وزارة الاتصالات وتقنية المعلومات

السياسات العامة لأمن المعلومات

في الجهات الحكومية

V - 0.1

السياسات العامة لأمن المعلومات في الجهات الحكومية

الصادرة بقرار مجلس الوزراء رقم (59) لسنة 2020م

V - 0.1

2021

جدول المحتويات

الباب الأول: أحكام تمهيدية 5
مقدمة 6
تعاريف 7
الباب الثاني: مدخل لسياسات أمن المعلومات 9
المبادئ الأساسية لضمان أمن المعلومات 10
الأهداف 11
متطلبات إدارة وتنفيذ أمن المعلومات 12
- خطة إدارة وتنفيذ أمن المعلومات 12
- تحديد سياسات أمن المعلومات 12
- إدارة وتنفيذ أمن المعلومات 13
- متطلبات أمن المعلومات 13
مجال ونطاق تطبيق السياسات 14
الأدوار والمسئوليات والواجبات العامة 15
- الجهة الحكومية 15
- ضابط أمن المعلومات 17
- الجهات الخارجية 18
الباب الثالث: السياسات العامة لأمن المعلومات 19
1. سياسة الأمن المادي والبيئي 20
2. سياسة أمن التوظيف والموظفين 21
3. سياسة التعاقد والتعامل مع أطراف خارجية 22
4. سياسة الإمتثال 24
5. سياسة تصنيف وحساسية المعلومات 24
6. سياسة إدارة الأصول المعلوماتية 27
7. سياسة ضبط التغيير 28
8. سياسة إدارة التحكم بالنفاذ والدخول 29
9. سياسة خصوصية البيانات 31
10. سياسة تطوير وصيانة الأنظمة والتطبيقات 31

11. سياسة أمن الشبكة 33
12. سياسة أمن الإنترنت 34
13. سياسة أمن البريد الإلكتروني 35
14. سياسة التشفير 37
15. سياسة الحماية من الشفرات الخبيثة وفيروسات الأجهزة 38
16. سياسة النسخ الاحتياطية والاستعادة في حالة الكوارث 39
17. سياسة إدارة الحوادث الأمنية وخطة الاستجابة للطوارئ 40
18. سياسة تقييم وتدقيق المخاطر الأمنية 40
19. سياسة مراقبة الأحداث الأمنية 41

أحكام تمهيدية

مقدمة

أصبحت تكنولوجيا المعلومات والاتصالات أحد العوامل المؤثرة في نهضة البلدان وازدهارها واستقرارها إلى درجة أنه لا يمكن لأي جهة أو مؤسسة أو شركة حكومية أو خاصة أن تعمل في استغناء عن تكنولوجيا المعلومات والاتصالات، ومع سرعة تعاظم ونمو تكنولوجيا المعلومات والاتّصالات، وتزايد أثرها في تعزيز التّنمية البشرّية والاقتصادّية والاجتماعّية والثّقافّية ودورها في تقديم خدمات الجهات الحكومية والخاصة، ازدادت المخاطر على المنظومات المعلوماتيّة وتنوّعت واختلفت أساليبها ودوافعها، وتجاوز سقفها سرقة المعلومات أو الاختراق أوالتّجسس إلى تعطيل الخدمات العامّة وايقاع خسائر ماديّة ومعنويّة كبيرة بالأفراد والمؤسسات والجهات الحكومية، وعُرف ما يسمّى بالحروب السيبرانية أو الهجمات الإلكترونية والتي قد تستهدف قطاع حيوي بأكمله على مستوى الدولة.

وعليه ولأهمية وضرورة تأمين بنية تحتيّة آمنة وموثوقة سواءً لإنجاز الأعمال والمهام أو لتقديم الخدمات الإلكترونيّة، ولزوم توفير البيئة الملائمة لتقليل خطر اختراق المنظومات المعلوماتيّة الحكوميّة، وكشف محاولات الاختراق واتّخاذ الإجراءات اللّازمة بأسرع وقت ممكن في حال حدوثها، فقد أعدت وزارة الاتصالات وتقنية المعلومات في الجمهورية اليمنية وثيقة سياسات أمن المعلومات العامة للجهات الحكومية.

حيث توفر هذه السياسات مجموعة متكاملة من المتطلبات الأساسية وإجراءات الحماية التي يجب توافرها على مستوى جميع الجهات الحكومية من وزارات وهيئات ومؤسسات وشركات وغيرها تابعة لحكومة الجمهورية اليمنية لضمان بيئة تشغيل وعمل آمنة للأصول المعلوماتية والمعلومات وبما يضمن ديمومة قيامها بمهامها وأعمالها بسلامة واطمئنان، حيث تعد معلومات هذه الجهات والمعلومات الوطنية وأنظمة دعم تكنولوجيا المعلومات وبيانات المواطنين ونحوها من الأصول المهمة للجهات الحكومة والتي يجب الحفاظ عليها. كما تعنى وزارة الاتصالات وتقنية المعلومات بتقديم الملحقات اللازمة من أدلة إرشادية ولوائح تفصيلية ومواد تأهيل وتدريب وتوعية لكافة الجهات الحكومية في مجالات أمن المعلومات.

تعاريف

(الجهة) الجهة الحكومية: جميع الوزارات والهيئات والمؤسسات والشركات وغيرها التابعة لحكومة الجمهورية اليمنية.

الوزارة: وزارة الاتصالات وتقنية المعلومات.

الجهات الخارجية: الأشخاص والشركات والمؤسسات والمجموعات وغيرها حكومية أو خاصة أو مختلطة الّتي تتعاقد معها الجهة الحكوميّة لتأدية خدمة أو مشروع أو عمل ما.

الموظفون: الأشخاص الذين يعملون في الجهات الحكومية بغض النظر عن الفترة والوظيفة.

المعلومات: مجموعة من البيانات طُبقت عليها عمليّات تغيير ومُعالجة حتى تحمل معنى وأهمية، ويكون ارتباطها وثيقاً بسياقٍ ما، ويمكن استخدامها في عدة مجالات نظراً لتعددية المعاني التي تحملها، ويعتبر هذا المصطلح له علاقة وثيقة بكلٍّ من المعرفة والتعليمات والتواصل والمعاني.

أمن المعلومات: الوسائل والتّدابير الخاصة المطبقة والمستمرة بشكل دائم بالحفاظ على سرّية، وتوافرية، وسلامة المعلومات، وحمايتها من الأنشطة غير المشروعة وبما يضمن الحماية اللازمة للمعلومات ومنع الوصول إليها من غير ذوي الصلاحية، ويشمل هذا المصطلح الأدوات والطرق والإجراءات اللازمة الواجب توفرّها لتحقيق الحماية من المخاطر التي قد تواجهها من الداخل أو الخارج.

الأنظمة المعلوماتية: مجموعة من الأجهزة والبرمجيات الحاسوبية والمعدات الملحقة بها.

الموارد المعلوماتية: أية معلومات أو ملفات (الكترونية أو غير الكترونية) أو اجهزة أو وسائط تخزين أو تسهيلات أو أشخاص لهم علاقة بعملية تبادل المعلومات ومعالجتها.

الأصول المعلوماتية: هي البيانات والمعلومات والبنية التحتية المحيطة بها من تجهيزات أو برمجيات أو خدمات أو مستخدمين أو مرافق ...الخ.

أصالة المعلومات: خاصّية كون الشيء حقيقياً ويمكن التّحقق منه والثّقة به، وضمان صحة الإرسال، أو الرّسالة أو المنشئ داخل المنظومة المعلوماتّية.

سـرية المعلومات: ضمان عدم الكشف عن المعلومات لأشخاص أو عمليات أو أجهزة غير مصرح لها بذلك.

سلامة المعلومات: الحماية من التعديـل أو الحذف غير المرخص للمعلومات أو التلف بأي شكل ولأي سبب وضمان أصالة المعلومات.

الـتـشـفـيـر: تحويـل البيانات (يدعى نص عادي) إلى شـيفرات (يدعى نص مشـفر) بشـكل يحافظ على المعنى الأصلي لهذه البيانات بهدف منع التعرف عليها أو استخدامها من قبل الغير مخول/ مصرح لهم بذلك.

الـمـخـاطـر: الخطر هو احتمال وقوع حدث سيء من شأنه المساس بأمن المعلومات والآثار المترتّبة على ذلك.

الـتّـهـديـدات: أي شـيء يمكن أن يسـبب ضـرراً على المعلومات كفعـل أو ظرف أو حدث وذلك من خلال تدميرها أو كشفها أو تعديلها أو إيقاف خدماتها ونحو ذلك.

نـقـاط الـضـعـف: خلل يمكن أن يستخدم للإضرار بالأصول المعلوماتية ويمكن أن يتواجد في إجراءات أو تصميم أو تنفيذ أو في الضوابط الّداخلّية لحماية الّنظام تحدث بشـكل عرضي أو أن يتم اسـتغلالها بشكل مقصود وينتج عنها خرق أمني أو انتهاك لسياسات الأمن.

