برنامج التعاملات الإلكترونية الحكومية
e-Government Program

الإرشادات المقترحة لأمن الاتصالات وتقنية المعلومات في الجهات الحكومية

إخلاء مسؤولية

يبذل برنامج التعاملات الإلكترونية الحكومية أقصى جهوده لتحقيق مستوى عالي من الجودة والدقة لمحتويات هذه الوثيقة، إلا أنه لا يتحمل أية مسئولية أو تبعات قد تنتج إثر الاستفادة من المعلومات الواردة فيها. ويسر البرنامج تلقي مشاركاتكم بالإبلاغ عن أية مقترحات لتحسين وتطوير هذه الوثيقة من خلال وسائل الاتصال المنشورة في صفحة "اتصل بنا" على موقع البرنامج.

الإصدار: ١,٠
التاريخ: ١٤٢٨/١١/٢٤هـ

فهرس المحتويات

١ مقدمة ٣

١-١ الهدف ٣
١-٢ المسؤوليات ٤

٢ السياسات ٥

٢-١ سياسة أمن المعلومات ٥
٢-٢ سياسة تقدير المخاطر ٥
٢-٣ سياسة إدارة الأصول ٦
٢-٤ تنظيم أمن المعلومات ٧
٢-٥ سياسة الموارد البشرية ٨
٢-٦ سياسة الدخول ٨
٢-٧ الأمن المادي والبيئي ٩
٢-٨ إدارة الاتصالات والعمليات ١٠
٢-٩ اقتناء نظم المعلومات وتطويرها وصيانتها ١١
٢-١٠ سياسة إدارة الحوادث الأمنية ١٢
٢-١١ سياسة إدارة استمرارية العمل ١٣
٢-١٢ سياسة الالتزام ١٤

٣ قائمة مرجعية ١٥

١ مقدمة

تتسم عملية اختيار ونشر الضوابط الأمنية المناسبة بالأهمية، ويمكن أن ينجم عن تنفيذ هذه المهمة ملابسات تتعلق بعمليات أية جهة حكومية وأصولها، وكذلك بالمزايا المتحققة للأفراد. والضوابط الأمنية هي عملية الإدارة، والتشغيل، والحماية التقنيّة أو التدابير الوقائية الموصى بها لنظام المعلومات، بهدف حماية النظام وضمان سريته وسلامته، وتوافر معلوماته.

ويتوجب على الجهات الحكومية، استخدام الضوابط الأمنية لتلبية المتطلبات الأمنية التي حددها النظام الحكومي من خلال الأوامر التنفيذية، أو التوجيهات، أو السياسات، أو المعايير، أو اللوائح.

وتواجه الجهات الحكومية تحديات على صعيد تحديد مجموعة الضوابط المناسبة، التي لو تم تطبيقها بحزم وفعالية، فإنها ستلبي المتطلبات الأمنية بالإضافة إلى كونها مجدية اقتصاديًا.

إن اختيار الضوابط الأمنية المناسبة التي تلبي المتطلبات المحددة، وأحيانا الفريدة للجهة للحكومية، هي مهمة غاية في الأهمية، حيث تعكس هذه المهمة التزام الجهة الحكومية بالأمن والجهود المخلصة المبذولة في سبيل حماية نظم المعلومات التابعة للجهة وضمان توافرها وسريتها وسلامتها.

ولكي يمكن مساعدة الجهات الحكومية في القيام بالاختيار المناسب لنظم المعلومات الخاصة بها، فقد تم استحداث الضوابط الأساسية، وهي بمثابة الحد الأدنى من الضوابط الأمنية التي يوصى باستخدامها في نظم المعلومات.

١-١ الهدف

تهدف هذه الوثيقة إلى توفير الإرشادات المتعلقة باستخدام الضوابط الأمنية لنظم المعلومات وتحديدها من قبل الجهات الحكومية في المملكة العربية السعودية، حسب الضابط رقم (٢١) من ضوابط تطبيق التعاملات الإلكترونية الحكومية في الجهات الحكومية الصادرة بقرار مجلس الوزراء رقم (٤٠) وتاريخ ١٤٢٧/٢/٢٧ (للإطلاع على ضوابط تطبيق التعاملات الإلكترونية الحكومية، راجع الموقع: http://www.yesser.gov.sa).

