الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة

الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

اللائحة رقم (1)

اللوائح التنظيمية الخاصة بالسياسة الوطنية لأمن المعلومات

النسخة الأولى

هاتف: 3937078 11 963+، فاكس 3937079 11 963+، ص.ب: قدسيا-47، بريد إلكتروني info@nans.gov.sy

ضبط الوثيقة

سجلات التغيير

Date	Author	Version	Change Reference
2/10/2014	مركز أمن المعلومات	1.0	

المراجعات

Date	Name	Position
12/10/2014	المدير العام للهيئة الوطنية لخدمات الشبكة	

جدول المحتويات

أولاً– مقدمة:

تهدف هذه اللائحة إلى تقديم دليل عمل للجهات الحكومية، بما يساعد على إعداد وتنفيذ وتطوير خطة إدارة أمن المعلومات لديها، من خلال توفير مجموعة من الإرشادات.

ترتبط هذه اللائحة بالسياسة الوطنية لأمن المعلومات الصادرة بالقرار التنظيمي رقم (7) تاريخ (2014/8/12).

ثانيا– التعاريف:

إن جميع التعابير المستخدمة في هذه الوثيقة متوافقة مع ما ورد في السياسة الوطنية لأمن المعلومات.

الهيئة: الهيئة الوطنية لخدمات الشبكة المحدثة بموجب قانون التوقيع الإلكتروني وخدمات الشبكة رقم /4/ لعام 2009.

المركز: مركز أمن المعلومات في الهيئة.

السياسة: السياسة الوطنية لأمن المعلومات (NANS/ISC/NSP1.0) المقرة بالقانون التنظيمي رقم (7) تاريخ 2014/8/12.

الجهة الحكومية: جميع الوزارات والهيئات والمؤسسات والشركات وغيرها التابعة لحكومة الجمهورية العربية السورية.

المعلومات: العلامات أو الإشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة التي تحمل معنى قابلاً للإدراك، مرتبطاً بسياق محدد.

الأصول المعلوماتية: هي البيانات والمعلومات والبنية التحتية والبيئة المحيطة بها(من تجهيزات أو برمجيات أو خدمات أو مستخدمين أو مرافق إلخ..).

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

أمن المعلومات: هو الوسائل والتدابير الخاصة بالحفاظ على سرية، وتوافرية، وسلامة المعلومات، وحمايتها من الأنشطة غير المشروعة التي تستهدفها.

أصالة المعلومات: خاصية كون الشيء حقيقياً ويمكن التحقق منه والثقة به، وضمان صحة الإرسال، أو الرسالة أو المُنشئ داخل نظام المعلومات.

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

سلامة المعلومات: الحماية من التعديل غير المرخص للمعلومات أو تدميرها، وضمان أصالة المعلومات.

توافرية المعلومات: ضمان النفاذ إلى المعلومات واستخدامها في الوقت المناسب وبشكل موثوق من قبل المخولين بذلك.

التشفير: تحويل البيانات (يدعى "نص عادي") إلى شيفرات (يدعى "نص مشفر") بشكل يحافظ على المعنى الأصلي للبيانات لمنع التعرف عليها أو استخدامها.

نقاط الضعف: خلل أو ضعف يمكن أن تتعرض له إجراءات أو تصميم أو تنفيذ أو الضوابط الداخلية لحماية الأنظمة المعلوماتية (من الممكن أن تحدث بشكلٍ عرضي أو أن يتم استغلالها بشكل مقصود) وينتج عنها خرق أو انتهاك لسياسة حماية الأنظمة المعلوماتية.

التهديدات: أي ظرف أو حدث أو فعل يمكن أن يسبب ضرراً على المعلومات من خلال تدمير أو كشف أو تعديل أو رفض خدمات أو أجزاء الأنظمة المعلوماتية.

المخاطر: احتمال أن يستخدم مصدر ما تهديد محدد (يحدث بشكلٍ عرضي أو يتم استغلاله بشكل مقصود) نقطة ضعف محددة في الأنظمة المعلوماتية.

النفاذ: القدرة على الاستفادة من أي مورد من موارد الأنظمة المعلوماتية.

البرامج الخبيثة: برنامج (مثال: حصان طروادة) يبدو كأنه يؤدي وظيفةً مفيدةً أو مرغوبة، ولكنه في الواقع يحصل على دخول غير مصرحٍ به إلى موارد الأنظمة المعلوماتية أو يخدع المستخدم لتنفيذ عملية مؤذية.

إدارة المخاطر: العملية الكلية لتحديد ومراقبة المخاطر ذات الصلة بالأنظمة المعلوماتية والحد من آثارها. وتتضمن تقييم المخاطر، ومقارنة المزايا والسيئات، وانتقاء وتنفيذ واختبار الإجراءات الوقائية وتقييم الحماية. تأخذ هذه المراجعة الشاملة لحماية الأنظمة المعلوماتية الفعالية والكفاءة بعين الاعتبار، متضمنةً الأثر على المهمة والقيود التي تفرضها السياسة والقوانين والأنظمة.

ثالثاً- خطة إدارة أمن المعلومات:

المرجع: البند (6-2) من السياسة الوطنية لأمن المعلومات NANS/ISC/NSP1.0

1. خطة إدارة أمن المعلومات هي عبارة عن وثيقة أو مجموعة من الوثائق مصادق عليها من قبل الإدارة العليا في الجهة المعنية تتضمن السياسات والإجراءات والتعليمات الخاصة بأمن المعلومات في هذه الجهة.
2. يتم إعداد خطة إدارة أمن المعلومات من قبل فريق مؤهل يرأسه مسؤول من الإدارة العليا في الجهة، ويضم في عضويته كل من مدير المعلوماتية وعدد من العاملين في مديرية المعلوماتية أو ما يكافئها لديها، إضافة إلى ممثل عن الشؤون الإدارية (شؤون العاملين) وممثل عن الرقابة الداخلية لدى الجهة المعنية.
3. تتضمن خطة إدارة أمن المعلومات مجموعة من سياسات أمن المعلومات في الجهة الحكومية، وذلك وفق أهمية المعلومات والبيانات أو الخدمات التي تقدمها، ووفقاً لتقدير المخاطر التي قد تتعرض لها منظوماتها.
4. تعتبر خطة إدارة أمن المعلومات لدى الجهة غير ثابتة ويمكن تغييرها بتغير بيئة العمل أو بتغير طبيعة عمل الجهة أو الخدمات التي تقدمها.
5. يتم نشر وتوزيع السياسات والتعليمات الخاصة بخطة إدارة أمن المعلومات على العاملين لدى الجهة والمتعاقدين معها.

6. لإعداد خطة إدارة أمن المعلومات يُطلب من الجهة تأهيل الفريق المكلف بإعداد خطة إدارة أمن المعلومات لديها تأهيل عالي المستوى بما يضمن تمكّنه من وضع الخطة اللازمة، ويُمكن للهيئة الوطنية لخدمات الشبكة القيام تأمين دورات متخصصة في هذا المجال.

رابعاً– تقييم ومعالجة المخاطر:

المرجع: البند (7–2) من السياسة الوطنية لأمن المعلومات NANS/ISC/NSP1.0.

1. يهدف تقييم المخاطر لجهة ما إلى تحديد التهديدات، والمخاطر الناجمة عن هذه التهديدات، وتحديد مدى تأثير هذه المخاطر على عمل الجهة بشكل عام والأنظمة المعلوماتية بشكل خاص، وذلك بهدف تحديد أولوية وضع وتطبيق سياسات أمن المعلومات الخاصة بمواجهة هذه المخاطر.
2. يتم وضع خطة لإدارة وتقييم ومعالجة المخاطر من خلال فريق أمن المعلومات في الجهة.
3. تتضمن خطة إدارة المخاطر تحديد التهديدات والمخاطر المحتملة والتي من الممكن أن تؤثر على عمل الجهة، وتقييم مستوى خطورتها وتأثيرها الفعلي على عمل الأنظمة المعلوماتية.
4. يجب أن تغطي سياسات أمن المعلومات الخاصة بالجهة جميع المخاطر المحتملة وذلك بحسب الأولوية وبناءً على درجة الخطورة وأهداف الجهة والخدمات التي تقدمها والجدوى الاقتصادية من تطبيق هذه السياسات، مثال: إذا أخذنا انقطاع التيار الكهربائي كتهديد، فهناك عدة تقييمات لهذا التهديد بحسب مجال عمل الجهة:

- في حالة كانت الجهة تقدم جميع خدماتها أو جزء منها عن طريق أنظمة إلكترونية فقط (مصارف، شركات اتصالات...) يعتبر الخطر الناجم عن تهديد انقطاع التيار الكهربائي مهم جداً لهذه الجهات، وبالتالي فمن المفروض أن تعطي هذه الجهات أهمية كبيرة جداً لسياسة استمرارية العمل والتي تتضمن استخدام وحدات عدم انقطاع ومولدات احتياطية أو حتى استخدام موقع احتياطي

كامل لتفعيل الخدمات في حالة انقطاعها وبالتالي الحفاظ على استمرارية الخدمة في حال انقطاع التيار الكهربائي.

- أما في حال كانت الجهة لا تقدم خدمات إلكترونية أساسية أو ذات أهمية فيمكن اعتبار تهديد انقطاع التيار الكهربائي لا يشكل خطراً على استمرارية العمل فلا يخصص له أهمية كبيرة في سياسات خطة إدارة أمن المعلومات.

5. التهديدات الأساسية والمخاطر الناجمة عنها:

نبين في الجدول التالي بعض التهديدات الأساسية التي يمكن أن تشكل خطر على الأصول المعلوماتية في جهة معينة:

نوع التهديد	التهديد
التهديدات الناجمة عن حوادث طبيعية	– فيضانات – زلازل وبراكين – تغيرات مناخية (درجة حرارة، رطوبة،...)
تهديدات ناجمة عن حوادث ضمن الأبنية	– حريق ضمن البناء. – تسرب في المياه داخل البناء. – مخاطر التلوث الناجمة عن مصادر داخل البناء. – تدمير المعدات أو التجهيزات سواء كان هذا التدمير متعمداً أو عن طريق الخطأ.

التهديد الناجم عن توقف الخدمات الأساسية	كهرباء، مياه، تكييف، اتصالات...إلخ.
التهديدات الناجمة عن التسرب الإشعاعي	– المجال المغناطيسي الكهربائي للتوتر العالي. – غرف الأشعة في المشافي وغيرها. – الرادارات في المطارات وغيرها.
التهديدات التي تستهدف المعلومات من خارج الجهة	– التجسس عن بعد. – سرقة البيانات أو وسائط تخزينها. – التنصت على البيانات خلال نقلها أو على المكالمات الهاتفية. – النفاذ إلى قواعد البيانات والتعديل عليها. – إيقاف الخدمات الإلكترونية من خلال هجمات الحرمان من الخدمة. – النفاذ إلى التطبيقات والعبث بها أو التعديل عليها. – تحميل البرمجيات الخبيثة إلى المنظومة المعلوماتية. – جميع عمليات الاختراق التي تتم من خارج الجهة.