الّـنـفـاذ: القدرة على الاستفادة من أي مورد من موارد تقنية المعلومات.

الـبـرامـج الخبيثة: برامـج توهم بأنهـا تؤدي عمل مفيـد أو مرغوب ولكنهـا في الواقع تحصل على دخول غير مصرح به إلى الأنظمة المعلوماتية لتنفيذ عملية غير مصرح بها أو تسبب في تلف الأنظمة المعلوماتية او المعلومات.

إدارة المخـاطـر: هي عمليّة مسـتمرة ومتكررة لتحديـد نقاط الضعف والتهديدات ذات الصلة بالموارد المعلوماتية ومراقبتها والحّد من آثارها. وتتضّمن تقييم المخاطـر، ومقارنة المزايـا والعيوب، ووضع وتنفيـذ واختبار الإجراءات الوقائّيـة وتقييم مسـتوى الحماية مـع الأخذ بعين الاعتبـار الفعالّية والكفاءة والأثر.

مدخل لسياسات أمن المعلومات

المبادئ الأساسية لضمان أمن المعلومات

تتمثل المبادئ الأساسية لضمان أمن المعلومات بشكل معياري في توفر التالي:

- الموثوقية أو السرية (Confidentiality):

حماية المعلومات الحساسة والسرية التابعة للجهات الحكومية من الكشف، وضمان عدم وصولها إلى أفراد أو أنظمة غير مصرح لهم، ويقتصر الوصول إلى هذه المعلومات على الأشخاص ذوي السلطة المناسبة والمصرح لها من قبل الجهة.

- التكاملية والسلامة (Integrity):

يجب أن تكون معلومات الجهات الحكومية كاملة ودقيقة ويجب أن تعمل جميع الأنظمة والأصول والشبكات بشكل صحيح وفقاً للمواصفات. ويتم الحفاظ على البيانات من التغيير أو التعديل من الأشخاص غير المخولين بالوصول إليها، وحماية دقة واكتمال المعلومات.

- توافر البيانات (Availability):

يجب توفير المعلومات وتسليمها إلى الشخص المناسب، في الوقت المناسب وعند الحاجة، والتأكد من أن المعلومات والخدمات الحيوية يمكن الوصول إليها للمستخدمين المصرح لهم عند الطلب.

- المسائلة وعدم الإنكار (Non-Repudiation):

عدم إنكار التصرف المرتبط بالمعلومات ممن قام به، ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما مرتبط بمعلومات الجهة الحكومية أو أصولها المعلوماتية، وضمان عدم إنكار بانه الذي قام بمثل هذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين.

الأهـــداف

تهـدف هذه الوثيقة لوضع أســس عامة لسياســات أمــن المعلومات الواجــب توافرها وإتباعها والعمل بها في جميع الجهات الحكومية التابعة للجمهورية اليمنية من أجل ضمان الحفاظ على أمن وســرية المعلومات والأصــول المعلوماتية التي تمتلكها أو تحتفظ بها هذه الجهات وبالشكل الذي يشمل كافة الموظفين ويتلاءم مع درجاتهم واختصاصاتهم ومهامهــم المختلفة في الإدارات والأقســام وبما يعزز أداء الجهــة الحكومية لأعمالها واستمرارها بتقديم خدماتها، وذلك من خلال:

أ. التأكــد مــن أن جميــع الموظفيــن على علــم ودراية بمهامهم وأدوارهم ومسؤولياتهم والامتثال الكامل للتشريعات ذات الصلة بأمن المعلومات.

ب. تحديد ووضع المتطلبات الأساسية لأمن المعلومات والإجــراءات اللازمة لحماية الأصول المعلوماتية تحت سيطرة وتحكم الجهة الحكومية.

ج. وصف مبادئ أمن المعلومات وشــرح كيفية تنفيذها في الجهات الحكومية وتوفير مرجعية لكافة النواحي المتعلقة بأمن المعلومات.

د. رفع مســتوى الوعي بأهمية وضرورة أمن المعلومات داخــل الجهات الحكومية واعتمادها كجزء لا يتجزأ من الأعمال والمهام الدائمة داخل تلك الجهة.

هـ. توفير بيئة آمنة لتقديم وتطوير الخدمات الإلكترونية.

وســتقوم وزارة الاتصــالات وتقنية المعلومــات بتوفير مجموعة مــن اللوائح التنظيمية التفصيلية والأدلة الإرشــادية والأعمال التوعوية للمســاعدة على تنفيذ هذه السياسات ومواكبة التقدم في هذا المجال.

متطلبات إدارة وتنفيذ أمن المعلومات

يجب وضع خطة شاملة وواضحة لحماية أصول المعلومات التابعة لكل جهة حكومية في الجمهورية اليمنية وبطريقة تتناسب مع قيمة تلك المعلومات وحجم الضرر المتوقع حال فقدانها أو إساءة الاستخدام أو السرقة أو التعديل بطرق غير قانونية، وبما يضمن استخدامها وتخزينها ونقلها وإدارتها بطريقة فعالة، ويجب أن يراعى في الخطة الاعتبارات التالية:

- **خطة إدارة وتنفيذ أمن المعلومات**

خطة إدارة وتنفيذ أمن المعلومات في الجهات الحكومية يجب أن تكون موثقة وتتضمن الإجراءات والتعليمات والسياسات الداخلية الواجب تنفيذها من قبل العاملين والمتعاقدين / المتعهدين لديها، ويجب أن تحظى هذه الخطة بدعم من قيادات الجهة وتتوافق مع سياسات ومعايير أمن المعلومات.

- **تحديد سياسات أمن المعلومات**

يجب تحديد سياسات أمن المعلومات في خطة أمن المعلومات للجهة وتعريفها وذلك وفق متطلبات أمن المعلومات، على أن يتم المصادقة عليها من قبل قيادات الجهة ونشرها لجميع المعنيين بتنفيذها، ويجب أن تتضمن كل سياسات البنود التالية:

- تعريف السياسات والغرض منها وأهدافها.
- تحديد المسئوليات والأدوار على كل شخص أو جهة تابعة لتنفيذ هذه السياسات والرقابة على الالتزام بها.
- إجراءات واضحة لحالات عدم الامتثال للسياسة.

- **إدارة وتنفيذ أمن المعلومات**

يجب أن تقــوم الجهة بوضع إطار عمل لإطلاق الخطة والتحكم بآليات التنفيذ، من خلال فريق متخصص وبصلاحيات محددة وفترة زمنية محددة وتطويرها بشــكل مســتمر بما يشمل:

- تحديــد فريق العمل المســئول عن تنفيذ السياســات أو مجموعة السياســات وإعداد تقارير عن مدى الالتزام مع الفترة الزمنية للتنفيذ.
- تحديد الجهات الداخلية سواءً كانت إدارات عامة أو إدارات أو أقسام ونحوها أو الجهات الخارجية والملزمين بتنفيذ السياسة.
- وضــع آلية واضحة لإبلاغ المعنيين في الجهة في حال حدوث أي طارئ يتعلق بأمــن المعلومات، كفقدان للمعلومــات أو الخدمــات أو أي اختراقات أو نحو ذلك.
- وضــع الأدوار والمســئوليات والمهام بيــن التفرعات الإداريــة الداخلية للجهة بحيث لا تتعارض واجباتها وبما يضمن تحديد الجهة المســئولة عن عدم تنفيذ السياسات أو عند حدوث أي طارئ.

- **متطلبات أمن المعلومات**

إن تحديــد متطلبــات أمــن المعلومات في الجهــات الحكومية يختلــف باختلاف أهمية المعلومــات والبيانات والخدمات الإلكترونية المعتمــدة، ويجري تحديد هذه المتطلبات في الجهات الحكومية اعتماداً على ثلاثة مصادر أساسية:

1. تقييم المخاطر التي قد تهدد الجهة الحكومية، مع الأخذ بعين الاعتبار أهدافها والخدمات التي تقدمها ومدى الضرر المتوقع من هذه المخاطر.
2. القوانين والأنظمة والتعليمات وغيرهــا مما يتعلق بعمل الجهة الحكومية، أو المتعلقة بالخدمات الإلكترونية التي تقدمها الجهة.
3. متطلبات نجاح الجهة الحكومية في تحقيق أهدافها وتنفيذ مهامها.

مجال ونطاق تطبيق السياسات

- تسري هذه السياسات على جميع الجهات الحكومية في الجمهورية اليمنية (داخل البلاد وخارجها) وعلى مسؤوليها وقياداتها وموظفيها والعاملين فيها بشكل دائم أو مؤقت، وعلى المتعاقدين معها، وعلى أي جهة أو فرع أو شركة أو وحدة يتم فيها تواجد بيانات ومعلومات خاصة بهذه الجهات الحكومية.
- نطاق سياسات أمن المعلومات يطبق على كافة الأصول المعلوماتية وعلى البيانات والمعلومات المخزنة التي تمتلكها الجهة سواء التي يتم معالجتها واستخدامها داخل الجهات الحكومية أو خارجها.
- تقوم الجهات الحكومية بدعم وتخصيص فريق أمن معلومات مختص ضمن الجهة وبحسب طبيعة وحجم الجهة (شخص أو أكثر، أو وحدة مختصة) للقيام بالمهام اللازمة لضمان أمن المعلومات فيها.
- تعتبر هذه الوثيقة وتعديلاتها أحد المكونات الأساسية للاستراتيجية الوطنية لأمن المعلومات التي يجب وضعها وإقرارها مستقبلاً على المستوى الوطني الشامل.