وتنطبق هذه الوثيقة على كافة المكونات والعناصر الخاصة بأي نظام للمعلومات يقوم بمعالجة، وتخزين، أو بث المعلومات الحكومية، كما أنها تساعد على الوصول إلى نظم معلومات محمية أمنيًا، وذلك من خلال:

- تبني أسلوب يتسم بالتجانس، وبقابليته للقياس، ولإعادة الاستخدام، في عملية اختيار وتحديد الضوابط الأمنية لنظم المعلومات.
- وضع التوصيات بخصوص الحد الأدنى من الضوابط الأمنية في نظم المعلومات، والواجب توافره ضمن النظم الحكومية للمعلومات.
- توفير فهرس للضوابط الأمنية الخاصة بنظم المعلومات يتسم بالاستقرار والمرونة، بحيث يفي باحتياجات الحماية الحالية للجهات الحكومية، وبالمطالبات المتعلقة بتوفير الحماية المستقبلية على أساس الاحتياجات والتقنيات المستجدة.
- تأسيس قاعدة لتطوير مبادئ التقدير وإجراءات تحديد فعالية الضوابط الأمنية.

١-٢ المسؤوليات

بهدف توفير الحماية الأساسية للمعلومات الوطنية والمعلومات التي تتاح للعموم، ينبغي على الجهات الحكومية العمل على وضع:

١. سياسة رسمية موثقة تشمل الهدف، والنطاق، والأدوار والمسئوليات والالتزامات.
٢. إجراءات رسمية موثقة، بهدف تسهيل عملية تطبيق السياسة والضوابط المرتبطة بها.

ومن ثم العمل على نشرها، والقيام بمراجعتها وتحديثها بصفة دورية.

٢ السياسات

نورد فيما يلي السياسات الأمنية المتوافقة مع المعايير الأمنية التي يتيحها المعيار العالمي ISO 27001، ويمكن للجهات الحكومية البدء في تنفيذ هذه السياسات بوصفها الحد الأدنى. ومن ثم يمكن لهذه الجهات الشروع في وضع الإجراءات بناءً على المتطلبات والسياسات المختارة.

٢-١ سياسة أمن المعلومات

يعتبر وجود سياسة لأمن المعلومات أمر حيوي لكافة الجهات الحكومية. وتهدف هذه السياسة إلى حماية كافة موارد البيانات من الفقدان الناجم عن خرق السرية، والسلامة، والتوافر. ويجب ألا ينظر إلى هذه السياسة على أنها قد تحول دون أداء العمليات اليومية، أو أنها قد تؤدي إلى تقييد هذه العمليات. بل يجب التعامل معها كآلية للاشتراك الآمن في المعلومات. وتعمل السياسة الأمنية على حماية المعلومات من مجموعة كبيرة من التهديدات، وذلك بهدف ضمان استمرارية العمل، والحد من الأضرار، ورفع مستويات الاستفادة من نظم المعلومات إلى أقصى حد.

وتغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- تحديث التوثيق الخاص بأمن المعلومات.
- تعديل التوثيق الخاص بأمن المعلومات.
- ضبط التغييرات على التوثيق.
- تعقب التوثيق.

٢-٢ سياسة تقدير المخاطر

لقد أدى تزايد استخدام التقنية، والتراجع الأمني الذي واكب ذلك، إلى تعاظم الإحساس بالقلق في ظل التهديدات والمخاطر القائمة والمستجدة. ما قد يتسبب في عدم توافر المعلومات، أو انتهاك سريتها أو سلامتها، ويؤدي بالتالي إلى خسارة أو تأثر العوائد والخدمات المقدمة للعملاء، وكذلك العمليات أو السمعة.

وهنا يأتي دور وظيفة إدارة المخاطر، حيث أنها تعمل على تحديد مختلف المخاطر التي تكون الجهة الحكومية عرضة لها، وعلى تبني عملية إدارة المخاطر لتعظيم الفوائد التي يقدمها العمل.

ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **مخزون أصول تقنية المعلومات**

ينبغي لأي جهة حكومية إدامة مخزون كامل وشامل، وفي كافة الأوقات، من جميع الأصول المعلوماتية الخاصة بها. وفيما يلي الأصول التي يتوجب تسجيلها ضمن هذا المخزون:

- الأصول المعلوماتية.
- أصول البرمجيات.

