناسب لمعالجتها.

٢,٩,٦,٤,٢ يجب أن يتوفر لدى الجامعة خطة موثقة للاستجابة لحوادث أمن المعلومات بحيث تغطي الأنواع المختلفة من حوادث أمن المعلومات. كما يجب فحص كل خطة من خطط الاستجابة لحوادث أمن المعلومات للتأكد من فاعليتها من خلال الوسائل المناسبة كاستخدام المحاكاة ومثال ذلك، خطة الاستجابة لحوادث هجمات الشفرات الخبيثة، الاستجابة لهجمات الاصطياد الإلكتروني الاصطياد الالكتروني، وغير ذلك.

٢,٩,٦,٤,٣ يجب إشراك الإدارة العليا لدى الجامعة في التحري عن أية حوادث أمن معلومات تتعلق بأنظمة المعلومات الحساسة والخدمات والعمليات والموظفين.

٢,٩,٦,٤,٤ يجب على إدارة أمن المعلومات ان تقوم بمراقبة الحوادث المسجلة وإجراء مراجعات دورية للحوادث القائمة للتأكد من حلها بالسرعة الواجبة.

٢,٩,٦,٤,٥ يجب على إدارة أمن المعلومات ان تتولى المحافظة على والاحتفاظ بتقارير حوادث أمن المعلومات بما في ذلك تقارير حل تلك الحوادث.

٢,٩,٦,٤,٦ يجب على الجامعة ان تجري تقييماً لاحقاً للحادثة المتعلقة بأمن المعلومات (حيثما ينطبق)، وتسارع باتخاذ الإجراءات الوقائية بناءً على الدروس المستفادة لتفادي أو الحد من وقوع أحداث مشابهة.

٢,٩,٦,٥ تجميع الأدلة

٢,٩,٦,٥,١ عندما تستدعي الإجراءات المتخذة بحق الشخص أو المنشأة المتورطين في حوادث أمن المعلومات اتخاذ إجراءات قانونية (سواء مدنية أو جنائية)، فإنه على إدارة امن المعلومات أن تتأكد من تجميع الأدلة والقرائن المطلوبة، والحفاظ عليها بشكل آمن، وتقديمها عند الحاجة، مع طلب تدخل الإدارة القانونية عند الحاجة لذلك.

٢,٩,٦,٦ تحليل التوجهات والتقارير التنفيذية

٢,٩,٦,٦,١ تقوم إدارة امن المعلومات بشكل دوري بتحليل الحوادث المسجلة لتحديد التوجهات التي تظهر بهذا الصدد.

٢,٩,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١٠ أمن الموظفين

٢,١٠,١ الغرض

الغرض من هذه السياسة هو الحد من احتمالات إساءة استخدام أو تدمير أنظمة المعلومات لدى الجامعة، وذلك من خلال التأكد من نزاهة الموظفين الذين يتم منحهم إمكانية الوصول إلى أنظمة المعلومات لدى الجامعة.

٢,١٠,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم

٢,١٠,٣ المسئول التنفيذي

مدير إدارة شؤون هيئة التدريس والموظفين / إدارة تقنية المعلومات / أي جهة تتعاقد مع موظفين

٢,١٠,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١٠,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١٠,٦ قيود سياسة أمن المعلومات

٢,١٠,٦,١ ما قبل التوظيف

٢,١٠,٦,١,١ عند التعاقد مع موظفين أو مقاولين، فإنه يتوجب على الجامعة أن تتأكد من خلفية المرشحين بصورة مناسبة و وفقاً للأنظمة واللوائح المطبقة في المملكة. ويشمل ذلك التأكد من السجلات الجنائية والائتمانية، وكذلك التحقق من صحة مرجعيات ومؤهلات المرشح.

٢,١٠,٦,٢ شروط وأحكام التوظيف

٢,١٠,٦,٢,١ يجب أن تتضمن أحكام وشروط التوظيف لدى الجامعة الإشارة إلى هذه السياسة الأمنية، وأن توضح بشكل محدد ما يلي:

- المسئوليات المتعلقة بالتعامل الآمن مع المعلومات وأنظمة المعلومات الخاصة بالجامعة من قبل الموظف أو المستخدمين التابعين للطرف الثالث.
- المسئوليات المتعلقة بالتعامل مع المعلومات المستلمة من الشركات أو الأطراف الثالثة.
- وجوب توقيع اتفاقية السرية / عدم الإفشاء الخاصة بـ الجامعة، وكذلك أية اتفاقيات سرية محددة مطلوبة من أية منشأة قانونية أو تنظيمية.
- إشارة إلى الإجراءات الإدارية التي ستطبق في حالة مخالفة أحكام التوظيف.

٢,١٠,٦,٢,٢ يتعين على جميع المستخدمين من الموظفين والمقاولين والأطراف الثالثة لدى الجامعة توقيع شروط وأحكام التوظيف/ الارتباط للدلالة على قبولهم بها.

٢,١٠,٦,٢,٣ يتعين على كل موظف أو مقاول أو مستخدم تابع لطرف آخر لدى الجامعة توقيع اتفاقية السرية المناسبة. وكجزء من اتفاقية السرية، على الشخص تأكيد التزامه بالحفاظ على سرية معلومات الجامعة أثناء ارتباطه بها وبعد ذلك.

٢,١٠,٦,٢,٤ يتعين على كل موظف أو مقاول أو مستخدم تابع لطرف آخر لدى الجامعة أن يقر بصفة رسمية أنه قرأ وفهم جميع السياسات والإجراءات والمعايير الأمنية المطلوب تطبيقها.

٢,١٠,٦,٣ الاعتماد على الأشخاص

٢,١٠,٦,٣,١ ينبغي على الجامعة الحد من مخاطر الاعتماد بصورة كبيرة على موظفين رئيسيين وذلك من خلال تفعيل المشاركة في المعرفة، وتخطيط التعاقب والإحلال الوظيفي، ووجود احتياطي من الموظفين، والوسائل الأخرى في هذا الصدد.

٢,١٠,٦,٤ عملية الإجراءات التأديبية

٢,١٠,٦,٤,١ يجب أن تتخذ الجامعة إجراءات تأديبية في حال تم انتهاك سياسات تقنية وأمن المعلومات.

٢,١٠,٦,٤,٢ يجب توثيق و اعتماد أي استثناءات تسمح بعدم تعريض أحد موظفي الجامعة للإجراءات التأديبية.

٢,١٠,٦,٥ استقالة أو إقالة الموظف أو المقاول

٢,١٠,٦,٥,١ في حالة استقالة أو إقالة موظف أو مقاول فإن على مدير إدارة الموارد البشرية/ مدير الإدارة المعنية إبلاغ إدارة تقنية المعلومات فوراً لإلغاء حقوق دخول ذلك الموظف أو المقاول إلى النظام.

٢,١٠,٦,٥,٢ عند إنهاء أو انتهاء خدمات موظف أو مقاول أو مستخدم من طرف ثالث، فإنه يجب استرجاع كافة أنظمة المعلومات التي منحت لذلك الشخص/ الطرف على الفور، وذلك قبل تسوية مستحقاته ومغادرته للجامعة.

٢,١٠,٦,٦ تغيير الدور، أو استقالة أو إقالة الموظف أو المقاول

٢,١٠,٦,٦,١ في حالة تغيير الدور أو استقالة أو إقالة موظف أو مقاول، فإن على مدير إدارة الموارد البشرية/ الإدارة المعنية القيام فوراً بإبلاغ عميد تقنية المعلومات لإلغاء/ تعديل حقوق وصول ذلك الموظف أو المقاول لأنظمة المعلومات. ويجب التعامل مع ذلك وفقاً لإجراءات تغيير الدور أو الاستقالة أو الإقالة.