التهديدات الناجمة عن المشاكل الفنية	– عطل أو فشل في التجهيزات (مخدمات، أجهزة اتصال،....). – الفشل في التطبيقات أو عملها بصورة غير صحيحة. – الأعطال في التيار الكهربائي أو أجهزة التكييف أو أي تجهيزات تؤثر على عمل الأنظمة المعلوماتية.
الاستخدام غير مصرح به للموارد أو استخدام الصلاحيات بشكل غير قانوني	– استخدام البرمجيات أو التجهيزات بغير الغرض الذي تم تخصيصها من أجله (كقيام أحد العاملين بنسخ بيانات خاصة بالجهة التي يعمل بها واستخدامها خارجها). – تجاوز المستخدمين للصلاحيات المعطاة لهم. – استخدام الصلاحيات الممنوحة من قبل الجهة بشكل غير قانوني. – استغلال الصلاحيات للقيام بأي نشاط غير قانوني كتنفيذ هجمات الحرمان من الخدمة

	DOS attack أو غيرها.

خامساً– سياسات أمن المعلومات:

المرجع، البند (1–3) في السياسة الوطنية لأمن المعلومات NANS/ISC/NSP1.0

1. تتضمن كل سياسة من سياسات أمن المعلومات البيانات التالية على الأقل:

- الهدف: على الفريق المكلف بوضع خطة إدارة أمن المعلومات وضع هدف لكل سياسة بحسب الغاية التي تم وضع هذه السياسة من أجلها.

مثال: لإعداد سياسة النسخ الاحتياطي يمكن أن يكون الهدف من السياسة هو حفظ نسخة احتياطية محمية للبيانات المهمة لجهة ما لاستعادتها في حالات الطوارئ.

- الجهة التي تخضع للسياسة: يجب تحديد القسم/الأقسام التي يُطلب منها تنفيذ كل سياسة من السياسات، مثال: من الممكن أن تكون الجهة المنفذة للسياسة المستخدم العادي أو قسم المعلوماتية في الجهة أو مديريات أخرى.
- الجهة المسؤولة عن مراقبة التنفيذ: يتوجب على الجهات العامة تحديد فريق أو شخص أو مديرية لمتابعة تنفيذ كل سياسة من سياسات أمن المعلومات والتأكد من مدى الالتزام بها.

مثال: تكون الجهة المسؤولة عن مراقبة التنفيذ قسم المعلوماتية، أو المدير المختص، أو رئيس القسم.

- المدة الزمنية للتنفيذ: يجب على أن تضمن خطة إدارة أمن المعلومات جدول زمني لتنفيذ كل سياسة من سياسات أمن المعلومات، وتتم متابعة مدى التقيد بالزمن المحدد للتنفيذ من قبل الجهة المسؤولة عن مراقبة تنفيذ هذه السياسات.

2. بناءً على تقييم ومعالجة المخاطر يتم تحديد سياسات أمن المعلومات والتي تتضمن العديد من السياسات الأمنية نورد أمثلة لبعض منها:

- سياسة إدارة التحكم بالنفاذ (الوصول واستخدام الأصول المعلوماتية)، ملحق (1).
- سياسة تصنيف المعلومات واستخدامها، ملحق(2).
- سياسة تطوير نظم المعلومات والتطبيقات وصيانتها، ملحق (3).
- سياسة النسخ الاحتياطي، ملحق (4).
- سياسة أمن الشبكات، ملحق (5).
- سياسة الأمن الفيزيائي وأمن البيئة المحيطة بالأصول المعلوماتية، ملحق (6).
- سياسة الحماية من البرامج الخبيثة، ملحق (7).
- سياسة التعامل مع شبكة الانترنت ومواقع التواصل الاجتماعي، ملحق (8).
- سياسة استخدام وإدارة الأصول المعلوماتية، ملحق (9).
- سياسة التشفير، ملحق (10).

ملحق (1)

سياسة إدارة التحكم بالنفاذ (الوصول واستخدام الأصول المعلوماتية)

1) معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2) يجب أن تتضمن هذه السياسة النقاط التالية:

أ. **المصادقة وقوائم النفاذ:**

- يجب أن يتم التحكم بالنفاذ إلى تجهيزات الشبكة ونظم المعلومات والموارد الخاصة من خلال قوائم ضبط النفاذ ACL(Access Control List)، بحيث يتم حصر المواقع التي يمكن النفاذ منها إلى تجهيزات الشبكة.
- استخدام وسائل مصادقة للتحقق من هوية الأشخاص الذين يمكنهم النفاذ إلى تجهيزات الشبكة ونظم المعلومات والتطبيقات وقواعد البيانات وتغيير إعداداتها.
- يفضل عدم النفاذ عن بعد للتجهيزات لتغيير الإعدادات، وفي حال استخدامها يجب استخدام بروتوكولات نفاذ محمية تستخدم وسائل تشفير قوية.
- تحديد صلاحيات كل مستخدم بالنفاذ إلى موارد الشبكة ومخدماتها وغيرها من التجهيزات الخاصة بنظم المعلومات من قبل قسم الدعم الفني، وتقييد عملية النفاذ بواسطة اسم مستخدم وكلمات مرور وغيرها من وسائل المصادقة (شهادة خاصة، بطاقة ذكية، علامات بيولوجية).

ب. **إعدادات تجهيزات الشبكة:** يجب أن تحقق مايلي:

- عدم استخدام بروتوكولات غير مشفرة في إدارة الشبكة.
- فصل بيانات إدارة الشبكة عن البيانات العادية ووضعها في شبكة افتراضية مستقلة.
- تعطيل عمل البروتوكولات غير الضرورية من الموجهات وتسجيل كامل الاتصالات من خارج الجهة إلى داخلها.
- تسجيل كل العمليات التي تجري على تجهيزات الشبكة من خلال نظام تسجيل مركزي ومراقبته بشكل مستمر.
- استخدام كلمات مرور قوية في إدارة تجهيزات الشبكة وتغييرها بشكل مستمر وتغيير كل كلمات المرور الافتراضية.
- إجراء نسخ احتياطي لإعدادات التجهيزات الشبكية بشكل متكرر وحفظها في مكان آمن.

ت. **الاختيار الأمثل لكلمات المرور:** تراعى الإرشادات التالية عند اختيار كلمة المرور:

- تجنب تضمين اسم المستخدم داخل كلمة المرور.
- تجنب استخدام كلمات المرور التي يصعب تذكرها أو كلمات المرور التي من السهل تخمينها (مثل الاسم، الكنية، تاريخ الميلاد،..)، وتجنب استخدام كلمات المعجم.
- ينبغي أن تكون كلمة المرور طويلة (أكثر من 10 محارف وحتى 14 محرف في التطبيقات الحرجة).
- استخدام مزيج عشوائي من الحروف والأرقام والرموز وأن تتضمن رموزاً خاصة كـ $ # @ كي يصعب تخمينها. حيث يمكن أن يعتمد كل شخص مصطلحات خاصة به لكلمة المرور؛ مثلاً يمكن اعتماد المحرف @ بدلاً من الحرف a ، والحرف o بدلاً من الرقم 0، والمحرف

! بدلاً من الرقم 1. فعلى سبيل المثال بدلاً من أن نكتب كلمة المرور على الشكل (samer1990) والتي تُعتبر كلمة مرور ضعيفة، يمكن كتابتها بالصيغة ($@m3r!99o) والتي هي عبارة عن كلمة مرور قوية ويسهل تذكرها.

- تجنب استخدام نفس كلمة المرور في جميع الحسابات الخاصة بالمستخدم.
- تجنب إفشاء كلمة المرور، وعدم كتابتها على أوراق خارجية.
- تجنب إرسال كلمات المرور عبر البريد الإلكتروني أو برامج المحادثة الفورية.
- تجنب تخزين كلمة المرور على الحاسوب بشكل ملف نصي، واستخدام برمجيات موثوقة وآمنة لتخزين كلمة المرور بشكل مشفر.

ملحق (2)

سياسة تصنيف المعلومات واستخدامها

1) معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2) يجب أن تراعى الإرشادات التالية وفقاً لخصوصية المعلومات في كل جهة:

- إنشاء قواعد بيانات لتخزين هذه المعلومات وإدارتها، وتنظيم حفظ واسترجاع جميع المعلومات المُخزنة، بشكل إلكتروني.
- تخزين وسائط حفظ المعلومات ونقلها في بيئة آمنة.
- الفصل الفيزيائي للشبكة التي تحتوي على المعلومات الحساسة الخاصة بالجهة عن الشبكة الداخلية المُخصصة للنفاذ إلى شبكة الإنترنت العالمية.
- عند الاستغناء عن وسائط تخزين المعلومات، يجب فصلها بشكل آمن والتأكد من خلوها من أي معلومة أو برنامج مخزن فيها، ومن ثم استخدام طرقاً آمنة وسليمة لمسح المحتويات السابقة.
- تطبيق الإجراءات والتدابير الاحترازية المناسبة عند نقل المعلومات الرقمية، ويشمل ذلك ما يلي:
  - تشفير المعلومات الهامة بشكل سري (إن أمكن).

- حساب تابع البصمة للبيانات المنقولة من مكان لأخر لتجنب تعديل هذه البيانات أثناء نقلها وخصوصاً إذا كانت البيانات المنقولة حساسة.
- إلحاق مستوى التصنيف بعنوان الملف الرقمي.
- على الجهة التي تستقبل المعلومات معاملتها بحسب تصنيفها.
- وضع السياسات والإجراءات المناسبة لضمان إمكانية استرجاع المعلومات المُشفرة في حال ضياع مفتاح التشفير أو فقدانه (في حال استخدام التشفير).
- استخدام البريد الإلكتروني الحكومي في تبادل المعلومات الرسمية بين الجهات واستخدام تقنيات التوقيع الرقمي والتشفير لحماية البريد الإلكتروني.