الأدوار والمسئوليات والواجبات العامة

- **الجهة الحكومية:**

- تطبيق سياسات أمن وحماية المعلومات التي توفر الحد الأدنى للممارسات المتعلقة بأمن وحماية المعلومات في الجهة.
- تعميم السياسات على جميع الموظفين والعاملين في هذه الجهة الحكومية كلاً فيما يخصه وجعلها في متناول المعنيين بشكل مستمر، كون أمن المعلومات هو مسؤولية كل موظف في الجهة الحكومة.
- وضع التعليمات والإجراءات المناسبة لتطبيق السياسات.
- تضمن الجهة أن الحماية الأمنية تكون متلائمة ومتوافقة مع تغيرات البيئة والتكنولوجيا.
- توفر الجهة بند مالي في الموازنة لتغطية احتياجات ومصادر الحماية الأمنية الضرورية.
- حفظ وصيانة البرمجيات وعقود الصيانة والضمانات سارية المفعول بعناية وبشكل سليم.
- تطبق الجهة سياسات فعالة للفصل بين المهام والواجبات لتجنب تنفيذ كل المهام الأمنية بشكل فردي.
- تعيين ضابط أمن معلومات وتوفير الدعم اللازم له من أجل توفير المهارات والتدريب الكافي للموظفين والعاملين في الجهة والإشراف على فهم وتطبيق السياسات والتعليمات الخاصة بأمن وحماية المعلومات فيها.
- ضمان سرية وسلامة وتوفر المعلومات وغيرها وبما يتعلق بالجوانب الأمنية لنظم المعلومات التابعة لها وبما يشمل أنظمة المعلومات المدارة من جهات خارجية.
- منح الموظفين أقل الصلاحيات اللازمة على موارد نظم المعلومات بما يضمن سير العمل، بناءً على تصنيف الإدارة التي ينتمي اليها الموظفون وطبيعة

عملها ومستوى المسؤولية لكل موظف.

- التدقيق الدوري على مدى الالتزام بهذه السياسات داخل الجهة بهدف تحديد ومعالجة أي قصور أو ثغرات لوحظت فيها.
- وضع وتوضيح الإجراءات المناسبة لمحاسبة الموظفين والعاملين في الجهة عن أي خلل أو قصور من شأنه الإخلال بأمن وحماية أي من الموارد المعلوماتية في الجهة طبقاً للأنظمة المعمول بها.
- يجب على الجهة إبلاغ الموظفين (الدائمين -المتعاقدين – المؤقتين) أنه في حال انتهاك أي من بنود سياسات أمن المعلومات قد يتعرضون للمحاسبة وإنهاء خدمتهم في الجهة وذلك تبعا لدرجة خطورة الانتهاك.
- يجب اختيار الموظفين المعنيين بمهام وأعمال أنظمة المعلومات/قواعد البيانات بعناية وفق سياسات أمن التوظيف والموظفين.
- يجب على الجهة إعلام الموظفين بمسؤولياتهم فيما يخص أمن المعلومات من بداية تعيينهم وخلال فترة عملهم في الجهة بشكل دوري.
- على كافة مدراء /مسئولي الانظمة والتجهيزات وقواعد البيانات تطبيق التعليمات والإجراءات على جميع الموارد المعلوماتية الموجودة في الجهة الحكومية بالتوافق مع سياسات أمن وحماية المعلومات.
- توفير الدعم الفني الكافي الذي يضمن تطبيق هذه السياسات من قبل المعنيين في الجهة.
- على جميع الموظفين الالتزام بقراءة السياسات وفهمها والرجوع إليها عند الحاجة، والتوقيع بالتقيد على ما جاء فيها.
- على كافة قيادات ومدراء وموظفي الجهات بذل أقصى الجهود الممكنة لتنفيذ السياسات والتعليمات المتعلقة بها في الجهة.
- على كافة الموظفين التعاون مع المختصين في مجال تكنولوجيا وأمن وحماية المعلومات والرجوع إليهم عند الحاجة والتعاون مع مدققي أمن المعلومات للقيام بمهامهم بيسر وسهولة.

- تتحمل الجهة المسؤولية الكاملة عن تحديث وتطوير سياسات أمن المعلومات لديها وبما يتناسب مع طبيعة نشاطها.
- تكون الجهة مسؤولة عن أي تقصير أو تهاون في تنفيذ هذه السياسات وما يرتبط بها وعن جميع نتائج وآثار ذلك.
- على الجهة تضمين لوائحها الداخلية والعقود والاتفاقيات بالعقوبات والجزاءات اللازمة بخصوص مخالفة سياسات امن المعلومات وبما يتناسب مع القوانين النافذة وحجم وأثر المخالفة.

- ضابط أمن المعلومات

- التأكد من تطبيق سياسات أمن وحماية المعلومات والتعليمات والإجراءات المتعلقة بها في الجهة بشكل دوري والرفع بتقارير عن درجة ومستوى تطبيق السياسات.
- الرفع بالمقترحات والتوصيات اللازمة ومنها الترقيات /أو الترتيبات الواجب توفيرها سواءً كانت حلول مادية (تجهيزات) او برمجية (انظمة) أو إدارية أو نحوها.
- التعاون مع جميع العاملين والمتعاملين مع الجهة من أجل تطبيق هذه السياسات والتعليمات والإجراءات بأعلى مستويات الدقة الممكنة.
- القيام بدور التوعية المناسب لتدريب ورفع مستوى مهارات العاملين في الجهة في مجال أمن وحماية المعلومات من خلال تطبيق برامج التوعية الخاصة بأمن وحماية المعلومات، والمشاركة في ورش العمل والندوات ذات العلاقة، من أجل العمل والالتزام بالممارسات الايجابية في مجال أمن وحماية المعلومات والالتزام بسياسات أمن وحماية المعلومات، وبيان الآثار السلبية المترتبة على عدم تنفيذها والالتزام بها أو ترك العمل بها.
- التدقيق على مدى التزام جميع العاملين والمتعاملين مع الجهة بهذه السياسات والتعليمات المتعلقة بها.

- الجهات الخارجية

- يجب أن يتقيد مزودو الخدمات الخارجية أو البرامج التجارية المتعاملين مع الجهة بسياســات أمن المعلومات في الجهة وأي من متطلبات أمن المعلومات التي تصدرها الحكومة.
- يجب على الجهة الحكومية مراقبــة ومراجعة معايير أمن المعلومات المقدمة من مزودي الخدمات والبرامج التجارية لكي تتأكد من إدارتها بشكل صحيح.
- يجب أن يخضع المستشــارون الخارجيون والمتعاقدون والموظفون المنتدبون والمؤقتــون الذين يعملون مع الجهة الحكومية لنفــس الضوابط والمتطلبات والمسؤوليات الخاصة بأمن المعلومات.

السياسات العامة لأمن المعلومات

1

سياسة الأمن المادي والبيئي

يجب تأمين المعدات والتحكم في الوصول المادي والبيئة الفيزيائية المحيطة بالأصول الخاصة لكل جهة حكومية وبما يضمن الاستخدام الآمن والأمثل لهذه الأصول، وبما يشمل:

- حماية أماكن المنظومات المعلوماتية التابعة للجهة والتي يتم فيها معالجة وحفظ المعلومات من الاختراق والكوارث الطبيعية أو الصناعية أو الدخول غير المصرح به.
- حماية كافة التجهيزات وجميع نظم المعلومات ووضعها في بيئة آمنة والسماح بالنفاذ/الوصول للموظفين المخولين فقط لمنع الوصول غير المسموح به.
- حماية وسائط حفظ البيانات ووسائط النسخ الاحتياطي التي تحتوي على معلومات أساسية أو حساسة على مسافة آمنة من الموقع الرئيسي لتفادي الأضرار التي قد تنجم عن كارثة في الموقع الرئيسي.
- اختيار مكان آمن للمعدات والتجهيزات التقنية بحيث تكون مؤمنة جيداً من ناحية الأمن المادي ومحمية من الكوارث والتهديدات الأمنية سواء طبيعية أو غيرها، وذلك لتقليل حجم الخسائر ومدة خروجها عن الخدمة وأن تكون في مستوى أمني مناسب.
- في حال وجود أي معدات تابعة للجهة وتحتوي على معلومات خاصة بها في عهدة أي من الموظفين فيجب تطبيق المعايير الأمنية للحفاظ على هذه المعدات وسلامة المعلومات المتواجدة بها.
- يجب أن تحدد أسماء الموظفين وتوصيفهم الوظيفي المخولين بالوصول إلى مواقع البيانات والمعدات، على أن يتم مراجعة هذه الأسماء بشكل دوري.
- يجب توفير تجهيزات وأنظمة أمنية خاصة بإدارة الدخول والإغلاق لمواقع البيانات وغرف المعدات وما شابه، مثل انظمة البصمة والبطائق الممغنطة وأن تكون ضمن إجراءات أمنية محددة وصارمة.
- تركيب أنظمة تسجيل ومراقبة لمواقع البيانات وغرف المعدات وأن تكون على مدار الساعة.