٢,١٠,٦,٧ مراقبة سلوك الموظف

٢,١٠,٦,٧,١ تقع على عاتق موظفي ومقاولي الجامعة مسئولية تبليغ إدارة أمن المعلومات/ الموارد البشرية/ أو الإدارة المعنية عن أي أنشطة مشبوهة يقوم بها زملاؤهم أو المقاولين أو الأشخاص الآخرين الذين لديهم إمكانية الوصول إلى أنظمة المعلومات لدى الجامعة.

٢,١٠,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١١ إدارة أصول المعلومات

٢,١١,١ الغرض

الغرض من هذه السياسة هو التأكد من أن أنظمة المعلومات لدى الجامعة قد تم تحديدها وتعيين مسئولين محددين عنها، وتصنيفها بشكل مناسب بما يتوافق مع طبيعة هذه الأنظمة وتصنيف مخاطر أمن المعلومات المتعلقة بها، مما يساعد على تحديد الضوابط الأمنية المناسبة لها.

٢,١١,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,١١,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١١,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١١,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١١,٦ قيود سياسة أمن المعلومات

٢,١١,٦,١ تعريف أنظمة المعلومات

٢,١١,٦,١,١ تعرّف الجامعة أنظمة المعلومات على أنها البنية التحتية التقنية و الطبيعية التي تؤثر بصورة مباشرة أو غير مباشرة على تحديد ومعالجة وتبليغ وتدمير وتخزين معلومات الجامعة، ويشمل ذلك ما يلي:

- البرامج التطبيقية لتقنية المعلومات؛
- البنية التحتية التقنية لمعالجة المعلومات (أجهزة الحاسوب وأجهزة معالجة المعلومات الأخرى مثل مقاسم الاتصالات (PABX)، والهاتف المتنقل، الطابعات، وغير ذلك)؛
- البنية التحتية للشبكة والأمن؛
- البنية التحتية المادية (المباني، المكاتب، غرف الاجتماعات، إلخ)؛
- الوثائق؛
- عناصر البنية التحتية الأخرى ذات العلاقة.

٢,١١,٦,٢ تحديد أنظمة المعلومات

٢,١١,٦,٢,١ يجب تحديد جميع أنظمة المعلومات لدى الجامعة من خلال إجراء جرد لتلك الأنظمة من قبل إدارة تقنية المعلومات وإدارة أمن المعلومات وفقاً لإجراءات تحديد أنظمة المعلومات. (مع ملاحظة أن المعلومات التي تم تجميعها في سجلات أنظمة المعلومات يجب دمجها في هذا الجرد لأنظمة المعلومات).

٢,١١,٦,٣ تصنيف أنظمة المعلومات

٢,١١,٦,٣,١ يجب تعيين درجة تصنيف لكل نظام من أنظمة معلومات الجامعة، مع الأخذ في الاعتبار الأثر المتوقع على نشاط الجامعة في حال انتهاك سرية أو سلامة أو توفر نظام المعلومات.

٢,١١,٦,٣,٢ يجب على المسئول عن نظام المعلومات بتصنيف أنظمة المعلومات طبقاً لنظام تصنيف أنظمة معلومات الجامعة، وذلك وفقاً لإجراءات تصنيف أنظمة المعلومات.

٢,١١,٦,٤ وضع بطاقات تعريفية على أنظمة المعلومات

٢,١١,٦,٤,١ يجب ان يتم وضع بطاقات على كل نظام من أنظمة المعلومات المادية من قبل راعي ذلك النظام.

٢,١١,٦,٥ المسئولون والراعون لأنظمة المعلومات

٢,١١,٦,٥,١ تُعرِّف الجامعة المسئول عن نظام المعلومات على أنه الشخص أو الإدارة الذين تكون لهم المسئولية النهائية ولديهم الصلاحيات المتعلقة بنظام المعلومات، ويقررون كيف ومن سيستخدم النظام.

٢,١١,٦,٥,٢ تُعرِّف الجامعة راعي نظام المعلومات على أنه الشخص أو الإدارة الذين تم تكليفهم بالمسئولية عن إدارة عمليات، وتغييرات، وصيانة، والتخلص من نظام المعلومات بتفويض من المسئول عن المعلومات.

٢,١١,٦,٥,٣ يضطلع المسئول عن نظام المعلومات بالمسئولية النهائية عن أمن ذلك النظام.

٢,١١,٦,٥,٤ يضطلع راعي نظام أمن المعلومات بالاشتراك مع إدارة أمن المعلومات بمسئولية تطبيق الضوابط المطلوبة لتوفير عوامل الأمان لذلك النظام.

٢,١١,٦,٦ تحديث جرد أنظمة المعلومات

٢,١١,٦,٦,١ يجب ان يتم مراجعة جرد أنظمة المعلومات بشكل منتظم وتحديثها إذا اقتضى الأمر وفقاً لإجراءات مراجعة وتحديث جرد أنظمة المعلومات.

٢,١١,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١٢ إدارة مخاطر أمن المعلومات

٢,١٢,١ الغرض

الغرض من هذه السياسة هو التأكد من قيام الجامعة باكتشاف و تحديد مخاطر أمن المعلومات المتعلقة بأنظمة المعلومات لديها مع الأخذ في الاعتبار التهديدات ونقاط الضعف التي تعاني منها تلك الأنظمة وأثر ذلك على سير العمل. كما تقوم الجامعة بالتخطيط لاتخاذ مبادرات مناسبة لتخفيف مخاطر التعامل مع أمن المعلومات التي تم تحديدها.

٢,١٢,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,١٢,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١٢,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١٢,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١٢,٦ قيود سياسة أمن المعلومات

٢,١٢,٦,١ التزام الجامعة بإدارة مخاطر أمن المعلومات

٢,١٢,٦,١,١ على إدارة الجامعة أن تتأكد من أنه تم تحديد مخاطر أمن المعلومات لدى الجامعة وإدارتها بشكل فاعل وبكفاءة وبالسرعة الواجبة مع الأخذ في الاعتبار آثار تلك المخاطر على نشاط الجامعة.

٢,١٢,٦,١,٢ يجب تقييم مخاطر أمن المعلومات وإدارتها كجزء من أنشطة العمل لدى الجامعة، ومثال ذلك العمليات اليومية لسير العمل، حيازة أنظمة المعلومات، التطوير والتنفيذ، عمليات أنظمة المعلومات، وغير ذلك، من خلال التأكد من التطبيق المناسب لسياسات وإجراءات ومعايير أمن المعلومات لدى الجامعة.

٢,١٢,٦,٢ تقييم المخاطر استنادا على سير العمل

٢,١٢,٦,٢,١ يمكن تقييم المخاطر على مستويات متعددة اعتمادا على غزارة التفاصيل المطلوبة. يجب أن يعتمد أسلوب الموظفين والأطراف الثالثة المعنية لتقييم مخاطر أنظمة المعلومات لدى الجامعة على مدى حساسية وأهمية تلك الأنظمة للشركة، أي باخذ درجة التصنيف المعطاة لأمن تلك الأنظمة بعين الاعتبار.

٢,١٢,٦,٢,٢ يجب أن يتم تقييم مخاطر أمن جميع أنظمة المعلومات من خلال:

- فهم التصنيف الأمني لنظام المعلومات .
- تحديد الضوابط الأمنية المطلوبة لأنظمة المعلومات.
- تقييم حالة تلك الضوابط من خلال مناقشتها مع أصحاب المصالح الرئيسية المعنيين بالأمر أو إجراء أساليب فحص أمنية مناسبة.