ملحق (3)

سياسة تطوير نظم المعلومات والتطبيقات وصيانتها

1) معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2) يجب أن تتضمن هذه السياسة النقاط التالية:

- تكوين فريق يقوم بالإشراف على نظم المعلومات قيد التطوير أو التعديل، وذلك لمتابعة العمل والتأكد من حُسن التنفيذ في كل مرحلة من المراحل سواء من ناحية أداء النظام للعمل المطلوب منه أو تحقيقه لمستوى الحماية المطلوب وغيرها.
- عند البدء بتطوير نظام معلومات ينبغي إجراء تقييم للتهديدات والمخاطر التي من المحتمل أن تواجه هذا النظام، وإيجاد طرق لتقليل نسبة تأثير هذه المخاطر إلى حد مقبول.
- عند تحديث نظام المعلومات إلى نسخة أعلى يجب الأخذ بعين الاعتبار الجدوى الاقتصادية، بالإضافة إلى التوافق مع متطلبات العمل ومدى الحاجة إليه ومدى استقراره من النواحي الأمنية.
- أن يتم إعداد خطط حماية لأنظمة المعلومات سواء كانت مستخدمة أو قيد التصميم، بالإضافة إلى ضرورة وجود نشرة خاصة ووثائق يتم فيها توصيف النظام بشكل مفصل.

- في حالة تعديل نظم المعلومات لأي سبب كان يجب تعديل النشرة والوثائق الخاصة به بما يتناسب مع هذا التعديل.
- يجب وضع ضوابط مناسبة لتصميم نظم المعلومات ضمن الجهة، بما في ذلك التطبيقات الخاصة بالمستخدمين وذلك لضمان عمل هذه الأنظمة بالشكل الأمثل بما ينعكس على استمرارية وجودة العمل.
- في حال تحديث أنظمة التشغيل الخاصة بالمخدمات أو غيرها من التجهيزات الحرجة ضمن الجهة يجب اختبارها للتأكد من أن هذا التحديث لا يؤثر سلبا على النواحي الأمنية الخاصة بهذه التجهيزات أو فيما إذا كانت النسخة الأحدث لا تتوافق مع متطلبات العمل أو مواصفات هذه التجهيزات.
- يجب التأكد من وجود موارد كافية ومناسبة تتوافق مع متطلبات نظم المعلومات وذلك لضمان استمرارية العمل والتأكد من إمكانية الوصول إلى هذه الأنظمة عند الحاجة إليه.
- يجب اختبار نظم المعلومات قيد التعديل أو التطوير في بيئة مستقلة عن بيئة العمل.
- يجب الأخذ بعين الاعتبار وجود سياسة مناسبة للنسخ الاحتياطي واستعادة البيانات في حال فقدانها خاصة بنظم المعلومات، وتأمين المتطلبات الخاصة بهذه السياسة من حيث توفر الموارد وغيرها.
- يجب تأمين مستوى كافي من التأهيل والتدريب لمستخدمي نظم المعلومات، وتعريفهم بمسؤولياتهم تجاه هذه الأنظمة من جميع الجوانب وكل حسب عمله.
- يجب أن تحتوي نظم المعلومات على وسيلة لتتبع الأحداث والأنشطة التي يتم تنفيذها عليها وذلك من أجل متابعة الأحداث في حالات الضرورة.

- يجب على الجهة التي تقوم بتطوير أو تعديل نظام معلومات معين تقديم تقارير مرحلية عن عملها في كل مرحلة من المراحل من أجل التأكد أن هذا النظام يتوافق مع متطلبات الجهة الطالبة له.
- يجب على الجهة وضع آليات مناسبة لتسجيل ومعالجة الأخطاء، بالإضافة إلى المراقبة الدائمة لبيئة أنظمة المعلومات لتسجيل أي حدث غير قانوني أو سلبي ضمنها.

3) متطلبات الحماية لنظم المعلومات:

يجب وضع خطة حماية تتضمن المتطلبات الخاصة بحماية أي نظام معلومات سواء كان قيد التصميم أو تحت الاستخدام، ونبين فيما يلي بعض النقاط التي يجب أخذها بعين الاعتبار:

- يجب وضع ضوابط تضمن التحكم بالنفاذ إلى نظم المعلومات بما يتوافق مع سياسات التحكم بالنفاذ في السياسة الوطنية لأمن المعلومات، بالإضافة لتأمين وسائل للتأكد من سلامة محتوى البيانات المرسلة من وإلى هذه الأنظمة.
- وضع ضوابط للتحكم بصلاحيات المستخدمين للنفاذ إلى نظم المعلومات، وكذلك التحكم بصلاحيات النفاذ الخاصة بالتقنيين ضمن الجهة وتحديد الأشخاص المخولين بالنفاذ إلى هذه الأنظمة.
- إعلام المستخدمين والمسؤولين عن تشغيل وصيانة نظم المعلومات عن مسؤولياتهم عند استخدام هذه الأنظمة.
- يجب توفير مستويات حماية جيدة لنظم المعلومات وذلك لضمان سرية وتوافرية وسلامة محتوى البيانات ضمنه.

- يجب مراقبة آخر التحديثات والترقيعات الأمنية Patches الخاصة بالشركة المصممة أو المنتجة لنظم المعلومات والتأكد من تطبيق جميع هذه التحديثات لسد الثغرات الأمنية في هذه الأنظمة ضمن الجهة وذلك بعد اختبارها والتأكد منها.
- يجب متابعة إخطارات الحماية الخاصة بالشركة المنتجة أو المصممة أو أي مصادر أخرى تقوم بنشر معلومات عن ثغرات أمنية ضمن المنتج وتقييم هذه الثغرات ومدى تأثيرها على نظام المعلومات وكيفية تلافي هذه الثغرات.
- يجب أن يتم عمل مسح أمني للثغرات الأمنية في نظم المعلومات التي يتم تصميمها قبل وضعها تحت الاستخدام، وكذلك الأمر بالنسبة لنظم المعلومات التي يتم التعديل عليها.
- يجب إجراء مسح دوري للثغرات الأمنية لنظم المعلومات قيد الاستخدام (سواء كانت هذه التطبيقات ضمن الشبكة الداخلية أو يتم استخدامها عبر شبكة الانترنت) لاكتشاف نقاط الضعف المحتملة واقتراح حلول لمواجهة المخاطر والتهديدات الناجمة عن هذه الثغرات.
- يجب أن تحتوي خطة الحماية الخاصة بأي نظام معلومات على معلومات عن متطلبات الحماية الخاصة بهذا النظام، بالإضافة للوسائل الخاصة بمواجهة المخاطر والتهديدات في كافة مراحل التصميم أو الاستخدام لهذا النظام.
- لا يجب أخذ اعتبارات الحماية ومتطلباتها بمعزل عن الوظيفة المطلوبة من نظم المعلومات، بمعنى آخر يجب أن يتم إجراء توازن بين حماية نظام المعلومات من جهة وأداء هذا النظام للعمل الذي صمم من أجله من جهة أخرى، وأن لا يتم التركيز على جوانب الحماية على حساب أداء النظام ككل.

- يجب أن تكون خطة الحماية الموضوعة من أجل نظام المعلومات شاملة وأن يتم تحديثها في كل مرحلة من مراحل دورة حياة هذا النظام سواء في مرحلة التصميم أو التنفيذ أو الاستخدام...إلخ، بمعنى أنه يجب أن يكون هناك تحديث على الخطة في كل مرحلة من المراحل، ليكون في النهاية هناك خطة حماية متكاملة خاصة بنظام المعلومات قيد التطوير.
- يجب أن تتضمن كل من نظم المعلومات ونظم التطبيقات وقواعد البيانات على ضوابط ومحددات لضبط مُدخلات أو مخرجات هذه الأنظمة والتحقق من صحتها.
- يجب أن لا يُسمح باستخدام معلومات شخصية أو معلومات حساسة لأغراض الاختبار في نظم المعلومات.
- في حالات استبدال أو إخراج نظام معلومات من الخدمة يجب أن تكون هناك طرق آمنة لإجراء ذلك دون كشف المعلومات والبيانات التي يحتوي عليها هذا النظام وخصوصاً البيانات السرية.
- يجب أن تكون بيئة تطوير نظم المعلومات أو تعديلها محمية بشكل جيد، وتشمل هذه الحماية الأشخاص والتجهيزات والبيانات وكل ما يتعلق بهذه البيئة.
- عند استخدام نظم المعلومات يجب التقيد بسياسات النفاذ في السياسة الوطنية لأمن المعلومات من حيث كلمات المرور المستخدمة أو سياسات منح الصلاحيات وغيرها.
- يجب حماية ملفات أنظمة التشغيل التي تحتوي على أنظمة المعلومات والتطبيقات وقواعد البيانات بشكل كبير، ونبين فيما يلي بعض النقاط التي يجب أخذها بعين الاعتبار:
    - يجب عدم استخدام المخدمات التي تحتوي على بيانات حساسة للجهة كمخدمات مشتركة بحيث يوضع عليها تطبيقات أو برمجيات أو تفعيل خدمات يتم استخدامها من خارج الجهة أو داخلها، وذلك بهدف حماية هذه البيانات، بمعنى آخر يجب الفصل بين

التطبيقات أو نظم المعلومات أو قواعد البيانات غير ذات الصلة، وذلك منعا لتسرب كامل البيانات في حال حصول أي خرق أمني.

- على الجهة التي تقوم بتطوير نظم معلومات جديدة أن لا تقوم بتشغيلها ضمن البيئة الفعلية للشبكة في مرحلة التطوير.
- في حالة قررت الجهة تحديث أو تغيير نظام التشغيل يجب الأخذ بعين الاعتبار متطلبات العمل ودراسة الإصدار الذي سيتم التحديث إليه من الناحية الأمنية.
- يجب حفظ ملفات تسجيل الأحداث في أنظمة التشغيل لمعرفة جميع الأنشطة التي تتم عليها، ومحاولات الوصول غير شرعية التي تستهدفها.
- يجب أن تضع الجهة ضوابط على تنصيب البرامج على أنظمة التشغيل، بالإضافة إلى تحديد الأشخاص المخولين بعمل ذلك.

4) حماية التطبيقات الخاصة بتقديم الخدمات عبر شبكة الانترنت:

بالإضافة إلى النقاط السابقة الخاصة بمتطلبات الحماية لنظم المعلومات يجب أن تُأخذ النقاط التالية بعين الاعتبار:

- يجب التأكد من أن جميع المستخدمين المستفيدين من الخدمة المقدمة (مستخدمي التطبيق عبر شبكة الانترنت) على علم مسبق بصلاحيات نفاذهم إلى نظم المعلومات أو استخدامهم لها.
- يجب توفير وسائل حماية للبيانات السرية مثل البيانات الشخصية التي يتم إرسالها عبر الشبكة كتشفير هذه البيانات وفق سياسة التشفير في السياسة الوطنية لأمن المعلومات.
- استخدام التوقيع الرقمي من قبل الأطراف المشتركة في استخدام هكذا خدمات وخصوصاً في حال كانت هذه الخدمات مالية.