- يجب تفعيل خاصية الحماية التلقائية في السيرفرات واجهزة الحاسوب والحواسيب المحمولة وغيرها بحيث يتم إغلاق هذه الأجهزة تلقائياً في حال عدم الاستخدام لفترة قصيرة ومحددة.
- يجب أن توضع شاشات العرض الخاصة بطريقة لا تسمح لغير المصرح لهم برؤيتها.

2

سياسة أمن التوظيف والموظفين

- علـى الجهة تحديد ووضع قائمة بالمهام والمسـؤوليات المناطة بشـكل يحقق مبدأ الفصل بين المهام وفق الحاجة والاختصاص.
- إلـزام جميع الموظفين والمتعاقدين بتطبيق السياسـات والتعليمات الواردة في خطة أمن المعلومات.
- يجـب إعطاء جميـع الموظفين الذين تـم تعيينهم الحد الأدنى مـن الصلاحيات والامتيازات اللازمة لإتمام أعمالهم حسـب الوصف الوظيفي لكل منهم، اعتماداً على مبدأ المعرفة على قدر الحاجة.
- التأكد من حصول الموظفين على المعلومات اللازمة والوعي والتدريب بما يضمن توفر المهارات والكفاءات الضرورية لحماية المعلومات الحكومية على نحو يتوافق مع تصنيفها من حيث الأهمية والخطورة.
- توضيح إجراءات وتعليمات الخصوصية والسلامة والأمان للموظفين.
- توضيح قواعد التقارير والتدقيق والمتابعة وقواعد التعامل مع المعلومات.
- التأكـد من مدى تأثير الإجراءات الإدارية الخاصـة بالعاملين (نقل، تقاعد، فصل...) علـى إدارة الأصـول المعلوماتية واسـتمرارية العمل، ووضـع الضوابط المنظمة لمثل هذه الحالات بما يضمن عدم تأثيرها على سـير وسلامة عمل أنظمة وامن المعلومات لدى تلك الجهة.
- فـرض توقيع تعهـد بعدم الإفصـاح عن المعلومـات من قبـل الموظفين عند البدء بممارسـة أعمالهم، والتي يتم مراجعتها وإقرارها بشـكل قانوني بين الجهة والموظفين.
- يجب تغيير/ تعديل / تجميد جميع الصلاحيات المسـندة للموظفين المنتقلين من إدارة/قسـم إلى أخرى داخل الجهة، بحسب المهام الجديدة الموكلة إليهم وفق الإجراءات المتبعة.
- في حال إنهاء خدمات أحد الموظفين التابعين للجهة فإنه يجب وضع آلية تتضمن تغيير/إيقاف سجل الدخول الإلكتروني وإلغاء أية صلاحيات للموظف الذي أنهيت خدماتـه، والتأكد من تسـليم جميع المعلومات الخاصة بالعمل، وتسـليم كل ما

بحوزتــه من مفاتيح ومعــدات وبطاقات مرور وغيرها، وضمــان عدم حيازته على معلومات سرية سواء كانت إلكترونية أو غير إلكترونية وتعهده بذلك، ويجب حفظ نســخة من صندوق البريد الإلكتروني الخاص به وسجلات الاحداث لفترة مناسبة لاستخدامها في حال استدعت الحاجة.

- توضيــح بأن على جميع الموظفين حمايــة المعلومات والأجهزة وأي معدات يتم استخدامها والمحافظة عليها من التلف أو التخريب أو الضياع.
- وضع عقوبات إدارية رادعة للموظفين أو المتعاقدين المخالفين لسياسات ومعايير أمن المعلومات.

3

سياسة التعاقد والتعامل مع أطراف خارجية

- يجـب ان يتم تحديد المخاطر المترتبة على التعاقـد أو التعامل مع أطراف خارجية وتحديد التدابير المناسبة والمتخذة لمعالجة هذه المخاطر.
- تكون الاسـتعانة بمزود خارجي وفق اتفاقية (عقد) موقعة مع الجهة على درجة عاليـة من الكفاءة والأمـان للقيام بمهمة التعاقد الخارجي بشـكل آمن وصحيح وفعال.
- يجب ألا تكون الاسـتعانة بمـزود خارجي فـي الخدمات المعلوماتيـة الجوهرية والحرجـة إلا في الحـالات الضرورية وبعد موافقة قيـادة الجهة. وتوقيع اتفاقية سرية البيانات وعدم الإفصاح/الإفشاء.
- يجب أن تتضمن سياسات أمن المعلومات ضمان حماية الأصول المعلوماتية التي يسـمح للجهات الخارجيـة الوصول إليها أو تعديلهـا أو تطويرها أو نقلها بموجب العقود/ الاتفاقيات المبرمة لهذه الغاية.
- إذا كان الغـرض الـذي سـيتم التعاقد الخارجي مـن أجله هو التدقيـق على أمن المعلومـات، فيجب موافقة قيادة الجهة ومراعاة اتفاقية سـرية البيانات وعدم الإفصاح في وثيقة العقد.
- يجب أن تتضمن العقود التي تتعلق بشكل مباشر أو غير مباشر بالأصول المعلوماتية على الاتي:
  - تعهد الجهة الخارجية بالالتزام بسياسات أمن المعلومات الخاصة بالمتعاقدين المعتمدة من الجهة الحكومية.
  - إلـزام الجهة الخارجية تقديم شـرح موثق لآليات العمـل والمراحل المتعلقة بإحداث تغييرات على الأصول المعلوماتية، مما يتيح للجهة الحكومية توثيق المراحـل التـي تمر بها هـذه الأصول ومعالجـة الصعوبات الطارئة بسـرعة وفعالية.
  - تحديد دور ومسئوليات الجهة الخارجية بوضوح.
  - تقديم كافة الوثائق المتعلقة بآليات التركيب والتنصيب والتشـغيل والصيانة والنسخ الاحتياطي والحماية ضمن مواد العقد.
  - اقتـراح أية منظومات خاصة بحماية وأمـن المعلومات لمخرجات العقد، مع

بيان السبب ومدى الحاجة إليها.

- تعهد بالالتزام والحفاظ على سرية البيانات وعدم الإفصاح عن أي معلومات تم الاطلاع عليها.
- يلتزم المتعاقد الخارجي بمبدأ نقل المعرفة للفريق المختص بالجهة الحكومية.
- توثيــق كافة مراحل العمل الــذي جرى التعاقد لأجله مــن قبل فريق الجهة الحكومية وتمكين فريق الجهة الخارجية للفريق المختص في الجهة الحكومية من كافة جوانب المشروع المتعاقد عليه وبما يضمن نجاح المشروع..

4

سياسة الامتثال

- يجـب الالتزام بالمتطلبات القانونية والسياسـات والإجـراءات اللازمة، بما يضمن الالتزام والامتثال للقوانين والأنظمة النافذة في الجمهورية اليمنية عند وضع أي خطة أو سياسات أو متطلبات أو عقود أو غيرها فيما يخص أمن المعلومات.
- يجب حماية الوثائق سـواءً كانـت ورقية أو إلكترونية والخاصـة بأمن المعلومات وكافـة الأصـول المعلوماتيـة والاحتفاظ بها بحسـب الحاجة وبمـا يتوافق مع القوانين والأنظمة النافذة.

5

سياسة تصنيف وحساسية المعلومات

- تتضمــن المعلومات المعنية في خطة أمــن المعلومات لأي جهة حكومية كافة المعلومات التي يتم حفظها أو تبادلها بشــتى الوســائل، سواءً كانت إلكترونية أو غيــر إلكترونية، مثل المعلومات المكتوبة، أو تلك التي يتم تبادلها مشــافهةً مثل الهاتف أو بشكل مرئي مثل الاجتماعات المرئية والمسموعة.

- علــى الجهة الحكومية وضع معايير شــاملة تتضمن تفاصيل مواردها المعلوماتية بهــدف تحديــد أهميتها وحساســيتها وآثارهــا القانونية، ووضع خطــة التصنيف المتبعة بالتوافق مع هذه السياسة.

- يجــب وضــع تصنيف لجميــع المعلومات المملوكــة للجهة الحكوميــة وتوضيح مدى حساســية وأهمية كل صنف، ووضع آلية تتم فيها إدارة المعلومات بشكل صحيح ابتداءً من مرحلة إنشــائها، مروراً بالاستخدام المرخص لها، وانتهاءً بالطريقة الصحيحة لإتلافها بحيث تتناسب هذه الالية مع مستوى التصنيف.