٢,١٢,٦,٢,٣ يجب ان تقوم الجامعة بإجراء تنقيح تفصيلي لمعايير الأمن المحددة لأنظمة المعلومات المصنفة على أنها ذات مخاطر عالية وذلك من خلال إتباع منهجية تقييم رسمية لمخاطر أمن المعلومات. قد تتطلب هذه المنهجية إجراء تحليل تفصيلي لبيئة وخواص أنظمة المعلومات، والتهديدات ونقاط الضعف المحددة في تلك الأنظمة، والتصنيف الأمني المتعلق بالملاحظات المحددة، مع الأخذ في الاعتبار أثر ذلك على أعمال الجامعة.

٢,١٢,٦,٢,٤ يضطلع المسئول عن أنظمة المعلومات بالاشتراك مع إدارة أمن المعلومات وإدارة تقييم المخاطر إن وجدت بمسئولية تخطيط وإجراء تقييم لمخاطر تلك الأنظمة المسئولين عنها.

٢,١٢,٦,٣ تخفيف المخاطر و القبول بها

٢,١٢,٦,٣,١ ينبغي على الجامعة التعامل بشكل مناسب مع مخاطر أمن المعلومات التي تم اكتشافها و تحديدها كجزء من عملية تقييم المخاطر.

٢,١٢,٦,٣,٢ يجب مراجعة الملاحظات التي تم اكتشافها جراء عملية تقييم المخاطر من حيث أثرها على الجامعة والطبيعة التقنية للخطر. و كما يجب تحديد الأشخاص المناسبين وإجراءات/ مبادرات التخفيف المتعلقة بالعمليات أو التقنية، ومن ثم يجب رفع المرئيات إلى إدارة الجامعة، واعتمادها وتطبيقها بشكل فاعل.

٢,١٢,٦,٣,٣ قد تقبل الجامعة أي مخاطر متبقية يتعذر تخفيفها بشكل فعال. وتكون الصلاحية النهائية للجنة توجيه أمن المعلومات بالتشاور مع الأطراف المعنية بشأن القرارات المتعلقة بقبول المخاطر المتبقية.

٢,١٢,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١٣ إدارة سياسات أمن المعلومات

٢,١٣,١ الغرض

الغرض من هذه السياسة هو ابقاء وتبليغ سياسات ومعايير وإجراءات أمن المعلومات لدى الجامعة، وذلك وفقاً لمتطلبات النشاط والأنظمة واللوائح المطبقة في المملكة العربية السعودية.

٢,١٣,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,١٣,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١٣,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١٣,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١٣,٦ قيود سياسة أمن المعلومات

٢,١٣,٦,١ مراجعة وتحديث سياسات ومعايير وإجراءات أمن المعلومات

٢,١٣,٦,١,١ يقوم مدير أمن المعلومات بإجراء مراجعة وتحديث سنوي لسياسات ومعايير وإجراءات أمن المعلومات وفقاً لأفضل الممارسات العالمية و نتائج تقييم مخاطر أمن المعلومات والمتطلبات القانونية والنظامية ومتطلبات الالتزام الأخرى.

٢,١٣,٦,١,٢ يجب اعتماد أي تحديث يتم على وثيقة سياسة أمن المعلومات من قبل إدارة الجامعة. كما يجب نشر وتبليغ السياسات والمعايير والإجراءات المتعلقة بالموظفين والأطراف الخارجية ذات الصلة.

٢,١٣,٦,١,٣ يعنى مدير أمن المعلومات بمسئولية تحديث سياسات ومعايير وإجراءات أمن المعلومات بما يتوافق مع أي تغييرات هامة تطرأ على بيئة مخاطر أمن المعلومات لدى الجامعة.

٢,١٣,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١٤ الأمن المادي والبيئي

٢,١٤,١ الغرض

الغرض من هذه السياسة هو تحديد القواعد الأساسية لمنع الدخول غير المصرح به والتداخل مع مرافق وأنظمة أمن المعلومات لدى الجامعة وكذلك الحفاظ على أمن المعلومات والموظفين من التعرض إلى التهديدات المادية المختلفة، والتي من شأنها التأثير سلبياً على خدمات أنظمة المعلومات أو توقفها عن العمل.

٢,١٤,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,١٤,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١٤,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١٤,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١٤,٦ قيود سياسة أمن المعلومات

٢,١٤,٦,١ ضوابط الأمن المادي القائمة على المخاطر

٢,١٤,٦,١,١ يجب أن تتأكد الجامعة من أن جميع منشآتها المادية تتمتع بعوامل الأمان بما يتوافق مع مخاطر أنظمة المعلومات في تلك المنشآت.

٢,١٤,٦,١,٢ يتم تحديد جميع المنشآت المادية لدى الجامعة وتعين تصنيف أمني لها.

٢,١٤,٦,١,٣ يتم تخطيط الأمن المادي والبيئي للمنشآت المادية لدى الجامعة مع الأخذ بعين الاعتبار درجة تصنيف أمن المعلومات والمعايير المتعلقة بالنوع المحدد من البنية التحتية المادية لدى الجامعة.

٢,١٤,٦,١,٤ تعنى إدارة الأمن والسلامة في الجامعة بمسئولية التأكد من تطبيق ضوابط الأمن المادي للمباني والمنشآت.

٢,١٤,٦,٢ المناطق الآمنة

٢,١٤,٦,٢,١ يجب أن تقوم الجامعة بتطوير مخطط الأمن المادي لمرافقها كما يجب توزيع المخطط المادي الخاص بـ الجامعة على مناطق بحيث يكون لكل منطقة مستوى أعلى من القيود التي تحكم متطلبات التصريح بالدخول. ويمكن تصنيف المناطق المحيطية كالتالي:

- المنطقة العامة ومنطقة الاستقبال: (قيود محدودة وتخضع هذه المنطقة للمراقبة العامة).
- منطقة المكاتب (دخول محدود، يتم تسجيل الدخول و مرافقة الزوار الذين يدخلون إلى هذه المنطقة. كما تخضع المنطقة للمراقبة العامة).
- منطقة الدخول الآمنة (دخول محدود، يتم تسجيل الدخول و مرافقة دخول الزوار. تخضع المنطقة للإشراف).
- منطقة الدخول المقيد – التي تقتصر على دخول الأشخاص المصرح لهم فقط. (الدخول يخضع لقيود عالية. يتم تسجيل الدخول. يجب حصول الموظفين والزوار الذين يدخلون إلى هذه المنطقة على تصريح محدد بالدخول. تخضع المنطقة للمراقبة).

٢,١٤,٦,٢,٢ يجب التأكد مما يلي:

- أن مرافق معالجة المعلومات لا تقع في منطقة غير مستقرة من ناحية البيئة.
- عدم وقوع مرافق معالجة المعلومات على مقربة من أي مرافق مجاورة خطرة (مثل المختبرات الكيمائية وخلافه).
- يتم تخزين المعدات المزمع استخدامها في الحالات الطارئة ووسائط النسخ المساندة على مسافة آمنة بعيداً عن الموقع الرئيسي لتفادي التعرض لنفس الكارثة التي تلم بالموقع الرئيسي.