- يجب أن يكون الاتصال الذي يتم عن طريقه تقديم الخدمة آمن ومحمي بشكل جيد وذلك من خلال استخدام بروتوكول طبقة المقبس الآمن.
- يجب أن تكون التطبيقات وقواعد البيانات المستخدمة محمية بشكل كبير وأن تكون مفصولة بأكثر من مستوى حماية عن شبكة الإنترنت، وأن لا يتعامل الزبون مع المخدمات التي تحتوي على قواعد البيانات بشكل مباشر.

ملحق (4)

سياسة النسخ الاحتياطي

1) معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2) يجب أن تحقق سياسة النسخ الاحتياطي المتطلبات التالي كحد أدنى:

- توفر آلية واضحة ومناسبة للنسخ الاحتياطي تتضمن صيغة النسخ الاحتياطي (نسخ كامل أو جزئي (تراكمي) وكذلك تردده يومي أسبوعي، شهري، سنوي.....) على أن تتوافق هذه السياسة مع متطلبات الجهة وكذلك مدى سرية وأهمية البيانات بالنسبة لها.
- يجب وضع النسخ الاحتياطية في مكان آمن ومحمي فيزيائيا ومؤمن ضد الحوادث الطبيعية.
- إمكانية النفاذ إلى برمجيات النسخ الاحتياطي ومخدماتها من قبل عدد محدود من المستخدمين ووفق صلاحيات محددة.
- يجب أن تكون عملية النسخ الاحتياطي آلية ومجدولة خلال أوقات محددة ومناسبة.
- يجب أن تتم مراقبة عمليات النسخ الاحتياطي أثناء عملها من قبل الفريق الفني في الجهة لمعرفة أنها تتم بشكل نظامي.
- توفر تجهيزات خاصة بالنسخ الاحتياطي، توفر مساحات تخزينية كبيرة بالإضافة إلى توفر برمجيات خاصة بالنسخ الاحتياطي واستعادة هذه النسخ في حال الحاجة إليها.

- يجب اختبار وسط التخزين الذي تخزن عليه النسخ الاحتياطية باستمرار للتأكد من إمكانية الاعتماد عليه في حالات الطوارئ.
- يجب تخزين نسخ احتياطية كاملة ودقيقة، وفي حال كانت البيانات على مستوى كبير من الأهمية والسرية يجب تشفير النسخة الاحتياطية.
- وجود سياسة مناسبة لأرشفة نسخ البيانات التي يتم إجراء نسخ احتياطي لها – تبين أنواع البيانات التي يتم أرشفتها ومدة الأرشفة ودوريتها– على أن يتم تخزين النسخ المؤرشفة ضمن وسائط تخزين مفصولة عن وسط التخزين الخاص بالنسخ الاحتياطي.

3) **البيانات التي يجب نسخها احتياطياً:**

- البيانات الخاصة بملفات تسجيل الأحداث في أنظمة التشغيل والتجهيزات المستخدمة بالإضافة إلى ملفات سجلات أنظمة التشغيل.
- جميع بيانات وإعدادات الخدمات الفعالة على المخدم.
- بيانات مخدمات مشاركة الملفات في حال وجودها.
- بيانات مخدمات البريد الإلكتروني.
- بيانات مخدمات الويب وبيانات المواقع المستضافة.
- بيانات مخدمات قواعد البيانات، بالإضافة للبيانات المخزنة ضمن قواعد البيانات الموجودة.
- بيانات متحكمات المجال والدليل الفعال.
- جميع إعدادات التجهيزات والمخدمات الخاصة بالجهة.
- جميع البيانات والكتب الرسمية والمعاملات والمعلومات المهمة بالنسبة للجهة.
- بيانات ومعلومات المستخدمين والموظفين ضمن الجهة.

4) **التوثيق:** يجب أن تتضمن سياسة النسخ الاحتياطي على جزء خاص بالتوثيق، ونبين فيما يلي الحد الأدنى من البيانات المطلوب توثيقها:

- توثيق أوقات استعادة البيانات بعد تلفها وكذلك أوقات اجراء النسخة الاحتياطية.
- توثيق معلومات عن صيغة النسخ الاحتياطي – نسخ كامل أو تراكمي – وكذلك تردده (يومي، أسبوعي ،شهري ، سنوي.....).
- معلومات عن الأشخاص المخولين بالوصول لوسائط تخزين البيانات المنسوخة احتياطياً أو المؤرشفة وأوقات وصولهم إليها.
- معلومات عن الأشخاص المسؤولين عن متابعة عمليات النسخ الاحتياطي واختبارها، وصيانة التجهيزات الخاصة بها، واستعادة هذه البيانات عند الحاجة.
- معلومات عن التجهيزات المتوفرة والسعة التخزينية والبيانات المخزنة عليها والبرمجيات المستخدمة في النسخ الاحتياطي واستعادة البيانات مع النسخة الخاصة بهذه البرمجيات.

5) **استعادة البيانات:**

- تتم استعادة البيانات المنسوخة احتياطياً عند حصول مشكلة بالبيانات الأصلية أو تدميرها لأي سبب من الأسباب.
- يجب أن تكون البيانات المنسوخة احتياطياً متاحة دائماً عند الحاجة لاستعادتها.
- يجب أن تتم عمليات استعادة النسخة الاحتياطية للبيانات من قبل فريق فني مختص يملك صلاحيات ذلك.
- يجب أن تتم عملية اختبار لإمكانية استعادة البيانات المنسوخة احتياطياً مرة واحدة كل شهر كحد أدنى.

ملحق (5)

سياسة أمن الشبكات

1) معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2) أمن الشبكات السلكية:

1. يجب أن تأخذ سياسة أمن الشبكات النقاط التالية بعين الاعتبار:

- يجب على كل جهة حماية الشبكات أنظمة المعلومات لديها (برمجيات، أدوات، معلومات، تجهيزات معالجة وإدارة البيانات) عبر وسائل حماية برمجية وتجهيزات بالإضافة إلى تجهيزات مراقبة الاستخدام والنفاذ.
- تكون المديرية الفنية المختصة في الجهة مكلفة بضمان الرقابة والمتابعة الفنية الدورية، للتأكد من التزام المُستخدمين بإرشادات الاستخدام والنفاذ الآمن.
- يجب على الجهة إجراء مسح أمني للشبكة وتجهيزاتها بشكل دوري لتقييم ومعالجة الثغرات التي يمكن استغلالها من قبل المخترق.
- يُصرح لمستخدمي الأنظمة والشبكات المعلوماتية في أي جهة استخدامها فقط لأغراض تخص العمل.

- لا يجوز استخدام الأنظمة والشبكات المعلوماتية في غير الأغراض المخصصة لها، أو بما يؤدي إلى الإضرار بالجهة أو بسمعتها.
- يُعتبر المُستخدم مسؤولاً مسؤولية كاملة عن كل ما يصدر عن حاسوبه أو عن الحساب الخاص به، وعليه الحرص على أمن النفاذ للنظم المعلوماتية التي يستخدمها.
- يمنع استخدام الشبكات والأنظمة المعلوماتية للأغراض التالية:
  - في أي عمل أو غرض يتنافى مع الأخلاق والآداب العامة والقيم الدينية.
  - النفاذ أو محاولة النفاذ إلى حسابات المستخدمين الآخرين أو محاولة استخدامها دون تصريح.
  - انتحال شخصية مستخدم أو جهاز آخر.
  - العبث بالمعلومات الخاصة بمستخدمين آخرين أو الاطلاع عليها أو نشرها أو محاولة فك تشفيرها دون تصريح.
  - مشاركة الآخرين في أي من حسابات الاستخدام الشخصية أو التنازل لهم عن تلك الحسابات، أو تيسير استخدامهم لها عن طريق التخويل المخصص له.
  - الاستخدام المسيء الذي يمكن أن يسبب تهديد شخصي، أو ابتزاز، أو تخريب، أو إزعاج، أو إهانة، أو مضايقة لأي شخص أو جهة أو أمنها الإلكتروني، مثل إرسال بريد إلكتروني بشكل متكرر، أو غير مرغوب فيه، أو لغرض الغش، أو لخداع الآخرين.
  - مراقبة أو محاولة مراقبة الاتصالات الإلكترونية للمستخدمين الآخرين عبر الشبكة المعلوماتية (التنصت) إلا من قبل الجهات المرخص لها.

- تعطيل الشبكة الحاسوبية الداخلية عن العمل، أو منع الوصول إليها، أو تدمير، أو حذف البرامج، أو تسريبها، أو إتلافها، أو تعديلها، أو فتح ثغرات أمنية في الشبكة، أو النشر المعتمد للفيروسات والبرمجيات الضارة وأعمال القرصنة والاحتيال.
- النفاذ غير المشروع إلى البيانات الخاصة بالجهة عبر الشبكة الحاسوبية الداخلية في تلك الجهة، للاطلاع على تلك البيانات، أو تعديلها، أو حذفها، أو نشرها.
- إحداث أي تغيير فني في البنية التحتية للنظم المعلوماتية دون امتلاك صلاحية وموافقة رسمية من المديرية الفنية المختصة، بما في ذلك تعديل أو استبدال الأنظمة والبرامج والتطبيقات الحاسوبية.
- النفاذ غير المشروع إلى الموقع الإلكتروني للجهة، لتغيير محتوياته أو إتلافه، أو تعديله.
- إنشاء موقع إلكتروني يمثل الجهة، أو إدارته، دون موافقة رسمية من تلك الجهة.
- الإخلال بأي من حقوق النشر أو التأليف أو الطبع، أو حقوق الملكية الفكرية لأي بيانات أو معلومات أو مصادر، أو نسخ وتوزيع البرامج المحمية بحقوق النشر.
- التعامل باسم الجهة أو أي من أقسامها أو أي من موظفيها عبر شبكة الإنترنت دون موافقة رسمية بذلك.
- استخدام الأنظمة المعلوماتية بشكل يؤدي إلى إهدار وقت العامل.
- التواصل مع المنظمات الإرهابية، أو ترويج أفكارها، أو تمويلها، عبر شبكة الانترنت.
- مزاولة النشاطات التجارية والربحية عبر شبكة الإنترنت كالبيع أو الإعلان أو الدعاية أو التوظيف أو غير ذلك، إلا في حال كانت طبيعة الجهة تُتيح ذلك.