- الجهــة الحكومية مســئولة عــن تصنيف المعلومــات، ويتم تصنيفهــا إلى أربعة مستويات وهي:

أ) المستوى الأول: المعلومات العادية

- هي معلومات قليلة الحساسية، لا يؤثر الإفصاح عنها على خصوصية أو أمن الجهة الحكومية أو أي من المتعاملين معها مثل الموظفين والعملاء والشركاء، أو تؤدي إلى (الاضرار/ إيذاء) أي من المصالح السياسية أو الاقتصادية أو غيرها، وتكون عادة متاحة للنشر عبر وسائل الاتصال والإعلام.

- لا توجد صلاحيات أو تحديدات على هذا النوع من التصنيف.

ب) المستوى الثاني: المعلومات المحدودة

- هي معلومات حساســة معدة للاستخدام الرسمي، وإذا ما تم الإفصاح عنها فإنها يمكن أن تعرض خصوصية وأمن الجهة الحكومية أو أي من المتعاملين معها للخطر، وبالتالــي فإن الإفصاح غير المرخص عن المعلومات المحدودة يمكن أن يؤثر ســلباً على الثقة بالموظفين والمواطنين، مثل البريد الإلكتروني غير المشفر، والتعميمات والمذكرات الداخلية، والمعلومات التي يتم وســمها بطريقــة تعكس محدوديتها، مثل "لاستخدام الجهة فقط".

- يجب على الجهة وضع وإعلان التعليمات المناسبة للكشف عن هذه المعلومات قبل تقديمها لأي جهات خارجية.
- يتم تصنيف المعلومات الشخصية على أنها "محدودة" ما لم تحدد تعليمات الجهة الحكومية غير ذلك.

ج) المستوى الثالث: المعلومات السرية

- معلومات حساسة معدة للاستخدام الرسمي المحدود، وإذا تم الإفصاح عنها فإنها ستعرض أمن وخصوصية الجهة الحكومية والمتعاملين معها للخطر، أو تسبب لهم ضرراً سياسياً أو اقتصادياً أو نحو ذلك، مثل المعلومات التي من المتوقع أن تكون مفيدة لبلدان أجنبية أو جهات غير حكومية، والمعلومات المستثناة من الإفصاح عن المعلومات العادية والمحدودة.

- إن تصنيف المعلومات على أنها "سرية" أو "سرية للغاية" يجب ألا يتم بشكل عشوائي، وإنما يجب أن يكون حسب التعليمات والأنظمة والقوانين.

- إن مسئول المعلومات في الجهة الحكومية المخول الوحيد وله صلاحية إقرار هذا المستوى من التصنيف أو تغييره وتحديد كيفية الإفصاح عن هذه المعلومات وبموافقة قيادة الجهة.

د) المستوى الرابع: المعلومات السرية للغاية

- هي المعلومات التي تعتبر غاية في الحساسية والأهمية للجهة الحكومية، والتي تعرض أمنها وخصوصيتها والمتعاملين معها للخطر الشديد، أو تلك المعلومات المعدة للاستخدام من قبل جهات معنية، ويمكن أن يؤدي الإفصاح عنها بشكل غير مرخص إلى تهديد حياة الأشخاص، أو أضرار مادية أو معنوية للجهة أو المتعاملين معها، أو يسبب ضرراً جسيماً بالمصلحة القومية للبلد ويعرض أمن الدولة للخطر، بالإضافة إلى المعلومات التي يترتب الإفصاح عنها بشكل غير مرخص إلى مسائلات قانونية، مثل معلومات الحسابات الشخصية، والتحقيقات الجارية، ومعلومات تتعلق بأمن الدولة، والمعلومات ذات الأهمية الاستخباراتية أو العسكرية.

- إن مسئول المعلومات في الجهة الحكومية وحده له صلاحية إقرار هذا المستوى من التصنيف أو تغييره وتحديد كيفية الإفصاح عن هذه المعلومات وبموافقة قيادة الجهة.

- يجب أن تتوافق عملية حفظ المعلومات مع مستويات تصنيفها، فيجب حفظ جميع وسائط التخزين في مكان آمن حسب تصنيف المعلومات المخزنة فيها، فمثلاً: (حفظ المعلومـات العادية دون الحاجة إلى تطبيق إجراءات أمنية صارمة، في حين يجب حفظ المعلومات "السـرية" و"السـرية للغاية" بطريقة صحيحة محمية من أي تهديدات أو أخطار ومن الوصول إليها أو تداولها بشكل غير مرخص).

- يجـب تداول المعلومات في الجهة الحكوميـة بطريقة تضمن حمايتها من الوصول إليها أو الإفصاح عنها أو تغييرها بشـكل غير مرخص أو فقدانها، ولهذا، فإنها يجب أن تعالج وتحفظ حسـب مسـتويات تصنيفها في سبيل حماية سـريتها ومستوى حساسيتها وسلامتها وإتاحتها.

- على الجهة الحكوميـة وضع التعليمات الخاصة بإتلاف المعلومات عند الحاجة إلى ذلك بطريقة تتوافق مع مستوى تصنيفها وبطريقة تتوافق مع القوانين والتشريعات الحكومية والأحكام والأنظمة والتعليمات السارية.

- يجب تخزين جميع المعلومات "السـرية للغاية" في مكان معزول وآمن، ويجب عزل جميـع المعلومات ضمن تصنيفاتها بطريقة فيزيائية أو إلكترونية حسـب مسـتوى حساسيتها.

6

سياسة إدارة الأصول المعلوماتية

تشــمل البيانات والمعلومات والبنية التحتية والبيئة المحيطة من تجهيزات أو برمجيات أو خدمات أو مستخدمين أو مرافق أو غير ذلك مما يؤثر على أمن المعلومات، وفيما يلي الأصــول المعلوماتية التي يجــب تحديدها وإدارتها ضمن خطــة أمن المعلومات للجهة الحكومية:

- تحديد الأصول المعلوماتية والمكلفين بحماية كل أصل معلوماتي للجهة الحكومية وبما يضمن:

أ- تحديــد الأصول وجردها وتوثيــق ذلك ضمن جداول وتحديثهــا لتتضمن أهم المعلومات عنها.

ب- يجب تعريف وتوثيق قواعد الاستخدام الآمن للأصول المعلوماتية.

ج- ضمان إعادة الأصول إلى أماكنها الأصلية بعد استخدامها.

د- يجــب أن تتضمــن جداول الأصــول كل من الأفــراد أو الفــروع التابعة للجهة الحكومية كإدارات أو أقسام أو غيرها المسئولة عن الأصول المعلوماتية.

- تصنيف المعلومات بحســب أهميتها بالتوافق مع سياســات تصنيف وحساسية المعلومات ومما يسهل وضع آليات حمايتها.
- وضــع آليات وإجــراءات التخزين والنقل والإتلاف الآمن للأصول بحســب تصنيفها بالتوافق مع سياسات تصنيف وحساسية المعلومات.

7

سياسة ضبط التغيير

هــي إجراءات ضمان أمن وحماية الموارد المعلوماتية عند القيام بأي تغيير يؤثر عليها وتشــمل هذه السياســات أي تغيير قد يؤثر على إعداد أو تنصيب أو إضافة أو إزالة أو اتلاف أي من الموارد المعلوماتية المملوكة للجهة الحكومية مثل الملفات والبرمجيات والاجهزة والمعدات والشبكات ووسائط التخزين والوثائق كما تغطي كذلك الاشخاص المسئولين عن تقديم طلبات التغيير ومراجعتها والموافقة عليها.

- على الجهة الحكومية وضع التعليمات والإجراءات المناســبة لتنظيم عملية ضبط التغيير داخل الجهة بالتوافق مع هذه السياسة.
- علــى الجهة الحكومية متابعة عمليات ضبط التغيير والتدقيق على مدى تطبيقها بالتوافق مع هذه السياسة.
- لا يســمح بإجراء أي تغيير يتعلق بــأي من الموارد المعلوماتيــة المملوكة للجهة الحكومية بدون المرور على عملية ضبط التغيير المعمول بها في الجهة.
- تقسم طلبات التغيير إلى نوعين رئيسيين:
  - **تغييرات مجدولة:** وهي التي تحتاج إلى موافقة مسبقة.
  - **تغييرات طارئة:** وتتعلق عادة بالتغييرات غير المخطط لها، وهنا يرجع فيها إلى المسئول المباشر في الجهة الحكومية، ومن ثم يتم الإبلاغ عن التغييرات التي تم إجراؤها فيما بعد من أجل توثيقها حسب الأصول.
- علــى الجهــة الحكوميــة تحديد المســئولين عن تقديــم طلبات التغييــر والجهة المسئولة عن مراجعتها والموافقة عليها، وتوثيق طلبات التغيير، والإجراءات التي تبعت هذه الطلبات بعد القبول أو الرفض.