٢,١٤,٦,٣ التحكم بالدخول المادي

٢,١٤,٦,٣,١ يسمح لموظفي وموردي ومقاولي الجامعة بالدخول إلى المرافق المادية لدى الجامعة بما في ذلك مرافق معالجة المعلومات، و ذلك فقط بناءً على التعريف بأنفسهم والتحقق من هويتهم وفقاً لإجراءات منح صلاحية الدخول المادي.

٢,١٤,٦,٣,٢ يتم اعتماد الوصول إلى المناطق الآمنة والمقيدة من قبل المسئول عن النشاط/ تقنية المعلومات. ويكون الدخول إلى المناطق التي تتمتع بتصنيف أمني مرتفع مثل مركز البيانات محصوراً على الأشخاص الذين لديهم مسئولية مباشرة عن تشغيل وصيانة مركز البيانات .

٢,١٤,٦,٣,٣ يجب أن يُطلب من موظفي وموردي ومقاولي الجامعة والزوار الآخرين أن يضعوا شارة تعريفية فريدة أثناء تواجدهم في مرافق الجامعة بشكل دائم.

٢,١٤,٦,٣,٤ ينبغي أن يوقع كل زائر على سجل الزوار الذي يتم الاحتفاظ به لزوار الجامعة. يجب أن يتم توثيق اسم الزائر وشركته والغرض من الزيارة ووقت الدخول ووقت المغادرة والتاريخ في ذلك السجل.

٢,١٤,٦,٣,٥ يمنع منعاً باتاً مشاركة الموظفين بعضهم باستخدام بطاقة الدخول إلى منشآت العمل.

٢,١٤,٦,٣,٦ يجب عدم وضع أدلة الهاتف والوثائق الداخلية المستخدمة في تحديد مواقع مرافق المعالجة الحساسة في مكان يسهل الوصول إليها من قبل الموظفين الداخليين والخارجيين الذي ليست لديهم الصلاحيات الأمنية المطلوبة.

٢,١٤,٦,٣,٧ يجب مرافقة جميع الزوار أثناء تجوالهم في المناطق الآمنة من قبل موظفي الجامعة.

٢,١٤,٦,٤ فحص مواد أمن المعلومات/ والمواد الداخلة إلى والخارجة من المناطق الآمنة

٢,١٤,٦,٤,١ يتعين القيام بتفتيش المواد الداخلة إلى والخارجة من الجامعة قبل نقلها من مناطق الدخول العامة إلى نقطة استخدامها. ويجب أن يتم التصريح رسمياً بجميع طلبات النقل من قبل المسئول عن المعلومات وتسجيلها من قبل موظفي الأمن المادي.

٢,١٤,٦,٥ صيانة البنية التحتية للأمن المادي والبيئي

٢,١٤,٦,٥,١ ينبغي أن تتم صيانة وإصلاح معدات الجامعة من قبل موظفي صيانة مصرح لهم ومؤهلين للقيام بذلك.

٢,١٤,٦,٥,٢ يتعين على الجامعة التفويض بمراقبة والتحكم بأي أنشطة صيانة وأنشطة تشخيصية يتم تنفيذها محلياً أو عن بعد. كما أن عليها مراقبة كافة عمليات الصيانة المحلية/ و التي تتم عن بعد والأنشطة التشخيصية، وعلى موظفي الجامعة المعنيين مراجعة سجلات الصيانة للأنشطة البعيدة.

٢,١٤,٦,٦ الحماية من الحريق

٢,١٤,٦,٦,١ تضطلع إدارة الأمن والسلامة بمسئولية الاستجابة لحوادث الحريق الطارئة وإجراء تمارين للتعامل مع الحريق.

٢,١٤,٦,٦,٢ ينبغي إجراء تمارين التعامل مع الحريق بشكل ربع سنوي. كما ينبغي مراقبة تلك التمارين، وتزويد جميع المشاركين بإفادات تتعلق بمساهمتهم وأدائهم.

٢,١٤,٦,٦,٣ تقوم إدارة الأمن والسلامة بتحديد المواقع الحرجة التي سيتم تجهيزها بطفايات حريق يدوية. وعليه فإنه يتعين وضع بطاقات واضحة على تلك المناطق والتبليغ عن موقعها بشكل دوري لجميع الموظفين أثناء التدريب التوعوي واستخدام النشرات الموجزة.

٢,١٤,٦,٦,٤ كجزء من تدابير الأمن المادي المطلوبة أثناء الإخلاء بسبب الحريق، يتم تجهيز أبواب مخارج الحريق لتفتح من الداخل فقط. كما ينبغي إعداد إنذارات الحريق لتنطلق فوراً عند فتح مخرج الطوارئ.

٢,١٤,٦,٧ مراقبة الأمن المادي والبيئي

٢,١٤,٦,٧,١ يجب أن تتأكد الجامعة من مراقبة ضوابط الأمن المادي والبيئي لديها بما يتوافق مع مستويات تصنيف المخاطر لبيئة الأمن المادي ذات العلاقة.

٢,١٤,٦,٧,٢ تقوم إدارة الأمن والسلامة بتطوير خطة مراقبة الأمن المادي والبيئي المبنية على المخاطر، والتي تحدد ضوابط الأمن المادي والبيئي الواجب مراقبتها والمسئوليات التي سيتم تحديدها بهذا الصدد.

٢,١٤,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١٥ النسخ الاحتياطية والاسترجاع في حالة الكوارث

٢,١٥,١ الغرض

الغرض من هذه السياسة هو التأكد من أن يتم عمل نسخ مساندة للمعلومات الإلكترونية و استرجاعها لدى الجامعة بشكل مخطط وسريع وفعال وآمن بناء على متطلبات العمل.

٢,١٥,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,١٥,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١٥,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١٥,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١٥,٦ قيود سياسة أمن المعلومات

٢,١٥,٦,١ متطلبات النسخ الاحتياطية

٢,١٥,٦,١,١ يتم اخذ نسخ احتياطية من البيانات الإلكترونية المخزنة في أنظمة المعلومات لدى الجامعة بناءً على احتياجات العمل ووفقاً لإجراءات تطوير خطة النسخ الاحتياطية.

٢,١٥,٦,١,٢ يتم تخطيط النسخ الاحتياطية لأنظمة المعلومات بناءً على مستوى التصنيف الأمني للمعلومات (عالي، متوسط، عادي) والضوابط ذات الصلة الواردة في السياسة الأمنية للمعلومات.

٢,١٥,٦,١,٣ مديرو الأنظمة مسؤولون عن متابعة النسخ الاحتياطي لجميع أنظمة تقنية المعلومات التي يديرونها وذلك بالتنسيق مع مدير النسخ الاحتياطي، وذلك وفقاً لخطط النسخ الاحتياطية التي تم تطويرها لتلك الأنظمة.

٢,١٥,٦,١,٤ مدير النسخ الاحتياطي مسؤول عن أخذ النسخ الاحتياطية لجميع الأنظمة التي تم التبليغ عن حاجتها للنسخ الاحتياطي وذلك بالتنسيق مع مدراء أنظمة المعلومات.

٢,١٥,٦,١,٥ يكون جميع موظفي الجامعة مسئولين عن أخذ والحفاظ على نسخ احتياطية مساندة لجميع المعلومات الحساسة الموجودة في أجهزة الحاسوب الشخصية، والحواسيب المحمولة.

٢,١٥,٦,٢ وسائط النسخ الاحتياطية

٢,١٥,٦,٢,١ يجب استخدام وسائط مناسبة لتخزين النسخ الاحتياطية، بحيث التأكد من أنها خالية من الأخطاء وصالحة للاستخدام.