2. أمن المخدمات المركزية:

يجب أن تتضمن سياسة حماية المخدمات المركزية النقاط التالية:

- تحديث نظم تشغيل المخدّمات المركزية بشكل منتظم وخلال فترات زمنية تحدد من قبل الجهة المشرفة على عمل المخدّمات، بالإضافة إلى تنصيب وتطبيق كافة الرقع والتصحيحات التي يتم إصدارها من قبل الشركات المطورة لنظم التشغيل بهدف سد الثغرات الأمنية.
- إجراء عمليات الاختبار والصيانة الدورية للعتاد الصلب للمخدّمات كل ثلاثة أشهر على الأقل، بحيث تشمل الصيانة كافة أقسام المخدم، بالإضافة إلى تنظيم خطة مدروسة لإجراء عمليات الصيانة الفورية للأعطال التي قد تطرأ على المخدّمات أثناء أوقات العمل الاعتيادية، مع الحرص على توفر قطع التبديل الأساسية للاستخدام الفوري في حالة الأعطال المفاجئة.
- الفحص اليومي للمخدّمات ضد جميع أنواع البرمجيات الخبيثة والتأكد من إزالتها بالكامل في حال وجودها.
- التأكد من أن غرفة المخدّمات المركزية مغلقة بإحكام بعدة مستويات حماية فيزيائية (طريقة الأقفال المتعددة).
- تزويد غرفة المخدّمات بنظام مراقبة بالكاميرات يعمل على مدار الساعة.
- أن تحتوي غرفة المخدّمات على مقاييس للمؤشرات البيئية للفضاء الداخلي للغرفة، كمقاييس درجة الحرارة ومستوى الرطوبة. والتأكد اليومي من هذه المؤشرات لجهة ضبط الظروف التشغيلية الأفضل لعمل المخدّمات.
- التأكد من جاهزية نظام إطفاء الحرائق ضمن غرفة المخدّمات بشكل مستمر.

- تحديد وتوثيق أسماء الأشخاص المخولين بالدخول إلى غرفة المخدّمات ضمن جداول مخصصة يوضح فيها اسم الشخص والأيام والأوقات التي يسمح خلالها له بالدخول إلى الغرفة بالإضافة إلى تفاصيل الصلاحيات الممنوحة له.
- وضع خطط دورية لعمليات النسخ الاحتياطي والتأكد من حفظ أقراص وأشرطة النسخ الاحتياطية في خزانات معدنية مخصصة ومقاومة لمختلف أنواع الكوارث، ويجب أن تتوافق سياسة النسخ الاحتياطي مع سياسة النسخ الاحتياطي في السياسة الوطنية لأمن المعلومات.
- يجب أن تكون كلمات المرور الخاصة بإدارة المخدّمات عن بعد مختلفة تماماً عن كلمات المرور المخصصة لحسابات الإدارة العليا: (Root, Administrator, Admin, others) بالإضافة إلى ضرورة استخدام كلمات مرور معقدة وتتوافق مع سياسة كلمات المرور في السياسة الوطنية لأمن المعلومات.
- على التقنيين الذين يملكون صلاحيات النفاذ بحسابات الإدارة العليا: (Root, Administrator, Admin, others) أن يكونوا متخصصين ومن ذوي الخبرة في إدارة نظم التشغيل الشبكية.
- على التقنيين المخولين تشغيل وإدارة المخدّمات إبقاء عدد مرات استخدام حسابات الإدارة العليا في حدوده الدنيا ويفضل عدم استخدام هذه الحسابات إلا عند الضرورة القصوى.
- تفعيل خدمات مراقبة ومتابعة وتسجيل أداء وعمل نظم تشغيل المخدّمات.
- التأكد من حماية المخدّمات المركزية بالأدوات والبرمجيات المتخصصة كالجدران النارية ونظم منع/ كشف التطفل وغيرها.
- يجب على المستخدمين وعلى اختلاف مستويات صلاحيات نفاذهم إلى المخدّمات القيام بقفل شاشات الحواسيب الخاصة بهم لدى تركهم لمكاتبهم حتى إذا كان لفترات زمنية قصيرة.

- التأكد من إيقاف تشغيل محطات العمل التي من الممكن النفاذ عبرها إلى المخدّمات وغير المستخدمة حالياً ضمن وخارج أوقات العمل.
- يجب على جميع المستخدمين الاعتماد على كلمات مرور قوية، وتغييرها دورياً.
- يجب أن تكون كلمات المرور فريدة على مستوى الشبكة.
- تحديد عدد محاولات النفاذ غير الناجحة إلى المخدّمات بثلاث محاولات كحد أقصى.
- تحديد عدد الاتصالات المتزامنة بالمخدّمات بالنسبة لنفس الحساب باتصال واحد كحد أقصى.
- إعداد القيود الزمنية للنفاذ إلى موارد الشبكة بحيث يتم رفض أي محاولة نفاذ تتم خارج أوقات ساعات العمل الاعتيادية.
- إلزام المستخدمين الذين تتطلب طبيعة عملهم النفاذ إلى الشبكة بالنفاذ إليها عبر محطات عمل ثابتة ومحددة.

3. أمن التجهيزات والموارد الشبكية:

- يجب وضع تجهيزات الشبكة من مبدلات وموجهات في غرفة مخصصة محكمة الإغلاق لا يتم الدخول إليها إلا من قبل الموظفين المسؤولين عن الشبكة وأي دخول آخر يتم تحت إشرافهم.
- تأمين المخدّمات وكامل التجهيزات الشبكية من انقطاع التيار الكهربائي بوصلها إلى تجهيزات عدم انقطاع التيار الكهربائي، والتأكد من عملها بشكل مستمر بحيث تعمل عند انقطاع التيار الكهربائي ريثما تعمل المولدات البديلة.
- توثيق كافة الأسلاك والتوصيلات الشبكية ومتابعتها بشكل دوري بالإضافة إلى تعطيل كافة نقاط النفاذ إلى الشبكة في حال عدم استخدامها.

- مراقبة الشبكة من قبل قسم الدعم الفني بواسطة نظم كشف التطفل بشكل مستمر لكشف التصرفات غير الشرعية.
- تمرير جميع الاتصالات الداخلة والخارجة عبر الجدار الناري، وإعداد التجهيزات الشبكية بحيث تقوم بإنهاء جلسات الاتصالات غير الفعالة.
- تصميم الشبكة بحيث يتم فصل المخدّمات الموجودة على الانترنت عن الشبكة الداخلية من خلال DMZ.
- القيام بجرد متكرر من قبل قسم الدعم الفني للحواسيب الموجودة والبرامج التي تعمل عليها لملاحقة التغيرات الإضافية غير المسموحة في مكونات الحواسيب والبرمجيات غير المرخص لها.

3) الشبكات اللاسلكية:

1. مسؤوليات عامة:

- يجب على الجهة حماية التجهيزات الخاصة بالشبكة اللاسلكية فيزيائياً من حيث وضعها في مكان يصعب الوصول إليه من المخترقين، كأن توضع أعلى الحائط وأن لا توضع في أول الممرات أو عند باب المبنى. وذلك بهدف منع المخترق من الوصول لهذه التجهيزات وتصفيرها Reset أو إعادة إعدادها لإزالة إعدادات الحماية أو حتى سرقة هذه التجهيزات.
- دراسة مكان توضع نقاط النفاذ بحيث تغطي كامل المبنى، والحرص قدر الإمكان على عدم انتشار الإشارة خارج البناء كي لا يتمكن المخترق من الحصول على الإشارة الخاصة بالشبكة.
- توعية وإرشاد المستخدمين إلى الطرق الأنسب لاستخدام الشبكة والتدابير الأمنية التي يجب عليهم مراعاتها.

2. مسؤوليات مدير الشبكة:

- إلغاء تفعيل خاصية إعداد الحماية للشبكة اللاسلكية (WPS) وهي خدمة توفرها بعض تجهيزات الشبكة اللاسلكية، لكن هذه الخدمة غير آمنة وتحتوي على ثغرة أمنية قد تمكّن المخترق من التنبؤ بكلمة المرور عن طريق هجوم البحث الشامل Brute Force.
- في حال وجود عدد محدود ومعروف من مستخدمي الشبكة، يفضل استخدام خاصية الفلترة على مستوى العنوان الفيزيائي MAC.
- استخدام البروتوكول WPA/WPA2 مع خوارزمية التشفير AES كوسيلة حماية وتشفير للبيانات المنقولة عبر الشبكة مع ضرورة استخدام مفتاح تشفير قوي يتطابق مع سياسة الخاصة بكلمات المرور.
- تغيير الإعدادات الافتراضية الخاصة بتجهيزات الشبكة الداخلية مثل معرف الشبكة SSID أو اسم المستخدم وكلمة المرور الخاصة بإدارة التجهيزة وغيرها من الإعدادات.
- إلغاء بث معرّف الشبكة اللاسلكية SSID وذلك لمنع التقاطه من قبل المخترق.
- يفضل إلغاء تفعيل خدمة DHCP ومنح الحواسيب المتصلة بالشبكة اللاسلكية عناوين رقمية IP يدوياً.
- في حالة المؤسسات الكبيرة والتي تستخدم بيانات عالية الأهمية على الشبكة، يفضل استخدام مخدّم Radius أو tacacs/+ في عملية الاستيقان الخاصة بتجهيزات الشبكة الداخلية وعدم استخدام نمط المفتاح المشترك (PSK).
- تقييد النفاذ إلى الشبكة السلكية من قبل مستخدمي الشبكة اللاسلكية عن طريق قواعد Rules مُعدة خصيصاً لهذا الغرض.

- إعداد جدار الحماية Firewall أو نظام لكشف / منع التطفل IDS/IPS إن دعت الحاجة في مكان مناسب من الشبكة مع المراقبة الدورية لملف Log File الخاص به.
- عدم استخدام طريقة الإدارة عن بعد، واعتماد نمط الإدارة فقط للحاسوب المتصل بشكل مباشر مع التجهيزة الشبكية. وفي حالات الضرورة استخدام SSH أو SSL.
- التحديث الدوري لنظم التشغيل الخاصة بمكونات الشبكة اللاسلكية (موجهات، نقاط النفاذ.... الخ).
- المراقبة الدائمة للنشاطات الجارية عبر الشبكة لاكتشاف أي إجراءات مشبوهة قد تجري عليها.

3. مسؤوليات مستخدمي الشبكة:

- عدم إرسال أو بث حجم كبير من البيانات على الشبكة مما قد يؤثر سلباً على أداء الشبكة أو حجب الخدمة.
- عدم التنصت على حركة المرور عبر الشبكة أو نسخها أو تشغيل أي أداة لتحليل هذه البيانات.
- عدم مشاركة أو تبادل حسابات المستخدمين الخاصة بالنفاذ إلى الشبكة.
- على كل مستخدم تفعيل جدار الحماية ومضاد فيروسات مع تحديثه بشكل دوري على محطة العمل الخاصة به.
- على المستخدم استخدام كلمة مرور قوية على محطة العمل الخاصة بالمستخدم.
- يجب على المستخدم عدم استخدام الشبكة لمحاولة اختراق أحد التجهيزات أو محطات العمل على الشبكة أو النفاذ إلى البيانات بشكل غير قانوني.