8

سياسة إدارة التحكم بالنفاذ والدخول

يجب أن تتضمن خطة أمن المعلومات لجهة حكومية ما يلي:

- تحديد حقوق الوصول إلى البيانات تحديداً واضحاً ويتم مراجعتها بشكل دوري.
- آليات واضحة للتحكم في النفاذ إلى أنظمة المعلومات وأصول المعلومات.
- التحقق من هوية المصرح لهم بالنفاذ إلى أنظمة المعلومات أو المرافق المستخدمة في معالجة المعلومات بما يتوافق مع متطلبات العمل.
- يجب مراقبة محاولات الدخول المتتابعة وغير الناجحة.
- المراجعة الدورية لملفات النفاذ إلى أنظمة المعلومات والمرافق وإلغاء الصلاحيات التي لم تعد لازمة لمتطلبات العمل، مع ضرورة إبلاغ المستخدمين بالتزاماتهم ومسؤولياتهم تجاه أمن المعلومات.
- التأكد من وضع وتنفيذ سياسات تتعلق بالنفاذ والدخول لمعلومات وخدمات الجهة الحكومية من خارج أماكن العمل الرسمية.
- التأكد من وضع وتنفيذ سياسات تتعلق بضوابط وأمن النفاذ من خلال الأجهزة الإلكترونية المحمولة (أجهزة اللابتوب المحمولة، هواتف ذكية، وغيرها).
- التأكد من وضع ضوابط فنية لمنع وتقييد ربط وتوصيل أي طرفيات أو أقراص صلبة قابلة للإزالة أو نحوها من وسائل تخزين محمولة ومتنقلة مالم تكن تلك الطرفيات أو الوسائل مسموحة من قبل إدارة / قسم أمن المعلومات بالجهة مع وجود القدرة للأنظمة على تسجل الأحداث مع هوية الطرفية ونوع العملية التي تمت منها واليها ووقتها.
- تحتفظ الجهة الحكومية بحقها بفحص جميع المعلومات المخزنة أو المرسلة عبر أنظمة المعلومات الحكومية مع مراعاة قوانين الخصوصية.
- يجب على الجهة الحكومية تحديد سياسات صارمة لكلمة المرور كتحديد الحد الأدنى لطول هذه الكلمة، طبيعة اختيار الكلمات، مدة استخدام الكلمة، بالإضافة إلى وجود إرشادات توضح كيفية اختيارها، وكذلك منع مشاركة كلمات المرور بين الموظفين أو إفشاء سريتها إلا عند الضرورة القصوى وبشكل موثق.
- عند تخزين كلمات المرور يجب حمايتها ويجب تشفير كلمات المرور عند انتقالها

خلال وسائل اتصال غير موثوقة.

- يجب تغيير جميع كلمات المرور الافتراضية لأي نظام من نظم المعلومات عند تشغيله واستخدامه بشكل رسمي ومن اللحظات الأولى.
- يجب تغير كلمات المرور بصورة دورية تفادياً لأي اختراق قد يحدث وحفاظاً على سرية المعلومات أو عند الاشتباه بأنها مخترقة أو عند الكشف عنها للفنيين من أجل الصيانة والدعم الفني.
- يمنع إضافة أي قسم أو شخص لأي نظام معلومات إلا بموافقة مسبقة من إدارة الجهة الحكومية وإدارة نظم/تقنية المعلومات فيها مع مراعاة المحافظة على مستوى مناسب من أمن المعلومات.
- يجب وضع آلية وإجراءات لتوثيق وتسجيل أنشطة نظم المعلومات التابع للجهة الحكومية وفقاً لاحتياجات العمل وتصنيف البيانات، وأن يتم الاحتفاظ بسجلات التوثيق وسجلات الاحداث والانشطة لفترة تتناسب مع استعمالها كأداة لمراجعة الأحداث.
- يجب وضع سياسات للتعامل مع السجلات تضمن الاحتفاظ بكافة سجلات الأحداث سليمة ومكتملة بكافة تصنيفاتها وعلى كافة المستويات ولكافة العمليات ولمدة زمنية مناسبة.

9

سياسة خصوصية البيانات

- يجب على الموظفين عدم الإفصاح لأي شخص عن أي معلومات تتعلق بالأفراد أو الأقسام أو الطرق المستخدمة لمعرفة نقاط الضعف لنظام معين أو أي أنظمة خاصة قد تعرضت للإتلاف بسبب الجرائم أو التجاوزات الحاسوبية.
- لا يجوز الكشف عن المعلومات المتعلقة بنظم المعلومات التي يمكن أن تمس أمن تلك النظم للمستخدمين أو أي طرف أخر إلا على أساس مبدأ الحاجة للمعرفة وبإذن مسبق من إدارة نظم المعلومات.
- يجب على الموظفين أن لا يفصحوا للأشخاص غير المصرح لهم عن طبيعة وموقع أنظمة المعلومات ولا عن أنظمة الرقابة المستخدمة أو وسائل النفاذ أو نوع وماهية التجهيزات والمكونات المستخدمة.
- يجب تشفير جميع المعلومات التي تصنف تصنيفاً حساساً (سري أو سري للغاية).
- يجب على الجهات الحكومية الالتزام بأمن أنظمة المعلومات كافة وعدم الاقتصار على تخزين ونقل ومعالجة وإتلاف المعلومات المصنفة.
- يجب مراعاة الخصوصية عند التعامل مع البيانات الشخصية للموظفين التابعين لتلك الجهة والبيانات الشخصية للمواطنين.

10

سياسة تطوير وصيانة الأنظمة والتطبيقات

- يجـب ان يكـون هناك ضمان لأي تصميـم أو تطوير أو تطبيـق أو اختبار لأنظمة المعلومات يتوافق مع متطلبات سياسات أمن المعلومات وخطة أمن المعلومات.
- يجـب على فريق تطويـر الأنظمة والتطبيقـات امتلاك الخطـط الأمنية وتنفيذ التدابير الأمنية والضوابط المناسبة للنظام قيد التطوير.
- يجب أن تصان الوثائق وقوائم الأنظمة والتطبيقات بشـكل سـليم على أن تقيد وفق معايير الحاجة للمعرفة.
- يجـب الحفاظ على سـلامة الأنظمة والتطبيقات في ظـل ضوابط أمنية ملائمة مثل آلية التحكم في الإصدار والفصل بين بيئات التطوير والاختبار والتشغيل.
- تعتبـر الدراسـات والوثائـق والمخططـات المتعلقـة بتحليـل وتصميـم أنظمة المعلومـات والبرمجيات المراد تطويرها أو صيانتهـا، والبرمجية المصدرية (الكود المصدري)، وكافة الملفات الخاصة بهذه الأنظمة والبرمجيات معلومات سـرية، يجب التعامل معها بالاسـتناد إلى سياسـات تصنيف وحساسية المعلومات وأن تكون ملكاً للجهة وليس لفريق التطوير أو غيره.
- لا يسـمح بإجراء أي تغييرات على أنظمة المعلومات والبرمجيات المستخدمة إلا إذا دعـت الحاجـة لذلك، علـى أن يتم توثيق ذلك عن طريـق عملية ضبط التغيير المتبعة في الجهة الحكومية بالتوافق مع سياسات ضبط التغيير.
- يسـمح بتطوير وشـراء البرمجيات المطورة خصيصاً للجهـة الحكومية عندما يتم ضمانها بدراسـة جدوى فعّالة ومدعّمة وبعد اختبـار أمنها وفحصها والتأكد من سلامتها.
- يجـب عند تطوير/اقتناء أي نظم معلومات جديـدة أن تختبر أولاً على بيئة خاصة بالتطوير والتجارب الى ان تحصل على الاعتماد والموافقة بعد نجاحها في تحقيق المؤشرات المطلوبة وخلوها من الثغرات ومن ثم ينتقل العمل على البيئة الفعلية.
- يجب اختبار أي تغييرات خاصة بأنظمة المعلومات أو البرمجيات المسـتخدمة في الجهة الحكومية بطريقة صحيحة وآمنة من قبل المختصين في الجهة قبل إقرارها ثم إطلاقها.

- لا يسمح باستخدام البيانات الحقيقية قيد الاستخدام عند اختبار الأنظمة قبل وضع ضوابط خاصة لضبط أمن هذه البيانات والمعلومات وسلامتها.
- يجب العمل بأنظمة المعلومات والبرمجيات المستخدمة في الجهة الحكومية بالتوازي مع الأنظمة والبرمجيات المطورة لحين التأكد من مطابقة الأخيرة لمتطلبات العمل ومتطلبات الأمن والحماية التي تم التطوير من أجلها.
- يجب التأكد من تطبيق التحديثات التي تعمل على تقليل درجة المخاطر للأخطاء الناجمة عن المعالجة الداخلية لكي لا تؤدي إلى التأثير سلبًا على سلامة أنظمة المعلومات والبرمجيات أو بياناتها.
- يجب تقييم المخاطر الأمنية للأنظمة من أجل تحديد فيما إذا كانت رسائل التحقق مطلوبة ولتحديد الطريقة الأنسب لتطبيقها.
- يجب استخدام أنظمة التشفير لحماية المعلومات في حال احتمال تعرضها للمخاطر، وعند عدم وجود ضوابط دخول قادرة على حمايتها بشكل كافٍ، وذلك بالتوافق مع سياسات التشفير.