٢,١٥,٦,٢,٢ يجب استبدال وسائط تخزين النسخ الاحتياطية على الفور بعد مواجهة أي خطأ أو على فترات زمنية محددة مسبقاً أيهما يقع أولاً.

٢,١٥,٦,٢,٣ يتم وضع بطاقات مناسبة على وسائط تخزين النسخ الاحتياطية وترقيمها آلياً بواسطة نظام النسخ الاحتياطية أويقوم مدير النسخ الاحتياطي بذلك بترقيمها يدوياً . ويجب أن تتضمن بطاقات تعريف وسائط النسخ الاحتياطية المعايير التالية على الحد أدنى:

- اسم النظام.
- تاريخ استحداث النسخة.
- التصنيف من حيث الحساسية.
- معلومات الاتصال مع الجامعة.

٢,١٥,٦,٢,٤ يتوجب على مدير النسخ الاحتياطي متابعة استخدام وسائط النسخ الاحتياطية، على أن يتم استبدال تلك الوسائط بعد استخدامها بحسب عدد التكرار المنصوص عليه.

٢,١٥,٦,٣ الاحتفاظ بالبيانات

٢,١٥,٦,٣,١ يقوم مدير النسخ الاحتياطي بالتأكد من الاحتفاظ بنسخ احتياطية للبيانات الخاصة بجميع أنظمة المعلومات، للمدة المطلوبة من قبل الجامعة، أو بموجب متطلبات الجهة التنظيمية المعنية أو حسب متطلبات النظام.

٢,١٥,٦,٤ استرجاع النسخ الاحتياطية

٢,١٥,٦,٤,١ يتم استرجاع النسخ الاحتياطية على أساس الحاجة، وبناءً على تفويض مناسب من المسئول عن المعلومات.

٢,١٥,٦,٤,٢ يتم استرجاع النسخ الاحتياطية وفقاً لإجراءات استرجاع النسخ الاحتياطية.

٢,١٥,٦,٥ فحص استرجاع النسخ الاحتياطية

٢,١٥,٦,٥,١ يقوم مدير النسخ الاحتياطي بإجراء اختبارات على استرجاع النسخ الاحتياطية على عينة من البيانات المخزنة في النسخ الاحتياطية بشكل دوريً للتأكد من قابليتها للاسترجاع وبالتنسق مع مدراء أنظمة المعلومات.

٢,١٥,٦,٥,٢

٢,١٥,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١٦ شراء وتطوير أنظمة المعلومات

٢,١٦,١ الغرض

الغرض من هذه السياسة هو التأكد من التكامل الأمني طوال دورة حياة شراء وتطوير أنظمة المعلومات لدى الجامعة.

٢,١٦,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,١٦,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١٦,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١٦,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١٦,٦ قيود سياسة أمن المعلومات

٢,١٦,٦,١ التخطيط المسبق لمتطلبات أمن المعلومات القائمة على المخاطر

٢,١٦,٦,١,١ ينبغي على الجامعة أن تطور وتحافظ على وثيقة متكاملة لإدارة دورة حياة تطوير النظام لجميع عمليات تطوير الأنظمة والتطبيقات. وتشمل وثيقة دورة حياة تطوير النظام بحد أدنى ما يلي:

- بدء المشروع (التخطيط)
- تحديد المتطلبات (التحليل)
- تصميم النظام
- تطوير النظام
- الفحص
- التنفيذ والدعم

٢,١٦,٦,١,٢ يجب تحديد المتطلبات الأمنية لأنظمة معلومات الجامعة بشكل مسبق كجزء من مرحلة التخطيط وتحليل المتطلبات في دورة حياة تطوير/ شراء النظام.

٢,١٦,٦,١,٣ يجب تبرير المتطلبات الأمنية والموافقة عليها وتوثيقها كجزء من الدراسة العملية الشاملة لكل نظام من أنظمة المعلومات.

٢,١٦,٦,١,٤ على الجامعة أن تقوم بتخطيط متطلبات أمن المعلومات استناداً إلى المخاطر. وعليه فإنه ينبغي التخطيط لمتطلبات أمن المعلومات لكل من أنظمة المعلومات بناءً على مستويات تصنيفها الأمني (مرتفع، متوسط، عالي) و كذلك الأخذ بكل من الضوابط في المعايير الأمنية المحددة لكل نظام لدى الجامعة وأفضل الممارسات المطبقة بهذا الصدد.

٢,١٦,٦,١,٥ على إدارة تقنية المعلومات أن تقوم بالتعاون مع إدارة أمن المعلومات بتحديد المتطلبات الأمنية لأنظمة المعلومات لدى الجامعة.

٢,١٦,٦,٢ الأمن في تطوير/ تنفيذ أنظمة المعلومات

٢,١٦,٦,٢,١ تتأكد إدارة تقنية المعلومات من التطبيق الملائم للمتطلبات الأمنية المحددة لنظام المعلومات أثناء دورة حياة تطوير/شراء ذلك النظام.

٢,١٦,٦,٢,٢ تخضع أنظمة المعلومات لدى الجامعة إلى التقييم/ الفحص الأمني في مرحلة التنفيذ. ويتم إجراء التقييم/ الفحص الأمني وفقا لتصنيف المخاطر لنظام المعلومات، ومعايير الأمن المحددة للنظام المعني وأفضل الممارسات المطبقة بهذا الصدد لدى الجامعة.

٢,١٦,٦,٢,٣ ينبغي أن يتم تغيير أسماء المستخدمين وكلمات المرور الافتراضية لجميع أنظمة المعلومات عند إعداد الأنظمة التي تم شراؤها وقبل تطبيقها.

٢,١٦,٦,٢,٤ يتم مراقبة نتائج بيانات الاختبارات الأمنية وحمايتها من الدخول غير المصرح به إليها.

٢,١٦,٦,٣ الإعدادات الأساسية

٢,١٦,٦,٣,١ يتعين على الجامعة تطوير وتوثيق والحفاظ على وجود إعدادات أساسية حديثة لنظام المعلومات الجديد.

٢,١٦,٦,٣,٢ يتعين على الجامعة تحديث الإعدادات الأساسية لنظام المعلومات كجزء متكامل من عملية تركيب أجزاء نظام المعلومات.

٢,١٦,٦,٤ أمن وثائق النظام

٢,١٦,٦,٤,١ يجب أن يقتصر الوصول إلى وثائق تصميم وتطوير عمليات النظام على الأشخاص المصرح لهم فقط والذين يؤدون مهام رسمية.

٢,١٦,٦,٥ اعتبارات أمنية عند إجراء تعديلات على أنظمة المعلومات

٢,١٦,٦,٥,١ تقوم إدارة تقنية المعلومات بتحديد و التعامل مع عواقب أمن المعلومات المتعلقة بأي تغييرات أساسية في الأنظمة لدى الجامعة وذلك قبل إجرائه.

٢,١٦,٦,٦ اعتبارات أمنية إضافية عند شراء أنظمة مطورة في دول أجنبية

٢,١٦,٦,٦,١ قبل شراء/حيازة أي نظام من أنظمة المعلومات، فإن على الجامعة أن تتأكد من الالتزام بالأنظمة والقوانين واللوائح المتعلقة بهذا الموضوع و كذلك الالتزام بإجراءات المشتريات الحكومية المتبعة في المملكة بخصوص حيازة، أو شراء، أو تطوير، أو تصنيع أنظمة المعلومات من الدول الأجنبية.

٢,١٦,٦,٦,٢ لا يجوز للجامعة حيازة/شراء أي نظام معلومات تم تطويره/ تصنيعه لدى دولة غير صديقة وفقاً للسياسات والإجراءات الحكومية في المملكة.