- أصول الأجهزة.
- الموارد البشرية.
- الأصول المادية.
- الخدمات

- **تقدير المخاطر**

ينبغي لكافة الجهات الحكومية، وفي حدود المعقول، القيام بتحديد التهديدات الداخلية والخارجية المتوقعة، التي من شأنها التأثير على سلامة البيانات على الأنظمة المعلوماتية. وبالإضافة إلى ذلك، يتوجب على كافة الجهات تقييم احتمالية وإمكانية وقوع الضرر نتيجة لهذه التهديدات، مع أخذ مدى حيوية أو حساسية نظام أمن المعلومات بعين الاعتبار.

- **تصنيف المخاطر**

تؤدي عملية تصنيف المخاطر، إلى تمكين الجهة الحكومية من تركيز آليات حماية الأصول، على تلك الأصول التي تعتبر عرضة أكثر من غيرها لمخاطر معينة. وسيتم تصنيف الأصول المعلوماتية بناءً على مدى قابليتها للتعرض للمخاطر. وفيما يلي نورد المخاطر التي توثر في المعلومات:

- فقدان السرية.
- تأثر سلامة المعلومات.
- عدم توافر المعلومات.

- **المستويات المقبولة للخطر**

يقع على عاتق الإدارات في الجهات الحكومية، مسئولية تحديد المستوى المقبول من المخاطر، حيث أن الإدارة على اطلاع على محركات العمليات في الجهة، وعلى معرفة بالتأثيرات التي قد تنجم فيما لو لم يتم تلبية الأهداف المتصلة بالعمليات. كما يقع –أيضًا –على عاتق الإدارة المسئولية الكلية لضمان تحقيق الجهة للأهداف المتعلقة بالعمل. ويتمثل دور "ضابط أمن المعلومات" في إحاطة الإدارة بالتأثيرات السلبية للمخاطر الأمنية الكامنة فيما يختص بتحقيق أهداف الجهة الحكومية.

٢-٣ سياسة إدارة الأصول

لا تتساوى كافة الأصول، في جميع الجهات الحكومية، من حيث أهميتها على صعيدي العمليات وتحقيق رؤية الجهة ومهمتها. فأهمية بعض الأصول تفوق أهمية الأصول الأخرى، ومن هنا فإنها بحاجة إلى عناية وحماية إضافيتين، مما يوجب تصنيف الأصول المعلوماتية طبقًا لذلك.

وستؤدي عملية التصنيف إلى تمكين الجهة الحكومية من تركيز آليات حماية الأصول على تلك الأصول التي تكون عرضة أكثر من غيرها لمخاطر محددة. وسيتم تصنيف الأصول المعلوماتية طبقًا لاحتمالات تعرضها للمخاطر.
ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **معايير تصنيف الأصول**

لا تتساوى كافة الأصول في جميع الجهات الحكومية من حيث أهميتها على صعيدي العمليات وتحقيق رؤية الجهة ومهمتها. فأهمية بعض الأصول تفوق أهمية الأصول الأخرى، ومن هنا فإنها بحاجة إلى عناية وحماية للحفاظ على العمليات الخاصة بالجهة، وستعمل هذه الوثيقة على توفير المعايير التي على أساسها سيتم تصنيف الأصول.

- **مستويات التصنيف**

يجب أن يتم تصيف كافة البيانات، والتوثيق الخاص بها، طبقًا لمستوى سريتها، وحساسيتها، وقيمتها وحيويتها للجهة.

- **خطة التصنيف**

يتم تصنيف المعلومات لتوضيح الحاجة للحماية، وأولوياتها، ودرجتها. ويجب وضع وتبني خطة محددة لتصنيف الأصول الموجودة في بيئة الجهة، أو التي سيتم استحداثها فيها.

٢-٤ تنظيم أمن المعلومات

ترمي هذه السياسة إلى إدارة أمن المعلومات ضمن أي جهة حكومية، والعمل على إدامة ضوابط أمنية مناسبة لوسائل معالجة المعلومات والمرافق الموجودة لديها، أو التي عُهد بها إلى طرف ثالث.

ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **منتدى إدارة الأمن**

يجب أن تعمل كافة الجهات الحكومية على تشكيل لجنة لأمن المعلومات، وذلك لضمان توفر التوجيه والإسناد الإداري الملائمين لكافة المبادرات الأمنية.