11

سياسة أمن الشبكة

يجب أن تتضمن خطة أمن المعلومات للجهة الحكومية على ما يلي:

- وضع التعليمات المناسبة في التعامل مع عناصر الشبكة المعلوماتية المملوكة للجهة الحكومية، وشرائها أو إصلاحها أو نقلها أو إتلافها، بما يتفق مع سياسات أمن وحماية المعلومات عامة وسياسات تصنيف وحساسية المعلومات.
- وضع التعليمات والضوابط الخاصة بربط عناصر الشبكة بأي معدات أو بالشبكة المعلوماتية للجهة الحكومية بنوعيها السلكية واللاسلكية.
- يمنع الإفصاح عن عناوين وإعدادات أي من أنظمة الشبكة الداخلية التابعة للجهة الحكومية دون موافقة الجهة.
- يجب حماية جميع الشبكات الداخلية المتصلة مع شبكة حكومية أو شبكة عامة أخرى بشكل صحيح.
- وضع كلمات مرور سرية مناسبة للدخول إلى الشبكة تعطى للأشخاص المخولين بالتوافق مع سياسات النفاذ والدخول.
- توفير الحد الأدنى لسرعة الشبكة بحيث يتم ضمان قدرة هذه السرعة على تلبية متطلبات العمل الخاصة بالجهة سواءً كانت محلية أو واسعة النطاق.
- يمنع الموظفون الموصولة أجهزتهم بالشبكة الداخلية من الاتصال بأي شبكة خارجية بأي شكل من الأشكال إلا بموافقة الجهة المختصة.
- لا يجوز للموظفين ربط أي جهاز نظم معلومات غير مصرح به إلى الشبكة الحكومية دون الحصول على موافقة الجهة المختصة.
- يجب أن يتم مراجعة إعدادات وإدارة أنظمة الاتصال والمعلومات بشكل دوري.
- يجب ان يتم مراعاة امن المعلومات عند تصميم ومعمارية الشبكات بحيث توفر قدر مناسب من العزل والاستقلالية لضمان الحماية والسرية وبما يستلزمه احتياج العمل.
- يجب ان لا تؤثر عملية الاتصال مع أي شبكة أخرى على المعايير الأمنية لطرفي الاتصال.

- يمنع توصيل الموارد الحاسوبية المملوكة للموظفين بالشبكة الداخلية من دون إذن مسبق من إدارة / قسم أمن الشبكات أو الجهة المختصة، وتمنح الجهة الحكومية موافقة استخدام هذه الموارد الشخصية بمعايير مطابقة لسياسات أمن المعلومات.
- يجب تشفير المعلومات المصنفة تصنيفا خاصاً عند نقلها من خلال اتصال خارجي غير آمن.
- يجب تشفير المعلومات المصنفة تصنيفاً عالي السرية عند نقلها داخل الشبكة المحلية على أن تكون آلية التشفير متوافقة مع سياسات أمن المعلومات.
- في حال وجود شبكات لاسلكية، يجب على الجهة الحكومية التوثيق والمراقبة والتحكم في الشبكات اللاسلكية المتصلة بشبكة الحكومة الداخلية ووضع الضوابط والإجراءات المناسبة لتشغيلها وإدارتها.
- يجب إتباع الضوابط الأمنية السليمة من توثيق الدخول واستخدام التشفير لحماية البيانات المنقولة عبر الشبكات اللاسلكية المتصلة مع شبكة الحكومة الداخلية.
- يمنع الوصول الى تجهيزات أو شبكة أو أنظمة الجهة الحكومية الداخلية من خارج الجهة عبر شبكة الإنترنت مباشرة أو باستخدام تقنيات الشبكة الظاهرية الخاصة الا للضرورة القصوى وعبر إجراءات وآليات عمل وتصاريح موثقة وبشكل محدود وآمن وبعد موافقة من إدارة / قسم أمن المعلومات أو الجهة المختصة.

12

سياسة أمن الإنترنت

- يجب أن تكون جميع طرق الوصول إلى الإنترنت إما عن طريق مركزية لبوابات الإنترنت أو من خلال بوابة الإنترنت الخاصة بالجهة بما يتماشى مع المعايير الأمنية.
- يجب على الجهات الحكومية أن تنظر في الفائدة من حجب بعض المواقع غير الخاصة بالعمل مثل مواقع التواصل الاجتماعي، مع الأخذ بعين الاعتبار أن عدم فلترة بعض المواقع لا يعني السماح للموظف بتصفح تلك المواقع.
- يجب أن يوضح كل قسم أو إدارة للمستخدمين لديه سياسته فيما يتعلق بالاستخدام المقبول للإنترنت.
- لا يجوز للموظفين تنصيب أي برامج تم تحميلها من شبكة الإنترنت ما لم يكن من مصدر موثوق بها وبعد موافقة إدارة /قسم/مختص أمن المعلومات بالجهة.
- يجب أن تحدد الجهة الحكومية سياستها بوضوح تجاه استخدام خدمات الإنترنت المجانية/التجارية لأداء الأعمال الحكومية سواءً الخدمات الممنوحة للأفراد أو المؤسسات مثل خدمات البريد الإلكتروني العامة مثل (gmail, mail,...etc) و خدمات وسائل التواصل الاجتماعي مثل (واتسآب, تيلجرام,...الخ) وخدمات التخزين السحابية للملفات مثل (google Drive, Dropbox) فيما يخص أعمال الجهة وإرسال واستقبال الوثائق ونحوها.
- يمنع على الجهة الحكومية تخزين وحفظ بيانات الجهة الحكومية أو معلوماتها أو أنظمتها على منصات الحوسبة السحابية خارج الوطن ويجب أن تكون مخزنة على منصات تلك الجهة داخلياً أو لدى مزود خدمات المعطيات الوطني.
- يجب أن تكون مواقع الإنترنت الخاصة بالجهات الحكومية مستضافة داخل البلد ويمنع استضافتها في الخارج.

13

سياسة أمن البريد الإلكتروني

- يجـب لأي جهة حكومية تتبنى العمـل بالبريد الإلكتروني امتـلاك بريد إلكتروني خـاص بها وضمن النطاق الوطني (ye.) كما يجب أن يكون نظام وقاعدة بيانات البريد الإلكتروني داخل البلد وليس مستضاف في الخارج.
- يجب على الجهة الحكومية توضيح سياستها للموظفين بشكل واضح فيما يتعلق بالاستخدام المقبول للبريد الإلكتروني.
- يجب أن تحدد الجهة سياسـتها (المناسبة لطبيعة عملها) تجاه استخدام خدمات البريد الإلكتروني العامة (المجانية أو التجارية) مثل (gmail, mail,...etc) ووسائل التواصل الاجتماعي مثل (واتساب, تيلجرام,...الخ) فيما يخص أعمال الجهة وإرسال وإستقبال الوثائق ونحوها.
- يجب على نظم المعلومات التابع للجهة الحكومية إنشاء عملية منهجية للتسجيل والاحتفاظ وحذف رسائل البريد الإلكترونية والسجلات المرفقة بها.
- يجب فحص الرسـائل الصـادرة والـواردة للبريد الإلكتروني من الفيروسـات وأي ملفات مشبوهة.
- يجـب حمايـة عناوين البريـد الالكتروني الداخليـة أو التي تحتوي علـى المواقع الحكومية من التعديل أو الوصول غير المصرح به.
- لا يجـوز التطفل على سـجلات البريـد الإلكتروني أو الدخول إليهـا إلا عن طريق صاحب البريد ومختص أمن المعلومات، باستثناء التدقيق في مثل الحالات التالية:
  - وجود أدلة على استخدام غير صحيح للسجل.
  - احتواء السجل على محتويات تتعارض مع سياسات هذه الوثيقة.
  - وجود حكم قضائي.
  - دواعي أمنية من الجهات المختصة.
- يجـب أن تكون كافة المعلومات التي يتم تبادلهـا عبر الإنترنت من خلال الأجهزة والتسـهيلات الخاصة بالجهة الحكومية هي ملك للجهة وليسـت للمستخدمين، لذا فإن للإدارة الحق في التدقيق ومراقبة الجهة المستقبلة ومحتوى المراسلات كلما دعت الحاجة، وذلك من أجل حماية مصالح الجهة الحكومية.