٢,١٦,٦,٦,٣ يتطلب قيام طرف ثالث بتطوير/ تنفيذ أنظمة معلومات ذات مخاطر حساسة وذات مخاطر عالية ما يلي:

- إخضاع نظام المعلومات قبل قبوله إلى الاختبارات الأمنية الدقيقة (بما في ذلك مراجعة الشفرة المصدرية عندما ينطبق ذلك).
- أن يكون لدى موظفي تصميم/ تنفيذ النظام المعني التابعين للطرف الثالث تصاريح أمنية للعمل في المشاريع الحكومية السعودية.

٢,١٦,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١٧ إدارة التغيير

٢,١٧,١ الغرض

الغرض من هذه السياسة هو التأكد من التحكم الفعال بجميع التغييرات التي تطرأ على أنظمة المعلومات الرئيسية كي يتسنى الحد من احتمالات انقطاع أو توقف خدمات تقنية المعلومات أو الغش والتحايل الناشئ عن التغييرات غير المصرح بها لأنظمة المعلومات.

٢,١٧,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,١٧,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١٧,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١٧,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١٧,٦ قيود سياسة أمن المعلومات

٢,١٧,٦,١ معايير التغيير

٢,١٧,٦,١,١ يجب أن تتأكد الجامعة من أن تتم الإشراف والسيطرة على جميع التغييرات بشكل رسمي بما في ذلك التغييرات الاعتيادية أو التغييرات الطارئة على أنظمة المعلومات الرئيسية لدى الجامعة أثناء وجودها في بيئة العمليات/ الإنتاج. كما ينبغي أن يتم تسجيل وتقييم التغييرات واعتمادها قبل تنفيذها، ومراجعتها بعد تنفيذها و مقارنتها بالنتائج التي قد تم التخطيط المسبق من أجلها.

٢,١٧,٦,١,٢ ينبغي على الجامعة أن تحدد فئات طلبات التغيير لديها بناءً على مدى أهميتها وحسبما هو موضح أدناه:

- التغيير الاعتيادي: وهي التغييرات على أنظمة المعلومات التي تتطلب فترة مسبقة للمراجعة واعتماد طلب التغيير قبل تنفيذها.
- التغيير الطارئ: وهي التغييرات التي يوجد لها أولوية نظراً لأهمية إجرائها بشكل مستعجل، وإلا فإنها قد تسبب أثراً سلبياً كبيراً على خدمات تقنية المعلومات الرئيسية. وهذا النوع من التغييرات يعطى الأولوية على التغييرات العادية ولا يخضع لمعاييرها نظراً لضيق الوقت ووجوب إجرائه بأسرع ما يمكن.

٢,١٧,٦,٢ التغييرات العادية

٢,١٧,٦,٢,١ يتعين على الجامعة أن تأخذ في اعتبارها آثار التغيير على أمن المعلومات، وأن تتخذ إجراءات التخفيف المناسبة للحد من الآثار المترتبة على التغيير.

٢,١٧,٦,٢,٢ قبل اعتماد وتنفيذ أي تغيير على أنظمة المعلومات، فإنه يجب التأكد من تحديد نظام/ أنظمة المعلومات الأخرى التي قد تتأثر جراء التغيير، وأنه يتم إشراك المسئولين والراعين لتلك الأنظمة في العملية, والحصول على الاعتماد المناسب منهم على تنفيذ التغيير/التغييرات.

٢,١٧,٦,٢,٣ يسمح فقط بإجراء التغييرات المصرح بها على إعدادات أنظمة المعلومات لدى الجامعة.

٢,١٧,٦,٢,٤ يتم اعتماد التغييرات العادية على البنية التحتية للتقنية من قبل عميد تقنية المعلومات .

٢,١٧,٦,٢,٥ يتم اختبار التغييرات في بيئة الفحص قبل التصريح بإصدار التغيير إلى بيئة الإنتاج.

٢,١٧,٦,٣ التغييرات الطارئة

٢,١٧,٦,٣,١ في حال إجراء تغييرات المهمات الحرجة و التي تتطلب إجراءات واستجابة طارئة، وجب أن يتم التجاوز مؤقتاً عن إجراءات إدارة التغيير العادي إلى الحد الذي يعتبر ضرورياً لضمان استمرارية الأعمال الأساسية لدى الجامعة.

٢,١٧,٦,٣,٢ وجب أن يتم مراجعة واعتماد التغييرات الطارئة من قبل صاحب الصلاحية الذي يعتمد طلب التغيير المستعجل، وهو عميد تقنية المعلومات في الجامعة الإسلامية.

٢,١٧,٦,٣,٣ يتم إجراء التغييرات الطارئة بشكل فعال وبالسرعة الواجبة وفقاً لإجراءات التغييرات الطارئة.

٢,١٧,٦,٣,٤ يتم استكمال إغلاق طلب التغيير وتوثيقه وذلك بعد الانتهاء من التغييرات الطارئة، على غرار الإجراءات المتبعة في حالة التغييرات العادية.

٢,١٧,٦,٤ متابعة وتقرير حالة التغيير

٢,١٧,٦,٤,١ يتم تبليغ طالبي التغيير وأصحاب المصالح المعنيين بآخر المستجدات بشأن حالة التغيير في أنظمة المعلومات.

٢,١٧,٦,٤,٢ تقوم إدارة تقنية المعلومات بإعداد وصيانة قاعدة بيانات لتسجيل طلبات تغيير أنظمة المعلومات والتغييرات المجراة على أنظمة المعلومات لدى الجامعة.

٢,١٧,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١٨ مراقبة أمن المعلومات

٢,١٨,١ الغرض

الغرض من هذه السياسة هو التأكد من أن مراقبة حالة أمن المعلومات المتعلقة بأنظمة المعلومات لدى الجامعة تتم بشكل دائم من خلال تخطيط ونشر أساليب أمنية ملائمة بما يتوافق مع المخاطر ومدى حساسية وأهمية أنظمة المعلومات.

٢,١٨,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,١٨,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١٨,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١٨,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١٨,٦ قيود سياسة أمن المعلومات

٢,١٨,٦,١ مراقبة أمن المعلومات بناءً على المخاطر

٢,١٨,٦,١,١ تقوم الجامعة بمراقبة أمن المعلومات بناءً على المخاطر التي تم اكتشافها.

٢,١٨,٦,١,٢ تقوم إدارة أمن المعلومات بالتخطيط لأنشطة المراقبة الأمنية باستخدام إجراءات مراقبة وتقييم أمن المعلومات.

٢,١٨,٦,١,٣ يتم تخطيط وتنفيذ مراقبة أمن المعلومات لأنظمة المعلومات بناءً على حساسية وأهمية وتصنيف المخاطر المتعلقة بأنظمة معلومات الجامعة حسبما تقتضي درجات التصنيف الأمني المعطاة لتلك الأنظمة (مرتفع، متوسط، عادي).

٢,١٨,٦,١,٤ يجب أن تحدد في وثيقة خطة المراقبة الأمنية المبنية على المخاطر الأشخاص الرئيسيين المعنيين والعمليات والضوابط المتعلقة بالتقنية الواجب مراقبتها بالنسبة لأي نظام مفرد أو مجموعة من أنظمة المعلومات، وذلك حسبما هو محدد في السياسة الأمنية المتعلقة بذلك النظام أو تلك الأنظمة والمتطلبات القانونية والنظامية الواجب تطبيقها وأفضل الممارسات الأخرى في هذا الصدد.