ملحق (6)

سياسة الأمن الفيزيائي وأمن البيئة المحيطة بالأصول المعلوماتية

1)معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2)المتطلبات العامة للحماية الفيزيائية:

1. يجب تحديد مستويات الحماية المطلوبة للبيئة المحيطة بالاعتماد على أهمية الأصول المعلوماتية وأهمية الموقع، ويجب أن يعتمد كذلك على نتائج تقييم المخاطر التي يمكن من خلالها تحديد مستوى الحماية الفيزيائية المطلوب لكل موقع من المواقع.
2. يجب حماية وسائط التخزين والبيانات الحساسة لأي جهة بالإضافة لمخدماتها والتجهيزات الحرجة ضمن أماكن محمية بشكل كبير مزودة بأنظمة إطفاء حريق وتكييف ومقاييس للرطوبة وتغيرات درجة الحرارة ومحمية من النفاذ الفيزيائي إليها بأكثر مستوى، بالإضافة لتزويدها بمنظومة كاميرات مراقبة خاصة.

3. يجب عدم وضع التجهيزات التي يتم مشاركتها للمستخدمين العموميين ضمن المناطق المحمية التي تحتوي على بيانات حساسة أو تجهيزات أو مخدمات خاصة بالجهة، وذلك من أجل عدم السماح الأشخاص الدخول إلى المناطق المحمية (أو التذرع بهذه التجهيزات المُشاركة للوصول للمناطق المحمية).
4. يجب إحكام قفل الأبواب والنوافذ في المناطق التي تحتوي على البيانات ومراقبتها والتحكم بالنفاذ إليها، كما ينبغي الأخذ بعين الاعتبار حماية النوافذ الخارجية المطلة على خارج المنشأة كالنوافذ في الطوابق الأرضية أو النوافذ المطلة على أسقف أبنية مجاورة.
5. يجب تخزين المواد الخطرة كالمواد القابلة للاشتعال في أماكن محمية وبعيدة عن المناطق التي تحتوي على البيانات أو التجهيزات الحساسة.
6. يجب الانتباه إلى عدم وضع معلومات حساسة أو شاشات الحواسب أو المخدمات مقابل النوافذ أو الأبواب كي لا تتم سرقة معلومات معينة من قبل أشخاص متجسسين سواء كان هؤلاء الأشخاص يقومون بأعمال تنظيف النوافذ ويسترقون النظر إلى هذه الشاشات أو موظفين عاديين يقوموا بسرقة البيانات أثناء مرورهم أمام المكاتب.
7. يجب أن تكون المباني أو الغرف أو المواقع التي تحتوي على البيانات سليمة من النواحي التصميمية وعدم جود ثغرات أو نوافذ أو أي فتحات يمكن عن طريقها النفاذ إلى هذه المواقع والحصول على البيانات، ويجب أن تكون جميع جدرانها الخارجية متينة ومناسبة.
8. يجب أن تكون الأبواب والنوافذ الخارجية لأماكن تخزين البيانات قوية ومن الصعب الدخول القسري إليها بالإضافة لوجود وسائل حماية لها، مثل الأقفال المتعددة (أنظمة بصمة، بطاقة ذكية، ...) بالإضافة إلى تجهيزات إنذار خاصة.

9. يجب أن يكون في أي جهة مكتب استعلامات للمراقبة والتحكم بالأشخاص الذين يريدون الدخول للمنشأة وينبغي عدم السماح بالدخول قبل مراجعة هذا المكتب وتسجيل بيانات كاملة للشخص، ونبين فيما يلي الحد الأدنى من البيانات الواجب حفظها في سجل الزوار:
   - اسم الشخص.
   - اسم الجهة التي يعمل لديها.
   - اسم الشخص الذي يريد زيارته ضمن الجهة.
   - وقتي الوصول والمغادرة.
10. ينبغي على الموظف الذي تتم زيارته من قبل شخص معين أن يكون مسؤول عن هذا الشخص خلال وقت الزيارة، وعن عدم قيامه بأي عمل يضر بالجهة أثناء هذه الزيارة.
11. يجب على الجهة عدم السماح بالوصول لمواقع البيانات الحساسة والتجهيزات إلا للأشخاص المخولين بذلك مع وجود سجل يحتوي على معلومات الأشخاص ووقت الدخول والعمل الذي قام به ووقت الخروج.
12. عند الحاجة لاستدعاء جهة خارجية للقيام بأعمال الصيانة يجب أن يسمح لهم بالنفاذ المقيد إلى المناطق التي تحتوي على بيانات أو تجهيزات أو مخدمات خاصة بعمل الجهة، وأن لا يتم ذلك إلا في حالات الضرورة القصوى وبوجود أشخاص من الجهة، بالإضافة إلى ضرورة التحكم بدخول موظفي الخدمة كموظفي التنظيف وغيرها إلى المنشأة والمراقبة والإشراف على عملهم.
13. ينبغي عدم السماح باستخدام الكاميرات وأجهزة التصوير أو تسجيل الفيديو أو الصوت ضمن المناطق المحمية التي تحتوي على بيانات حساسة إلا بترخيص خاص، وأن يخضع هذا الأمر لرقابة صارمة من قبل الجهة.

14. عند ترك موظف العمل لأي سبب كان ينبغي أخذ جميع البيانات التي يمتلكها والتي تخص الجهة وإلغاء جميع الحسابات التي يمتلكها سواء على تطبيقات الجهة أو تجهيزاتها، وتغيير كلمات المرور التي يعرفها وإعلام مكتب الاستعلامات بأن هذا الشخص لم يعد عاملاً لدى الجهة.

15. يجب على الجهة الاختيار المناسب لأماكن وضع التجهيزات وذلك للحد من التهديدات والمخاطر التي تواجهها سواء كانت طبيعية أو مفتعلة مثل (السرقة، الحريق، التدخين، فشل في تمديدات أو شبكة المياه، الغبار، الاهتزاز، الآثار الكيميائية، الانقطاع في التمديدات الخاصة بالتيار الكهربائي داخل المبنى، التأثير الإشعاعي).

16. يجب وضع التجهيزات التي تتم مشاركتها مثل الطابعات والفاكسات وغيرها في أماكن آمنة وأن لا توضع في أماكن تعرضها للخطر مثل وضعها في الممرات أو غيرها.

17. يجب إزالة أوراق البيانات التي يتم طباعتها عن طريق الطابعة أو الفاكسات أو أي تجهيزة مشابهة بشكل مباشر بعد الطباعة كي لا تتعرض هذه البيانات للسرقة أو أي خطر آخر.

18. يجب على الجهة منع تناول الأطعمة أو المشروبات بجانب التجهيزات واتخاذ الاحتياطات الضرورية لمنع انسكاب أي مادة على هذه التجهيزات.

19. يجب على الجهة حماية البيانات والكتب الرسمية والوثائق المهمة في مكان محمي بشكل جيد من الوصول غير الشرعي إليها.

3) الحماية من انقطاع الطاقة وحماية الكابلات:

1. يجب على الجهة استخدام وحدات عدم انقطاع التيار الكهربائي للحواسب المكتبية والتجهيزات الشبكية (مبدلات وموجهات وجدران حماية ومخدمات، وغيرها)، وذلك لمنع فقد البيانات في حالات انقطاع التيار الكهربائي.

2. ينبغي فحص تجهيزات عدم انقطاع التيار الكهربائي بشكل دوري والتأكد من أنها تعمل بشكل سليم، والعمل على صيانتها إذا كانت هناك أي مشكلة بعملها.
3. يجب على أي جهة توفير مولدات احتياطية باستطاعة كافية لتشغيل التجهيزات الخاصة بها وأن يتم إعدادها لتقلع بشكل مباشر عند انقطاع التيار الكهربائي عن المنشأة مع إمكانية وجودة مولدة احتياطية خاصة بالتجهيزات والخدمات الحرجة من أجل تشغيلها في حالات الحوادث أو عدم عمل المولدات الرئيسية.
4. يجب أن تكون التمديدات والكابلات الخاصة بالكهرباء والاتصالات محمية بشكل جيد، كأن تكون محمية تحت الأرض عند مرورها خارج المنشأة أو في مكان من غير الممكن أن يتم اعتراضه أو تدميره من قبل المخربين.
5. يجب حماية التمديدات الشبكية أثناء مرورها داخل الجهة وذلك من خلال وضعها داخل قساطل خاصة بها وأن تكون على ارتفاع مناسب بحيث لا يمكن لأي شخص قطعها أو اعتراض البيانات التي تمر عبرها.
6. يجب على الجهة عدم وضع الكابلات الخاصة بالتيار الكهربائي مع الكابلات الخاصة بالشبكات أو الاتصالات في نفس القساطل أو تمريرها عبر نفس المكان وذلك لمنع التشويش أو تشوه الإشارات أثناء مرورها وبالتالي التأثير على دفق البيانات أثناء مروره.
7. ينبغي وجود كابلات احتياطية في حالات تلف الكابلات الرئيسية لأي سبب كان وذلك في الأماكن الحرجة لمنع انقطاع الخدمة.
8. يجب أن يكون لدى الجهة مخططات كاملة لجميع التمديدات سواء كانت خاصة بالتيار الكهربائي أو الشبكات أو الاتصالات أو غيرها.

4) حماية الغرفة الخاصة بمركز المعطيات Data Center:

1. يجب أن تكون الغرفة الخاصة بمركز المعطيات معزولة عن جميع التأثيرات الخارجية، ومزودة بجدران خاصة عازلة لتغيرات المناخ من درجة حرارة ورطوبة وغيرها.
2. يجب أن تكون الغرفة مزودة بباب متين من الصعب كسره أو اقتحامه عنوة مع أكثر من مستوى للقفل كاستخدام نظام بصمة أو بطاقة ذكية أو غيرها، مع تزويده بجهاز إنذار خاص بحالات الاقتحام أو فتحه عنوة.
3. يجب تزويد مركز المعطيات بمنظومة كاملة من تجهيزات إطفاء الحرائق التي تعمل بشكل أوتوماتيكي بالإضافة إلى منظومة كاميرات مراقبة ومنظومة إنذار خاصة وتجهيزات لمراقبة تغيرات درجات الحرارة والرطوبة وغيرها.
4. يجب تجهيز مركز المعطيات بتجهيزات تكييف خاصة به للمحافظة على التجهيزات من ارتفاع درجات الحرارة، بالإضافة إلى وجود تجهيزات خاصة بعدم انقطاع الطاقة ومولدة احتياطية خاصة به.
5. يجب حماية التمديدات والكابلات الشبكية والكهربائية وفق الجزء المتعلق بحماية التمديدات والكابلات.
6. يجب على الجهة تقييد الدخول إلى مركز المعطيات من قبل أشخاص محددين مع وجود سجل يتم فيه حفظ بيانات الدخول الخاصة بالمعنيين وسبب الدخول ووقته ووقت المغادرة والعمل الذي قام به.
7. يجب أن يتم أخذ نسخة احتياطية من جميع البيانات والإعدادات في مركز المعطيات ووضعها في مكان آمن ومحمي فيزيائياً وبعيد عن مكان النسخة الأصلية وذلك لمنع تلف النسخة الاحتياطية في حال تلف النسخة الأصلية.
8. يجب على الجهة الاحتفاظ بوسائط التخزين ضمن منطقة محمية بشكل جيد، على أن لا تكون عرضة للحوادث التي من الممكن حدوثها.