- يجب تشـفير رسائل البريد الإلكتروني بما يتوافق مع سياسات التشفير وسياسات تصنيف وحساسية المعلومات.
- لا يسمح باستخدام إعادة الإرسال بشكل آلي في الحالات التي تحمل فيها الرسالة معلومات مشفرة.
- يمنع فتح أو إعادة توجيه رسائل البريد الإلكتروني المرسلة من مصادر مشبوهة.
- يجـب وضع آلية واضحة للموظفين للإبلاغ عن أي حالة اشـتباه في اختراق للبريد الالكتروني الى إدارة / قسـم امن المعلومات للقيام بالإجراءات المناسبة وتأمين وحماية البريد الالكتروني في الوقت المناسب.

14

سياسة التشفير

- في حال تبادل المعلومات الحساسة عبر الشبكات أو البريد الإلكتروني، يجب أن تعتمد الجهة الحكومية على تقنيات التشفير وذلك لضمان سرية وسلامة ومصداقية هذه المعلومات وبالتوافق مع سياسات تصنيف وحساسية المعلومات.
- استخدام خوارزمية تشفير مثبتة ومعتمدة عالمياً، أو أي خوارزميات يتم الموافقة عليها من قبل الجهة المختصة بذلك.
- وضع التعليمات المناسبة التي تضمن إجراء عملية التشفير وفك التشفير بطريقة آمنة وصحيحة.
- تحديد وتوثيق أسماء الموظفين المخولين الذين يجب أن تصرف لهم مفاتيح تشفير وبرامج تشفير حسب متطلبات أعمالهم.
- وضع التعليمات التي تحدد كيفية التعامل مع الوثائق والملفات التي تم فقدان أو الإفصاح عن مفاتيح تشفيرها أو فك تشفيرها بشكل غير مرخص.
- وضع التعليمات الخاصة بإدارة مفاتيح التشفير، على أن تراعى فيها الأمور التالية:
  - حفظ نسخ احتياطية عن مفاتيح التشفير الخاصة بالإدارة في مكان آمن لاستعمالها عند الحاجة.
  - مواصفات الأنظمة والبرمجيات المستخدمة في إدارة مفاتيح التشفير طوال دورة حياتها.
  - اعتماد أو إلغاء اعتماد مفاتيح التشفير (عند الإفصاح عنها بشكل غير مرخص أو استقالة الموظف مثلاً).
  - يجب تحديد مدة صلاحية المفاتيح وتغييرها بصورة دورية.
  - يجب تحديد الحد الأدنى لأطوال مفاتيح التشفير المستخدمة.
  - إدارة مفاتيح التشفير داخل الجهة الحكومية بشكل آمن.

15

سياسة الحماية من الشفرات الخبيثة وفيروسات الأجهزة

- يجب تنصيب برامج موثوقة ومرخصة لمكافحة الفيروسات والبرامج الخبيثة على جميع أجهزة الحاسوب المملوكة للجهة الحكومية من خوادم، وأجهزة محمولة، وأجهزة مكتبية، مع متابعة تحديثها بشكل مستمر.
- عند ظهور فيروسات لا تستطيع برامج مكافحة الفيروسات الكشف عنها والتخلص منها، فإنه يجب على الدعم الفني للجهة الحكومية الاتصال بالدعم الفني صاحبة المنتج، ومحاولة مكافحة الفيروس بأنفسهم بأسرع وقت ممكن.
- يجب فحص الملفات المنقولة عبر شبكات الحاسوب للجهة باستخدام برامج مكافحة الفيروسات من أجل التأكد من خلوها من البرامج الخبيثة.
- على الجهة الحكومية إجراء تقييم بين فترة وأخرى للتأكد من مدى مطابقة برامج مكافحة الفيروسات وإعداداته بما يتوافق مع سياسات أمن وحماية المعلومات.
- على الجهة الحكومية تطبيق الفقرات الخاصة بالتعامل مع البرامج الخبيثة في سياسات البريد الإلكتروني.
- يمنع استخدام وسائط التخزين والملفات من المصادر مجهولة الأصل إلا بعد فحصها وتنظيفها من الفيروسات والشيفرات الخبيثة.
- يمنع الموظفون من تطوير أو تشغيل أو نسخ أو نشر فيروسات الكمبيوتر أو الشفرات الخبيثة.
- يجب على الجهة الحكومية أن تنفذ تدابير مناسبة لحماية أجهزة الاتصال اللاسلكية أو الأجهزة الحاسوبية المتنقلة من الفيروسات والشيفرات الخبيثة.

16

سياسة النسخ الاحتياطية والاستعادة في حالة الكوارث

يجـب أن تتضمن خطة أمن المعلومات للجهة الحكومية على إجراءات واضحة للنسـخ الاحتياطي والاستعادة في حالة الكوارث كما يلي:

- وضع آليات النسخ الاحتياطي والاسترداد على أن يتم فحصها بشكل دوري وتنفذ بشكل سليم.
- أن يتـم تنفيذ النسـخ الاحتياطي علـى فترات منتظمة ومناسـبة لطبيعة العمل وعلى أن يتم مراجعة نشاطات النسخ الاحتياطي بشكل منتظم.
- حفظ نسـخ النسـخ الاحتياطي في مكان بعيد عن موقع النظـام على أن تكون محمية بشكل جيد، كما أن الوسائل المستخدمة في النسخ الاحتياطي أثناء النقل يجب أن تكون محمية من الأشخاص غير المصرح لهم بالوصول إليها أو الاستخدام الخاطئ.
- عند إعداد تعليمات النسـخ الاحتياطي فعلى الجهة الحكومية أخذ التاريخ الزمني للمعلومات المشـمولة في النسـخ الاحتياطية، والفترة الزمنية اللازمة لاسترجاع المعلومات.
- علـى الجهـة الحكومية تحديد المختصيـن المخولين والمعنيين بإجراءات النسـخ الإحتياطـي والتأكيـد على توثيـق كافة عمليات النسـخ الإحتياطـي والإحتفاظ بالسجلات التي تؤكد إتمامها بنجاح.
- وضع آليات آمنة لإتلاف وسـائط التخزين أو مسـحها عند إعادة اسـتخدامها بما يتلاءم مع سياسات تصنيف وحساسية المعلومات.

17

سياسة إدارة الحوادث الأمنية وخطة الاستجابة للطوارئ

- يجـب أن تضمن خطة أمن المعلومات إجـراءات واضحة لإدارة الحوادث المرتبطة بأمن المعلومات ومعالجتها بطريقة فعالة وفي الوقت المناسب.
- يجب توقع الحوادث الأمنية المحتملة والتخطيط للاسـتجابة لها وبما يتلاءم مع دراسة تقييم المخاطر المحتملة وخطط استمرارية الأعمال لدى الجهة.
- يجب على الجهة الحكومية إعداد خطة للاسـتجابة للطوارئ تتضمن تحديد فريق طوارئ ومهام وإجراءات واضحة ومناسبة.
- يتعيـن علـى المعنييـن الإبلاغ عن حـوادث أمـن المعلومات الهامـة المتعلقة بالهجمـات الإلكترونية ومحاولات الاختراق التي تتعرض لها الجهة، حتى يتسـنى للمختصين في وزارة الاتصالات وتقنية المعلومات تقديم الدعم الفني المناسب.

18

سياسة تقييم وتدقيق المخاطر الأمنية

- يجـــب أن يتم تقييـــم المخاطر الأمنية لنظم المعلومـــات والتطبيقات لمرة واحدة علـــى الأقل كل عامين، على أن يتم انجاز تقييم المخاطر الأمنية قبل التحســـينات والتغييرات الرئيسية المرتبطة بتلك النظم والتطبيقات.
- يجب أن يكون اســـتعمال البرمجيات المســـتخدمة لتحليل تقييـــم المخاطر الأمنية مقيدة ومضبوطة.
- يجـــب أن يتـــم تقييم نظم المعلومات دورياً من قبل مدققين من طرف مســـتقل وموثـــوق به ومعتمد من قبل وزارة الاتصالات وتقنية المعلومات، وذلك لتحديد الحد الأدنى من الضوابط اللازمة لتقليل المخاطر الأمنية إلى مستوى مقبول.
- يجب أن يتم مراجعة وتقييم مدى الامتثال لسياسات أمن المعلومات كافة.
- يجـــب أن يتـــم تقييد وضبط اســـتعمال البرمجيات المســـتخدمة لتحليـــل التدقيق الأمني.
- يجب ان يتم تأمين وتقييد نتائج عمليات التقييم والتدقيق وحصرها على المعنيين فقط.

19

سياسة مراقبة الأحداث الأمنية

- يجب على الجهات الحكومية تطبيق آلية لتحديد الحوادث ومراقبتها بهدف احتواء ومنع الحوادث الأمنية.
- يجب أن تكفل الجهات الحكومية أن سـجلات الأنظمة ومعلومات الدعم الأخرى محفوظة لغرض إثبات وتتبع الحوادث الأمنية.
- يجب إجراء خطوات فورية في حال وجود احتمال اختراق لأي نظام وفقاً لخطوات معالجة الحوادث الأمنية الموثقة.
- يجب على الجهات الحكومية أن تنشـئ وتوثق وتحفظ خطوات معالجة الحوادث الأمنية لأنظمة المعلومات التابعة لها.