- **الأدوار والمسئوليات المرتبطة بأمن المعلومات**

يقع على كاهل " لجنة أمن المعلومات" في أي جهة حكومية، مسئولية صياغة الإجراءات الخاصة بتحديد الأدوار والمسئوليات المرتبطة بأمن المعلومات على مستوى الجهة.

- **التفويضات ذات الصلة بأمن المعلومات**

ينبغي السعي في كافة الجهات الحكومية لاستصدار تفويض من الإدارة بخصوص أية تغييرات أو إضافات على وسائل معالجة المعلومات.

٢-٥ سياسة الموارد البشرية

يعتمد جزء مهم من أمن المعلومات على السياسات ذات الصلة بإدارة الموارد البشرية. ويمكن تحقيق الأهداف الخاصة بأمن المعلومات، وإلى حد بعيد، من خلال إدراج بنود محددة في عقود الموظفين، ومن خلال تطبيق التدابير المناسبة أثناء عملية التوظيف، أو ترك الموظفين للخدمة، أو في حالات إنهاء عقد موظف، مع تخصيص الواجبات والمسئوليات المناسبة ، بالإضافة إلى تدريب الموظفين وتوعيتهم بشكل متواصل.

ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **التدقيق الأمني على الموظفين وحفظ الملفات**

يجب القيام بعملية التدقيق الأمني عند التحاق الموظف بالعمل في الجهات الحكومية. وينبغي التحقق من كافة التفاصيل الشخصية للفرد الذي يتم توظيفه، وذلك قبل التحاقه بالجهة. وتتم عملية التدقيق الأمني من قبل إدارة الموارد البشرية.

- **القواعد العامة للتوظيف**

على إدارة الموارد البشرية في أي جهة حكومية ضمان أن "وصف الوظيفة" لكل مستخدم يتطلب منه الالتزام بكافة السياسات الأمنية في الجهة.

- **توعية وتدريب المستخدمين**

ينبغي أن يتلقى كافة موظفو الجهة الحكومية تدريباً في مجال التوعية الأمنية، وأن يلتزموا بأفضل الممارسات في أدائهم لعملهم.

- **تغيير الواجبات الوظيفية أو ترك العمل**

يجب أن تحتفظ إدارة الموارد البشرية في كافة الجهات الحكومية بتعليمات موثقة تتضمن التدابير الأمنية الملائمة فيما يتعلق بتغيير الواجبات الوظيفية، أو انتهاء خدمات الموظف.

- **المسائل القانونية والتعاقدية**

على كافة موظفي الجهات الحكومية أن يكونوا على معرفة بالعواقب ذات الصلة بالمسائل القانونية أو التعاقدية الناجمة عن عدم التزامهم بالتوجيهات الأمنية كما ينبغي، أو خرق السياسة الأمنية، أو تسريب المعلومات الحساسة للجهات الخارجية.

٢-٦ سياسة الدخول

تمتلك كافة الجهات الحكومية نظم للمعلومات وتقوم تشغيلها، وتستخدم هذه المعلومات من قبل مستخدمين بهدف إسناد العمليات الخاصة بالجهة ودعمها. وتتضمن نظم المعلومات الحاسبات الآلية الشخصية، والخوادم، والشبكات، والتطبيقات، والبيانات المخزنة في النظم وتعود ملكيتها جميعاً للجهة. وينبغي على كافة المستخدمين استخدام النظم بطريقة فعالة تتماشى مع المعايير الأخلاقية والقانونية.

ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **الاستخدام الملائم لنظم المعلومات**

يتم ضبط عملية الدخول إلى المعلومات على أساس متطلبات العمليات والأمن، بالإضافة إلى قواعد الضوابط الأمنية المحددة لكل نظام معلوماتي.

- **خدمات الإنترنت ونظم البريد الإلكتروني**

يقتصر استخدام الإنترنت والبريد الإلكتروني في الجهات الحكومية على الأغراض المتعلقة بالعمل فقط، وعلى المستخدمين المخولين الالتزام بالسياسة الأمنية ذات العلاقة.

- **آليات التشفير**

يجب تزويد كافة الموظفين الذين يقومون بعملية الدخول عن بعد، بوسيلة اتصال آمن (مثل طبقة المقاييس الآمنة SSL، أمن العناوين IPSec، شبكة خاصة افتراضية VPN، تشفير) إلى أي من شبكات نظم الجهة الحكومية.

- **كلمات السر**

ينبغي لكافة المستخدمين إتباع سياسة كلمة السر الخاصة بالجهة الحكومية، بخصوص طريقة استخدامهم وإدارتهم لكلمة السر الخاصة بهم.