5) حماية الطرفيات (الحواسيب) التي تستطيع الوصول إلى البيانات الحساسة:

1. يجب أن يتم إغلاق المكاتب التي تحتوي على هذه الطرفيات عندما لا تكون قيد الاستخدام أو عدم وجود أي شخص داخلها.
2. يجب أن لا تكون شاشات هذه الطرفيات مكشوفة عن طريق النوافذ بشكل مباشر حتى لا يتم استراق النظر إلى بيانات مهمة.
3. عندما يتطلب العمل تغيير الأماكن التي يتم من خلالها الوصول للبيانات الحساسة في الجهة ينبغي دراسة الموقع الجديد وتقييم المخاطر التي من المحتمل وجودها والعمل على حلها قبل تغيير موقع العمل.
4. يجب على الجهة عدم استخدام طابعات شبكية للبيانات الحساسة، وخصوصاً إذا كانت هذه الطابعة غير موجودة فيزيائياً في نفس المكان، وإذا كان لابد من استخدام الطابعة الشبكية، فيجب استخدام طابعة خاصة يتم وصلها إلى الحاسب الخاص بمدير نظام المعلومات وأن تتم جميع عمليات الطباعة عن طريقه وذلك لمنع تسرب البيانات.
5. يجب إتلاف نسخ البيانات المهمة التي يتم طباعتها ولم يعد هناك حاجة لها بشكل مناسب، وذلك حتى لا يتم تسريب وثائق مهمة إلى متجسسين أو مخترقين أو غيرها عن طريق البحث ضمن النفايات.

6) الحماية الفيزيائية لتجهيزات الشبكة:

1. يجب وضع التجهيزات الخاصة بالشبكة (مبدلات، موجهات،...) ضمن خزانة خاصة مقفولة بإحكام، كما يجب أن توضع في مكان عالي لا يمكن الوصول إليه كأن توضع أعلى الحائط.
2. يجب أن تكون الخزائن الخاصة بالتجهيزات الشبكية ذات مراوح تهوية مناسبة لحماية هذه التجهيزات من درجات الحرارة.

3. يجب تزويد التجهيزات الشبكية بوحدات عدم انقطاع الطاقة لحمايتها من الانقطاع المفاجئ في التيار الكهربائي.
4. يجب تمييز الكابلات سواء الخاصة بالشبكة أو التيار الكهربائي أو غيرها عن طريق إشارات معينة (قصاصات ورقية مكتوب عليها) أو عن طريق الألوان.
5. وضع إجراءات لحماية هذه التجهيزات من الحوادث الطبيعية أو المفتعلة ضمن المبنى – حريق، فيضانات أو تسريب مائي، غبار أو تلوث أو غيرها–.

7) متطلبات الحماية الفيزيائية الخاصة بمستخدمي الحواسب الشخصية:

1. التأكد من وضع الحاسوب في الأماكن غير المغلقة، التي تسمح للهواء بالمرور إلى داخل مكونات الحاسوب من خلال فتحات التهوية.
2. حماية الحاسوب وملحقاته من خطر السقوط أو التعرض للصدمات.
3. إيقاف تشغيل الحاسوب بعد الانتهاء من العمل.
4. تجنب وضع أجهزة تولد طاقة حرارية بالقرب من الحاسوب، وتجنب وضع الحاسوب في مكان تصل إليه أشعة الشمس بشكل مباشر.
5. التأكد من تأمين شروط الحماية من مخاطر الطاقة الكهربائية، وذلك بعدم ربط الحاسوب مباشرة إلى مصدر الطاقة، حيث يفضل استخدام وحدة عدم انقطاع التيار الكهربائي UPS.
6. تجنب وضع المشروبات بالقرب من الحاسوب أو ملحقاته.
7. في حال حدوث أي عطل فني طارئ، ينبغي عدم العبث بالحاسوب، ومحاولة إصلاحه دون توفر خبرة فنية كافية، بل يجب الاتصال مباشرةً مع التقنيين المعنيين في قسم الدعم الفني.
8. تأمين مكان فيزيائي لحماية الحاسوب وملحقاته من الوصول إليه أو إلى أجزائه الداخلية.

9. الوقاية من مخاطر الهندسة الاجتماعية من خلال عدم السماح للمراجعين أو الأشخاص الغرباء أو الزوار أو الزملاء في العمل بالنظر الى شاشات الحواسيب أو لوحة المفاتيح.

ملحق (7)

سياسة الحماية من البرامج الخبيثة

1)معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2) يجب أن تتضمن السياسة الخاصة بالفيروسات والبرامج المؤذية النقاط التالية:

1. يجب إعداد سياسة مناسبة من أجل منع استخدام التطبيقات والبرمجيات غير المصرح باستخدامها ضمن الشبكة الداخلية الخاصة بها.
2. يجب أن تتضمن السياسة السابقة إجراءات من أجل الحماية من استخدام البرمجيات غير المصرح باستخدامها والكشف عن هذه التطبيقات في حال استخدامها وتحديد مكان استخدامها، بمعنى آخر وجود قائمة بالبرمجيات التي من المسموح استخدامها وفيما عدا ذلك تكون البرمجيات في القائمة السوداء ويتم كشفها ومنع استخدامها عند تنصيبها.
3. يجب تطبيق وسائل لمنع والكشف عن استخدام المواقع الإلكترونية التي تتضمن أو من الممكن أن تتضمن على محتوى مؤذي والذي من الممكن أن يضر بالشبكة الداخلية أو بتجهيزات الجهة، وذلك بوضع قائمة سوداء بالمواقع الإلكترونية التي يمنع تصفحها والعمل على حجبها عن طريق استخدام وسائل مناسبة.

4. يجب وضع سياسة مناسبة من أجل حماية الشبكة الخاصة بها من الملفات المؤذية التي من الممكن أن يتم تنزيلها من شبكة الإنترنت أو وسائط التخزين الخارجية القابلة للنزع (قرص صلب خارجي أو أي نوع من أنوع وسائط التخزين القابلة للنزع) بحيث تتضمن هذه السياسة مجموعة من الإجراءات الاحترازية التي يجب اتباعها لتجنب ذلك.
5. يجب اجراء مسح للثغرات الأمنية بشكل دوري وتقييم هذه الثغرات والعمل على سد الثغرات التي من الممكن أن تُستغل من قبل برامج مؤذية معينة.
6. يجب تنصيب برنامج نظامي للحماية من البرمجيات المؤذية وأن يتم تحديثه باستمرار وأن يتم عمل مسح دوري للحواسيب والتجهيزات ضمن الجهة على أن يشمل هذا المسح ما يلي:
   - جميع الملفات التي يتم استقبالها عن طريق الشبكة أو عن طريق أي وسائط تخزين خارجية لاكتشاف فيما إذا كانت تحتوي على ملفات مؤذية قبل استخدامها.
   - جميع المرفقات التي يتم استقبالها عبر البريد الإلكتروني وكذلك الأمر بالنسبة للملفات التي يتم تنزيلها من شبكة الانترنت، على أن يتم هذا الفحص في أكثر مكان أو مرحلة، فيجب أن يتم فحص هذه الملفات ضمن مخدم البريد الإلكتروني في حالة مرفقات البريد الإلكتروني كما يجب أن يتم فحصها أثناء مرورها ضمن الشبكة عن طريق تجهيزات خاصة، وكذلك الأمر فيجب فحصها ضمن الحاسب الشخصي الذي يستقبلها.
   - محتوى صفحات الويب للتأكد من خلوها من المحتويات المؤذية.
7. يجب تحديد المسؤوليات تجاه أنظمة اكتشاف الملفات والبرمجيات المؤذية والإجراءات المتبعة لتدريب العاملين على استخدامها، وكيفية التصرف في حالات الإصابة بهذه الملفات أو البرمجيات والإجراءات المتبعة للإبلاغ عن هكذا حوادث وكيفية التعامل معها.

8. يجب تأمين خطة بديلة في حالة حدوث إصابة بملفات أو برمجيات مؤذية وتعطُل الشبكة أو أنظمة المعلومات عن العمل، بحيث يتم تأمين استمرارية الخدمة وخصوصاً الخدمات الحرجة التي لا يجب أن تتوقف.
9. يجب أن يتم الاطلاع على معلومات عن البرمجيات المؤذية التي يتم إطلاقها وآخر الهجمات ذات الصلة وذلك عن طريق المواقع الإلكترونية المتخصصة بذلك أو مواقع شركات الحماية التي تنشر معلومات وأخبار عن ذلك وذلك بغية أن يبقى الفريق الفني لدى الجهة على دراية بأخر هجمات الملفات المؤذية وكيفية التعامل معها.
10. في حالات الإصابة ببرمجيات مؤذية من الممكن أن تضر بعمل الجهة ككل يجب أن يتم عزل البيئة المصابة وذلك لمنع انتشار الإصابة إلى كامل بيئة العمل، وأن يتم معالجة هذه الإصابة بشكل منفصل.
11. يجب أن تحتوي جميع المخدمات على نسخة نظامية من مضاد فيروسات من أحد الشركات المعروفة وأن يتم تحديثه باستمرار مع عمل فحص آلي لجميع الملفات والتطبيقات الموجدة أو التي يتم تنصيبها على المخدم.
12. يجب على فريق المعلوماتية في الجهة مراقبة الشبكة الداخلية للجهة من أجل معرفة فيما إذا تم تنصيب أي برمجيات مؤذية أو كان هناك أي سلوك غير نظامي على الشبكة.
13. يجب أن تحتوي المخدمات على برمجيات لمكافحة التجسس anti-spyware وذلك لحماية هذه المخدمات من الوصول غير الشرعي إليها سواء عبر الإنترنت أو من داخل الشبكة سواء هذا الوصول لتنصيب برمجيات أو أي غرض مؤذي من الممكن أن يؤثر سلباً على عملها.