٢,١٨,٦,١,٥ تكون إدارة أمن المعلومات والإدارات الأخرى المعنية مسئولة عن مراقبة أمن المعلومات لأنظمة المعلومات لدى الجامعة بناءً على مسئولياتها المخطط لها والمتعلقة بالمراقبة الأمنية.

٢,١٨,٦,٢ إدارة التحديثات و ملفات الرقع الأمنية

٢,١٨,٦,٢,١ يقوم مدراء الأنظمة بالتأكد من أنه تم تحديد وفحص وتطبيق كافة الرقع والتحديثات الأمنية لكافة أنظمة المعلومات بالسرعة الواجبة ووفقاً لإجراءات إدارة التحديثات والرقع الأمنية.

٢,١٨,٦,٢,٢ حيثما يتطلب الأمر في حالة الخدمات الحساسة التي تعتمد على الإنترنت، فإنه يجوز للجامعة الاشتراك في خدمات المراقبة النشطة لدى طرف ثالث معروف ليحصل موظفو أمن المعلومات لدى الجامعة على إشعارات بشأن الأنشطة الغير مصرح بها عبر الإنترنت.

٢,١٨,٦,٣ تسجيل ومراقبة أحداث النظام

٢,١٨,٦,٣,١ ينبغي على الجامعة أن تتأكد من وجود آليات مناسبة في أنظمة معلوماتها لتسجيل الحوادث الأمنية تقتضيه خطط المراقبة الأمنية لتلك الأنظمة، ويشمل ذلك دون حصر:

- سجلات محاولات دخول النظام الناجحة والمرفوضة؛
- سجلات المحاولات الناجحة والمرفوضة للوصول للبيانات والموارد الأخرى؛
- التغييرات على إعدادات النظام؛
- استخدام الامتيازات؛

- استخدام وسائل وتطبيقات النظام؛
- الملفات التي تم الوصول إليها ونوع الوصول؛
- عناوين وبروتوكولات الشبكة المستخدمة؛
- سجلات الكشف عن / منع الاختراقات إلى النظام؛
- سجلات جدار الحماية؛
- سجلات أخطاء النظام؛
- النسخ الاحتياطية من البيانات وسجلات الاسترجاع؛

٢,١٨,٦,٤ التقارير الإدارية

٢,١٨,٦,٤,١ يجب أن يتم استخراج عدد ملائم من التقارير الإدارية بصفة شهرية وفي الأوقات المحددة، ومن ثم تقديمها إلى إدارة أمن المعلومات أو الإدارة المعنية لإطلاعهم بشأن الوضع الأمني الخاص بأنظمة المعلومات لدى الجامعة بشكل مستمر.

٢,١٨,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,١٩ الالتزام بالسياسات والإجراءات المحددة

٢,١٩,١ الغرض

الغرض من هذه السياسة هو التأكد من مراقبة الالتزام بالسياسات والمعايير والإجراءات الأمنية الخاصة بأمن المعلومات لدى الجامعة من قبل موظفيها والأطراف الثالثة العاملة معها.

٢,١٩,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,١٩,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,١٩,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,١٩,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,١٩,٦ قيود سياسة أمن المعلومات

٢,١٩,٦,١ الالتزام بالسياسات والمعايير الأمنية

٢,١٩,٦,١,١ من الواجب على جميع منسوبي الجامعة والأطراف الثالثة الأخرى العاملة معها الالتزام بسياسات وإجراءات ومعايير أمن المعلومات المحددة لدى الجامعة.

٢,١٩,٦,١,٢ يجب على جميع منسوبي الجامعة التأكد من التطبيق الفعال لسياسات ومعايير وإجراءات أمن المعلومات في الجامعة ضمن حدود مسئولياتهم.

٢,١٩,٦,٢ التبليغ عن قضايا عدم الالتزام

٢,١٩,٦,٢,١ يتوجب على جميع منسوبي الجامعة الذين يكتشفون قضايا عدم الالتزام بسياسات وإجراءات ومعايير أمن المعلومات للجامعة أن يبلغوا فوراً عن تلك الحوادث وفقاً لسياسة إدارة حوادث أمن المعلومات لدى الجامعة.

٢,١٩,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتباراً من تاريخ (اعتمادها)

٢,٢٠ إدارة الخدمات المقدمة من طرف ثالث

٢,٢٠,١ الغرض

الغرض من هذه السياسة هو التأكد من أن الجامعة تدير مخاطر أمن المعلومات التي قد تنجم عن أنشطة الأطراف الثالثة التي تقدم خدماتها للجامعة.

٢,٢٠,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٢٠,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,٢٠,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٢٠,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٢٠,٦ قيود سياسة أمن المعلومات

٢,٢٠,٦,١ إدارة العقود

٢,٢٠,٦,١,١ يجب توقيع عقد رسمي بين الجامعة وكافة الأطراف الثالثة التي تقدم خدماتها إلى الجامعة أو التي تستخدم أنظمة معلومات الجامعة.

٢,٢٠,٦,١,٢ يتم تقديم الضوابط المتعلقة بسياسات وإجراءات أمن معلومات الجامعة إلى المقاولين / الموردين الذي يتعين عليهم قراءة وفهم سياسات وإجراءات أمن المعلومات وتقديم إقرارهم بقبولها.

٢,٢٠,٦,١,٣ تحتفظ الجامعة بحقها في رفض خدمات أي موظفين تابعين لأي طرف ثالث بناءً على كفاءتهم الفنية وقدراتهم التنفيذية والاعتبارات الأمنية وأي جوانب أخرى متعلقة بهذا الصدد و التي يمكن اعتبارها مسببة لضرر الجامعة.

٢,٢٠,٦,٢ تبادل المعلومات

٢,٢٠,٦,٢,١ على الجامعة أن تفرض على جميع الأطراف الثالثة توقيع اتفاقية رسمية لاحترام السرية قبل مشاركتهم في معلوماتها.

٢,٢٠,٦,٣ إدارة أداء الأطراف الثالثة

٢,٢٠,٦,٣,١ في حالة إخلال الطرف الثالث للعقد، فعلى إدارة الجامعة اتخاذ الإجراء اللازم وذلك بموجب اتفاقية العقد الموقعة مع ذلك الطرف.

٢,٢٠,٦,٣,٢ تضطلع الإدارات المعنية لدى الجامعة والتي تحصل على الخدمات التي تم إسنادها إلى أطراف الثالثة مسئولة عن مراقبة وتقديم تقارير لأداء تلك ألأطراف مقارنة بمتطلبات العقد، وذلك بهدف توفير مرئيات بناءة لتحسين مستوى الخدمات المقدمة من ألأطراف الثالثة.

٢,٢٠,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)

٢,٢١ إدارة استمرارية النشاط

٢,٢١,١ الغرض

الغرض من هذه السياسة هو تحديد الإجراءات المناسبة الواجب اتخاذها لتخفيف آثار حدوث أي توقف أو انقطاع لأنشطة العمل، وحماية عمليات/ أنشطة العمل الحساسة من الآثار الناجمة عن إخفاق/ تعطل أنظمة المعلومات أو الكوارث، والتأكد من استعادة الأنظمة بأسرع ما يمكن.

٢,٢١,٢ مجال تطبيق السياسة

تنطبق هذه السياسة على منسوبي الجامعة وأي طرف ثالث سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم
تغطي هذه السياسة جميع بيئات أنظمة المعلومات التي تقوم الجامعة بتشغيلها أو تعاقدت الجامعة على تشغيلها مع طرف ثالث.