- **كشف المعلومات الخاصة بالجهة**

يجب على الجهات الحكومية وضع كافة الضوابط الأمنية المتعلقة بالتحكم بالدخول إلى البيئة المعلوماتية التابعة لها، وذلك لضمان عدم كشف معلوماتها.

- **التخزين**

يجب على الجهات الحكومية ضمان تطبيق الضوابط الأمنية للحد من عمليات الدخول إلى مرافق وسائل التخزين الموجودة في البيئة التابعة للجهة.

٢-٧ الأمن المادي والبيئي

تهدف هذه السياسة إلى الحيلولة دون الدخول المادي، غير المصرح به، إلى المرافق، والأصول المعلوماتية، ونظم المعلومات التابعة للجهة، كما تقوم هذه السياسة بتناول موضوع المخاطر المادية والبيئية التي يمكن لها أن تلحق الضرر بسرية، وسلامة، وتوافر المعلومات ونظم المعلومات التابعة للجهة.

ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **المواضيع العامة ذات الصلة بالأمن المادي والبيئي**

يجب أن يتم تقسيم الموقع المادي، لمرافق وسائل معالجة المعلومات التابعة للجهة الحكومية، إلى مناطق. ويكون لكل منطقة مستويات مختلفة من قيود الدخول ومن المتطلبات المتعلقة بتخويل الدخول.

- **بناء المرافق وتصميمها**

يجب أن يتم تزويد كافة المرافق التابعة للجهات الحكومية، بتدابير كافية لاكتشاف ومكافحة الحريق، وبنظم للتكييف، التي يجب تطبيقها لضمان ملائمة بيئة العمل.

- **مراقبة وضبط الدخول المادي**

على كافة الجهات الحكومية ضمان نشر نظم للمراقبة بهدف تعقب أي أنشطة مثيرة للشك تقع ضمن النطاق المادي للجهة.

- **التحكم بدخول الأشياء وخروجها من المبنى**

ينبغي القيام بإجراء تفتيش للمواد، والإمدادات، والمعدات الداخلة إلى المبنى أو الخارجة منه، وأن يتم عند اللزوم تسجيلها طبقًا لسياسة الأمن المادي الخاصة بالجهة.

- **أمن مكان العمل**

على كافة الجهات الحكومية ضمان تنفيذ كافة الأعمال تحت إشراف الإدارة ذات العلاقة.

٢-٨ إدارة الاتصالات والعمليات

تهدف هذه السياسة إلى ضمان التشغيل الصحيح والآمن لوسائل معالجة المعلومات، وذلك بهدف الحد من المخاطر الناجمة عن تعطل النظم، وحماية سلامة هذه الوسائل وكذلك البرمجيات. كما تعمل هذه السياسة- أيضًا- على اقتراح التوجيهات اللازمة لضمان تشغيل الشبكة، وتبادل المعلومات بصورة آمنة في الجهة.

ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **إدارة العمليات**

يجب على كافة الجهات الحكومية، ضمان وجود كافة الإجراءات الخاصة بالعمليات اللازمة لإسناد أو تطبيق السياسات الأمنية، وأن يتم توثيق هذه الإجراءات وإدامتها. كما يجب العمل على ضبط كافة التغييرات على النظم من خلال إجراءات رسمية لإدارة التغيير.

- **الفصل بين مرافق الاختبار والتشغيل**

يجب اختبار النظم الجديدة في كافة الجهات الحكومية ضمن بيئة اختبار أو محاكاة، وأن تكون مفصولة تمامًا عن بيئة التشغيل.

- **سجلات المشغلين**

على كافة المشغلين في شبكة الجهة الحكومية، ومشغلي مركز عمليات الشبكة لديها، إدامة سجل بخصوص الأنشطة التي تصدر عنهم. وينبغي إخضاع هذه السجلات لعمليات تحقق منتظمة للتأكد من التزامهم بإجراءات التشغيل.

- **أمن التوثيق الخاص بالنظام**

يتوجب على كافة الجهات الحكومية ضمان تطوير، وإدامة، وحماية، التوثيق الخاص بالنظم أو التطبيقات الخاصة بإدارات الجهة الحكومية، التي يستخدمها المبرمجون والمشغلون والموظفون.

٢-٩ اقتناء نظم المعلومات وتطويرها وصيانتها

تهدف هذه السياسة إلى وضع المبادئ المتبعة في عملية اقتناء الأصول المعلوماتية وتطويرها وصيانتها للجهة الحكومية. وتعمل هذه السياسة على معالجة عملية تطوير أصول تقنية المعلومات وصيانتها، من قبل الموظفين التابعين للجهة، أو من قبل أطراف خارجية.

وينبغي أن يكون الأمن أحد الخصائص الرئيسة لنظم المعلومات التي يتم تطويرها واستخدامها من قبل الجهة. كما ينبغي أن يتم تصميم نظم المعلومات وتطويرها وربطها بالنظم الأخرى، وإدارتها ومراقبتها وتشغيلها بطريقة ترفع من مستويات ثقة العملاء، وضمان الالتزام بالإطار التنظيمي للجهة، وتوفير الدعم لأهدافها.

ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **اقتناء أو تطوير نظم المعلومات والتطبيقات.**

يجب أن تراعي عملية تطوير النظم المعلوماتية في كافة الجهات الحكومية، المنهجيات المتبعة، والتقنيات، والأدوات بما يتماشى مع أفضل الممارسات العالمية.

- **مبادئ تصميم نظم المعلومات**

في حالة اقتناء أو تطوير نظم معلومات جديدة في كافة الجهات الحكومية، من قبل إطراف خارجية، يقوم قسم تطوير نظم تقنية المعلومات بدراسة معمقة لتحديد المتطلبات.

- **الرموز البرمجية للمصدر (Source Code)**

لابد من توافر قيود صارمة على الدخول إلى الرموز البرمجية (Source Code)، لكي يمكن الحد من مخاطر التلف الجزئي أو الكلي لكافة التطبيقات التابعة للجهات الحكومية، بسبب القيام بتعديلات غير مصرح بها (عن قصد أو عن غير قصد).

- **اختبار وقبول نظم المعلومات**

يتوجب على كافة الجهات الحكومية بعد الانتهاء من عملية اقتناء نظام المعلومات أو تطويره، وقبل وضعه في بيئة الإنتاج، القيام بالمراجعة والاختبار الأمني للنظام باستخدام أساليب التهديد الممكنة بناءً على مدى حيوية النظام.

- **تركيب نظم المعلومات**

يجب وضع نظام المعلوماتية في بيئة الإنتاج بالجهات الحكومية من قبل موظفين لم يتولوا مسئولية تطوير النظام.

- **دليل تشغيل نظام المعلومات**

يجب العمل على تجهيز دليل النظام والتطبيق قبل وضعهما في بيئة الإنتاج، في كافة الجهات الحكومية.

- **تشغيل وصيانة نظام المعلومات**

يجب أن يتم تشغيل كافة النظم التابعة للجهات الحكومية طبقًا لذلك للسياسات المعتمدة، بالإضافة إلى إجراءات توثيق عمليات الصيانة والموافقة عليها.

- **سحب نظم المعلومات من الخدمة**

يجب أن يتم سحب كافة نظم المعلومات فقط عندما لا تكون هنالك ضرورة لاستخدامها، وليست هنالك حاجة (قانونية، أو تجارية، أو غير ذلك) لاسترجاع الملفات الموجودة في النظام.

٢-١٠ سياسة إدارة الحوادث الأمنية

تهدف هذه السياسة إلى تطوير إطار للتعامل بفعالية بدون تأخير مع الحوادث الأمنية. والحادثة الأمنية هي عبارة عن عملية انتهاك مشتبه بها أو مؤكدة، لسلامة المعلومات الحكومية وتوافرها أو سريتها التي تسببت في حدوث ضرر للجهة أو قد تتسبب في حدوثه.

وتتمثل عملية اكتشاف الحادثة الأمنية المحتملة في تحديد هذه الحادثة في حينها، بينما يتم في نفس الوقت، توفير الحماية من الحوادث الفعلية الرامية إلى تعريض الموقف الأمني الخاص بالجهة الحكومية للخطر.

ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **تحديد الحوادث الأمنية**

يجب أن يكون المستخدمون وموظفو تقنية المعلومات، في كافة الجهات الحكومية مسئولين عن تحديد الحوادث الأمنية والإبلاغ عنها.