٢,٢١,٣ المسئول التنفيذي

عميد تقنية المعلومات في الجامعة الإسلامية

٢,٢١,٤ راعي وثيقة السياسة

مدير إدارة أمن المعلومات في عمادة تقنية المعلومات في الجامعة الإسلامية

٢,٢١,٥ إلزامية التنفيذ

في حالة مخالفة أي من منسوبي الجامعة أو طرف ثالث (موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة فسيتعرض لإجراءات نظامية وفقاً لسياسات الجامعة، وأنظمة ولوائح المملكة العربية السعودية، والتي تشمل- دون حصر - نظام العمل والعمال، ونظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية، وغيرها.

٢,٢١,٦ قيود سياسة أمن المعلومات

٢,٢١,٦,١ استمرارية النشاط وتقييم المخاطر

٢,٢١,٦,١,١ ينبغي على الجامعة أن تطبق إطاراً مناسباً لإدارة استمرارية النشاط للحد من التأثير الذي قد تتعرض له الجامعة، واسترجاع خسارة المعلومات التي فقدت أثناء الكوارث الرئيسية مثل الحريق، الفيضان، الهزات الأرضية، العواصف، الأعطال الرئيسية لنظام تقنية المعلومات (الأجهزة)، فقد سجلات البيانات (البرامج)، فقد خدمات المنافع لفترة طويلة، الاضطرابات المدنية والإضرابات، فقد الموارد، القنابل، إلخ.

٢,٢١,٦,١,٢ يجب أن يستند تخطيط استمرارية النشاط على المخاطر المحددة التي من شأنها أن تسبب انقطاع عمليات/ خدمات النشاط، وعلى تحليل الآثار، لتحديد إمكانية وأثر تلك الانقطاعات من حيث الفترات الزمنية، ونطاق الضرر الواقع، وفترة الاستعادة.

٢,٢١,٦,١,٣ تقوم إدارة أمن المعلومات، بمشاركة كاملة من المسئولين عن العمليات/ الخدمات، وموارد العمل الأخرى بإجراء تقييم للمخاطر بصفة دورية، أو بعد وقوع تغيير رئيسي في بيئة أنظمة المعلومات، يتبعه تحليل الأثر.

٢,٢١,٦,١,٤ يجب أن يشتمل تقييم المخاطر على تحديد المخاطر وأولوياتها مقابل معايير وأهداف الجامعة، وأن يتضمن الموارد الهامة والحساسة، أثر انقطاع/ توقف العمل، الفترات المسموح بها لانقطاع الخدمة، وأولويات الاستعادة.

٢,٢١,٦,٢ إعداد وتنفيذ خطط استمرارية النشاط بما في ذلك أمن المعلومات

٢,٢١,٦,٢,١ يتم تقديم ترتيبات الطوارئ لتمكين عمليات/ خدمات النشاط (وخدمات معالجة المعلومات المساندة/ خدمات الشبكة) من الاستمرار في تأدية عملها بالسرعة الواجبة في حالة وقوع كارثة.

٢,٢١,٦,٢,٢ تتأكد إدارة الجامعة أن إدارة استمرارية النشاط لديها تتضمن الجوانب المتعلقة بأمن المعلومات، وتحديد التدابير الكافية لأمن أنظمة المعلومات.

٢,٢١,٦,٢,٣ تتأكد إدارة الجامعة من تحديد الموارد المالية والتنظيمية والفنية والبيئية الكافية لتلبية متطلبات أمن المعلومات من أجل استمرارية النشاط.

٢,٢١,٦,٢,٤ يكون مدراء الإدارات مسئولين عن وضع وتطبيق خطط استمرارية النشاط في إداراتهم.

٢,٢١,٦,٢,٥ يتم خزن وحفظ خطط استمرارية النشاط في موقع بعيد، على مسافة مناسبة للنجاة من أي ضرر تحدثه الكوارث في الموقع الرئيسي. كما يجب أن يتم حفظ المواد الأخرى الضرورية لتنفيذ حفظ استمرارية النشاط في موقع بعيد.

٢,٢١,٦,٣ إطار تخطيط استمرارية النشاط

٢,٢١,٦,٣,١ يجب أن يشتمل إطار تخطيط استمرارية العمل لدى الجامعة على العناصر التالية:

- شروط تنشيط الخطط (أي كيفية تقييم الوضع، ومن سيتم إشراكه في ذلك، وخلافه) وذلك قبل تنشيط كل خطة من الخطط.
- إجراءات الطوارئ التي تصف الإجراء الفوري الواجب اتخاذه عقب وقوع الحادثة ذات التأثير السلبي على عمليات النشاط و/أو حياة الأشخاص. ويتضمن ذلك ترتيبات التعامل مع وسائل الإعلام (لتفادي أو الحد من الخسارة) والتنسيق الفعال مع السلطات المحلية المناسبة (كالشرطة، وخدمات الإطفاء، والإدارات الحكومية المحلية).
- إجراءات الإنقاذ لنقل أنشطة العمل الضرورية أو خدمات الدعم إلى مواقع بديلة مؤقتة وإعادة تشغيل العمليات ضمن الأطر الزمنية المطلوبة.
- إجراءات استئناف العمليات الاعتيادية.
- جدول صيانة ومتابعة الخطة الذي يحدد كيف ومتى سيتم فحص الخطة، وعملية إدامتها.
- أنشطة التوعية والتعليم المصممة لفهم واستيعاب عمليات استمرارية النشاط والتأكد من استمرارية فاعلية العمليات.
- مسئوليات الأشخاص، التي تصف من المسئول عن تنفيذ كل جزئية واردة في الخطة. كما يجب تسمية البدلاء المطلوبين، فضلاً عن معلومات الاتصال مثل أرقام هواتف وعناوين هؤلاء الأشخاص.
- أنظمة وموارد المعلومات الحساسة المطلوبة كي يتسنى تنفيذ الإجراءات الطارئة وإجراءات الإنقاذ واستعادة النشاط.

٢,٢١,٦,٤ فحص، وإبقاء، وإعادة تقييم خطط استمرارية النشاط

٢,٢١,٦,٤,١ يجب فحص خطط استمرارية النشاط بشكل منتظم للتأكد من تحديثها وفاعليتها. ويتعين وضع جدول فحص استمرارية النشاط، يوضح كيف سيتم فحص كل عنصر من عناصر الخطة، ويتعين على الجامعة فحص خطة الطوارئ في الموقع البديل لإطلاع موظفي الطوارئ بالمرافق والمصادر المتاحة لتقييم قدرات وإمكانيات الموقع لدعم عمليات الطوارئ.

٢,٢١,٦,٤,٢ يتم الحفاظ على خطة استمرارية النشاط وإدامتها من خلال المراجعات والتحديثات المستمرة، نظراً للتغييرات التي تطرأ على بيئة النشاط، مثل:

- الموظفين.
- العناوين وأرقام الهواتف.

- إستراتيجية العمل.
- المواقع، والمرافق، والموارد.
- التشريعات.
- المقاولين، والموردين، والعملاء الرئيسيين.
- العمليات القائمة أو الجديدة أو المسحوبة.
- المخاطر (التشغيلية والمالية).

٢,٢١,٦,٥ موقع التخزين البديل

٢,٢١,٦,٥,١ يجب أن يكون لدى الجامعة موقعاً بديلاً للتخزين/ المعالجة، وذلك بناءً على نتائج تحليل أثر النشاط وإستراتيجية الإنقاذ.

٢,٢١,٧ تاريخ نفاذ السياسة

يبدأ نفاذ تطبيق هذه السياسة اعتبارً من تاريخ (اعتمادها)