- **تحجيم الحادثة الأمنية**

ينبغي على فريق التعامل مع الحوادث الأمنية، في الجهات الحكومية، وبالتعاون مع مالكي المعلومات، العمل على وضع أولويات للمهام التي يتوجب تنفيذها على صعيد التعامل مع الحادثة الأمنية.

- **كشف الحادثة الأمنية والتخلص منها**

ينبغي على فريق التعامل مع الحوادث الأمنية، في كافة الجهات الحكومية إجراء تدقيق أمني لنظم المعلومات ذات العلاقة، وذلك بهدف كشف نقاط الضعف الكامنة والتي تسببت في الحادثة الأمنية، أو أن تكون قد نجمت عن الحادثة الأمنية.

- **استرجاع نظم المعلومات**

عندما يتم التعامل في كافة الجهات الحكومية بنجاح مع الحادثة الأمنية، فإنه يتوجب على مدير تقنية المعلومات بالتعاون مع إداري النظام، القيام بالتحقق من الإعدادات الأمنية، وذلك للتأكد من ملائمة الآليات الأمنية.

- **تحليل الحادثة الأمنية**

عندما يتم، في كافة الجهات الحكومية، التعامل بنجاح مع الحادثة الأمنية، فإنه يتوجب القيام بتحليل واف، وتوثيق لها، بحيث يتم تغطية الأسباب، والآثار المباشرة أو غير المباشرة، والإجراءات التي تم اتخاذها.

- **الإجراءات القانونية والتأديبية**

عندما يتم، في كافة الجهات الحكومية، التأكد من أن أحد الموظفين قد تسبب في الحادثة الأمنية، فإنه يتوجب التحقق من الحالة، واتخاذ الإجراءات التأديبية أو القانونية المناسبة بحقه.

- **نقل المعلومات إلى الطرف الثالث**

يجب ألا يتم نقل المعلومات ذات الصلة بالحوادث الأمنية في كافة الجهات الحكومية إلى طرف ثالث (الجمهور، الصحفيين، وغيرهم).

٢-١١ سياسة إدارة استمرارية العمل

تهدف هذه السياسة إلى وضع الإطار الخاص بإدارة استمرارية عمل الجهة، وذلك للحد إلى المدى الممكن، من الآثار التي قد تنجم عن الانقطاع الممكن في أنشطة العمل، وضمان استمرارية العمليات الحيوية، وذلك في حالة التلف الجزئي أو الكلي.

ويجب أن تغطي هذه السياسة الفئات التالية، وذلك على سبيل المثال لا الحصر:

- **وضع إطار لتخطيط استمرارية العمل**

يجب الاحتفاظ بإستراتيجية أو إطار عمل واحد لخطط استمرارية العمل وذلك لضمان وجود التجانس، ووضع الأولويات في كافة الجهات الحكومية. ويجب أن تتضمن خطة استمرارية العمل، وبوضوح، المعايير الخاصة بتفعيل الخطة، وأن تورد أسماء الأفراد (ومن ينوب عنهم) المسئولين عن تنفيذ الخطة.

- **وضع خطة لاستمرارية العمل والتخطيط للتعافي من الكوارث**

يتوجب على كافة الجهات الحكومية إدارة إجراءات لتطوير استمرارية العمل والتعافي من الكوارث وإدامتها على مستوى الجهة. ويجب أن تعمل هذه الإجراءات على توطيد الصلة بين كافة العناصر الرئيسة الخاصة باستمرارية العمل والتعافي من الكوارث، وأن تكون منسجمة مع الأهداف والأولويات المعتمدة من قبل الجهة.

- **وضع وتطبيق آليات التعافي من الكوارث**

ينبغي أن تتضمن كل خطة، من خطط الجهات الحكومية، المعلومات الأساسية اللازمة للاستعداد، والتعافي من الحادثة الأمنية. وقد يتضمن ذلك إستراتيجية التعافي، ونتائج تحليل الآثار على العمل، وتفاصيل الفرق الخاصة بتحقيق التعافي، أو الأعضاء والمهام وغيرها.

- **إدارة عمليات الحفظ الاحتياطي**

يجب إجراء الحفظ الاحتياطي لكافة الجهات الحكومية بشكل منتظم، وذلك لضمان إمكانية استرجاع البيانات عند اللزوم، وأن يتم تحديد العناصر التي تتطلب القيام بالحفظ الاحتياطي بخصوص كل تطبيق من التطبيقات، وأن تتم جدولة مواعيد عمليات الحفظ الاحتياطي، وذلك للتأكد من أن هنالك نسخة من كافة البيانات الحيوية، دون التأثير على عمل النظام.

٢-١٢ سياسة الالتزام

تخضع معالجة المعلومات وتصميم نظم المعلومات وتشغيلها واستخدامها وإدارتها لضوابط تنظيمية، وكذلك للالتزامات التي تنجم عن الاتفاقيات المبرمة بين الجهة الحكومية والأطراف الثالثة. وتعمل هذه السياسة على بحث الالتزامات الأساسية التي تنبثق من الإطار التنظيمي الحالي الخاص بأمن المعلومات.

هذا، وتهدف هذه السياسة إلى تغطية ما يلي:

قد تخضع عملية تصميم نظم المعلومات وتشغيلها، واستخدامها، وإدارتها لمتطلبات تشريعية أو تنظيمية أو تعاقدية. ومن هذا المنطلق، فإنه ينبغي تحديد السياسات المناسبة والالتزام بها. ويعود الهدف من وراء ضمان الالتزام، إلى تجنب حدوث أي اختراقات للقانونين الجنائي والمدني، وللمتطلبات التشريعية، والتنظيمية. كما يؤدي ذلك إلي ضمان أن التقنيات التي يتم تطبيقها في كافة الجهات الحكومية، تتوافق مع المعايير والمراجعات الدورية، وأنه يتم القيام بعمليات التدقيق بخصوص:

- تحديد الإطار التنظيمي لأمن المعلومات.
- حماية البيانات الشخصية.
- سرية الاتصالات.
- حقوق الملكية الفكرية.
- تراخيص البرامج.
- التشفير.
- حماية المعلومات.
- مراقبة وتدقيق استخدام النظم.
- جمع الأدلة.
- عقود العمل.
- اتفاقيات الطرف الثالث.
- مواضيع أخرى.

٣ قائمة مرجعية

السياسة	أهمية السياسة	رقم إصدار السياسة	مالك السياسة
سياسة أمن المعلومات			
سياسة تقدير المخاطر			
سياسة إدارة الأصول			
مخزون الأصول			
تصنيف المعلومات			
عنونة المعلومات والتعامل معها			
تنظيم أمن المعلومات			
التزام الإدارة بأمن المعلومات			
تخصيص مسئوليات أمن المعلومات			
إدراج الأمن في اتفاقيات الطرف الثالث			
سياسة الموارد البشرية			
المسئولية الأمنية في دليل الموظف وفي عقد عمله			
التوعية بأمن المعلومات			
الإجراءات التأديبية			
سياسة الدخول			
تسجيل المستخدمين			
إدارة كلمة السر الخاصة بالمستخدم			
مراجعة صلاحيات دخول المستخدمين			
سياسة المكتب الخالي والشاشة الخالية			
الحوسبة والاتصالات النقالة			
الأمن المادي والبيئي			
ضوابط الدخول المادي			
تأمين المكاتب، والغرف، والمرافق			
دخول الجمهور، مناطق التحميل والتنزيل			
التخلص الأمن من المعدات أو إعادة استخدامها			
إدارة الاتصالات والعمليات			
إجراءات التشغيل الموثقة			
إدارة التغيير			
الفصل بين مرافق التطوير والاختبار والتشغيل			
مراقبة ومراجعة خدمات الطرف الثالث			
الضوابط الخاصة بالبرامج الضارة			
الحفظ الاحتياطي للمعلومات			
سياسات وإجراءات تبادل المعلومات			
التراسل الإلكتروني			
اقتناء نظم المعلومات وتطويرها وصيانتها			
مواصفات وتحليل المتطلبات الأمنية			
التحكم بالبرمجيات الخاصة بالتشغيل			

السياسة	أهمية السياسة	رقم إصدار السياسة	مالك السياسة
سياسة إدارة الحوادث الأمنية			
الإبلاغ عن نقاط الضعف الأمنية والحوادث			
سياسة إدارة استمرارية العمل			
تطوير وتطبيق خطط استمرارية العمل بما في ذلك أمن المعلومات			
سياسة الالتزام			
تحديد التشريعات ذات العلاقة			
حقوق الملكية الفكرية			
حماية البيانات وخصوصية المعلومات الشخصية			
الالتزام بالسياسات والمعايير الأمنية			
ضوابط تدقيق الأنظمة المعلوماتية			