ملحق (8)

سياسة التعامل مع شبكة الانترنت ومواقع التواصل الاجتماعي

1) معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2) الاستخدام الآمن لتطبيقات شبكة الانترنت:

1. يجب وضع سياسة مناسبة للنفاذ لشبكة الانترنت من قبل موظفيها وذلك من خلال حجب قائمة من المواقع غير مرغوب بها وبحسب طبيعة عمل الجهة.
2. وجود سياسة مناسبة لمراقبة النفاذ لشبكة الانترنت بحيث يتم وضع سجل للأحداث يحتوي على المواقع التي تم زيارتها والبروتوكولات والمستخدمة والزمن وغيرها.
3. تجنب إرسال أو ذكر أيّة معلومات شخصية أو مالية عبر مواقع الإنترنت (مثل أرقام البطاقات المصرفية أو رقم الهاتف الشخصي، ..) أو أية معلومات تدل على تفاصيل بيئة العمل كالعنوان ونوع العمل أو اسم الشركة وما إلى ذلك، يستثنى من ذلك المواقع الآمنة التي تستخدم شهادات رقمية موثوقة.
4. تجنب وضع أية صور شخصية أو عائلية كي لا يتم استغلالها لأغراض سيئة من قبل الآخرين.
5. تجنب كتابة أية بيانات قد تساعد المتلصصين على اكتشاف كلمة المرور المستخدمة في هذه المواقع.
6. الحذر عند قبول طلبات الإضافة من قبل أشخاص غير معروفين ومحاولة الاتصال بهم للتأكد من هوياتهم (عن طريق البريد الإلكتروني مثلاً) قبل قبول طلباتهم.

7. مراجعة سياسات الخصوصية في مواقع التواصل الاجتماعي المراد استخدامها، ويُفضل الاشتراك بالمواقع التي تراعي حجب ومنع بيانات المشترك الشخصية من الظهور للجميع إلا لأشخاص يقوم المشترك نفسه بالسماح لهم بمشاركته هذه البيانات.
8. التأكد من اعتمادية الموقع الذي يتعامل بالدفع الإلكتروني ومن الوجود الفعلي للمتجر أو الشركة عن طريق التقصي والبحث أو عن طريق الاتصال الهاتفي المباشر.
9. التأكد من استخدام البروتوكول الآمن (HTTPS) لمواقع الدفع الإلكتروني.
10. استخدام البطاقات ذات الرصيد المنخفض نسبياً في التعاملات الإلكترونية.
11. تجنب التعاملات المالية عبر الشبكات أو الحواسيب الموجودة في الأماكن العامة.

3) الاستخدام الآمن للبريد الإلكتروني:

يجب مراعاة الإرشادات التالية عند التعامل مع البريد الإلكتروني:

1. تجنب استخدام كلمة المرور الخاصة بالبريد الإلكتروني الرسمي عند التسجيل بالمواقع والمنتديات على شبكة الإنترنت.
2. تفعيل خاصية حذف الرسائل الواردة والصادرة والحاوية على فيروس تلقائياً في البرنامج المضاد للفيروسات.
3. عند إنشاء بريد إلكتروني جديد لدى إحدى الشركات العالمية التي تقدم خدمة البريد الإلكتروني المجاني كالـ Yahoo و Hotmail و Google وغيرها، يفضل اتباع ما يلي:
   - إدخال معلومات وهمية بحيث لا يتوقعها المُخترق، وخاصةً جواب السؤال السري.

- عند الانتهاء من قراءة الرسائل يجب تسجيل الخروج من موقع أو برنامج تصفح البريد الإلكتروني، لأن معظم برامج البريد أو المواقع تتذكر الزائر لمدة تصل إلى ثمان ساعات.

4. تجنب فتح أي ملف مرفق مع رسالة إلكترونية مُرسلة من مُرسِل مجهول، حتى وإن كان المُرفق موقعاً رقمياً أو ظهر على شكل ملف نصي أو صورة لا تحمل فيروساً لأنه يمكن التلاعب باسم الملف ليظهر الملف التنفيذي الذي يحمل فيروساً بمظهر سليم يحمل صورة أو نصاً.
5. تجنب فتح أي ملف مرفق مع رسالة إلكترونية مُرسلة من مُرسل معروف، إلا في حال توقع استقبال ذلك الملف. وفي حال الشك بسلامة الملف المرسل يمكن التحقق من المُرسل بأي طريقة اتصال مُتاحة، لوجود احتمال بأن يكون الإرسال قد تم بواسطة نوع من الفيروسات يقوم بإرسال رسائل عشوائية تحوي ملفات مؤذية إلى القائمة البريدية للمُرسل الفعلي.
6. التأكد من امتداد الملف المُرفق مع الرسالة قبل تشغيله على الحاسوب. مع التنويه إلى أن امتدادات البرمجيات المؤذية غالباً ما تكون على شكل ملف تنفيذي واضح مثلEXE، DLL.
7. إلغاء تفعيل خاصية تحميل الملفات المُرفقة مع الرسالة في برنامج تصفح البريد الإلكتروني.
8. فحص الملف المرفق المُراد تحميله على الحاسوب باستخدام برنامج مضاد للفيروسات للتأكد من خلوه من برمجيات مؤذية.
9. تجنب التحديثات الوهمية المُرسلة عبر البريد الإلكتروني والتي يزعم مرسلوها أنها مرسلة من الشركة الأم.
10. تفعيل خاصية فلترة الرسائل غير المرغوب بها في برنامج تصفح البريد الإلكتروني.
11. تفعيل خاصية استقبال الرسائل الإلكترونية من أشخاص غير موثوقين ضمن مجلد البريد غير المرغوب به في برنامج تصفح البريد الإلكتروني.
12. تجنب الرد على الرسائل الإلكترونية التي تطلب معلومات شخصية لأغراض مختلفة.

13. تجنب كتابة العنوان البريدي الشخصي أو الرسمي في مواقع الدردشة ومواقع الانترنت غير الموثوق بها.

14. حذف أية رسائل غير مرغوب بها فور وصولها أو عند اكتشافها.

4) إدارة الحسابات الرسمية للجهات على مواقع التواصل الاجتماعي

يمكن تكليف أحد العاملين في الجهة، بالتواصل الرسمي مع المواطنين عبر شبكات التواصل نيابةً عن الجهة نفسها، وتمثل كل التعليقات والآراء التي يرسلها هذا العامل وجهة النظر الرسمية لتلك الجهة، وفي هذه الحالة، يجب تحقيق المتطلبات التالية:

1. المتطلبات الإدارية:

- موافقة الجهة على إنشاء حساب على موقع التواصل الاجتماعي بوصفه حساباً رسمياً لهذه الجهة. ومن الأفضل أن تقوم هذه الجهة (قبل اتخاذ هذا القرار) باستشارة المديرية الفنية المختصة في تلك الجهة عن آلية التعامل مع أي مخاطر تقنية محتملة، فضلاً عن الرجوع إليها في مسائل مثل مراقبة إعدادات الخصوصية. ويجب أن تأخذ تلك الموافقة في اعتبارها عوامل عدة مثل مدى ملائمة شبكة التواصل لمتطلبات الجهة والمستفيدين.
- إصدار قرار تكليف العامل بإدارة الحساب على شبكة التواصل كتابةً بحيث يحدد الموقع المشار إليه، واسم ووظيفة العامل (أو العاملين) الذين سيتحملون مسؤولية إدارة هذا الحساب. وينبغي أيضاً أن يحدد القرار السياسات أو الخدمات المُحددة التي يمكن أن يشملها تواصل العامل مع المستفيدين عبر هذا الحساب.

2. المتطلبات الذاتية والسلوكية:

- درجة تأهيل العامل ومستوى تمكّنه من المسائل التي سيتم التواصل بشأنها ومناقشتها مع المستفيدين عبر شبكات التواصل.
- يجب أن يمتلك المُكلف مهارات لغوية ومهارات تواصل.
- يجب أن يكون على مستوى عالي من الوعي بشبكات التواصل الاجتماعي، ومُعتاد على استخدام طرق التواصل الموجودة ضمنها.
- مدى استعداده للبقاء على اتصال مع والمستفيدين عبر شبكات التواصل خارج أوقات الدوام الرسمي، والتعامل مع المواقف التي قد تتطلب الرد أو أي إجراء آخر في أي وقت من اليوم، وعلى مدار الأسبوع.
- التصرف بأسلوب يحفظ سمعة الجهة التي يعمل لديها.
- مراعاة أرقى المبادئ الأخلاقية في ردوده ومشاركاته التفاعلية.
- عدم استخدامه للمعلومات التي يحصل عليها أثناء أدائه للمهام الوظيفية في غير محلها.

3. متطلبات حماية خصوصية البيانات:

ينبغي على الجهات العامة تنفيذ المتطلبات التالية، كحدٍ أدنى لضمان حماية خصوصية البيانات من أي أخطار محتملة على الخصوصية قد تنتج من شبكات التواصل:

- تحديد نوع المعلومات التي يجوز للعاملين نشرها على شبكات التواصل.
- ألا يفترض العاملين وجود خصوصية في شبكات التواصل، فالتعليقات المُرسلة إلى تلك الشبكات تظل هناك لفترة طويلة، ويمكن لزوار تلك الشبكات الاطلاع عليها ونقلها إلى شبكات أو مواقع أخرى، من دون الحاجة إلى طلب تصريح من المُرسل.

- ضمان عدم استخدام العاملين عنوان أو كلمة مرور بريدهم الإلكتروني الحكومي لتسجيل الدخول إلى حساباتهم في شبكات التواصل.
- توعية العاملين بشأن أخطار الحماية هذه، وبخاصة الأخطار المرتبطة بالهندسة الاجتماعية، وأساليب التخفيف من المخاطر.

ملحق (9)

سياسة استخدام وإدارة الأصول المعلوماتية

1) معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2) يجب أن تحقق السياسة المتطلبات التالية:

1. يعتبر المستخدم مسؤولاً مسؤولية كاملة عن الحسابات الخاصة به على الشبكة الخاصة بالجهة وعن كلمات المرور الخاصة به وعدم إفشائها لأي سبب كان.
2. يجب على المستخدم عدم استخدام حساب خاص بمستخدم آخر حتى إذا كانت كلمة المرور الخاصة بهذا الحساب معروفة بالنسبة إليه.
3. يجب على المستخدم استخدام الأصول الخاصة بالجهة التي يعمل بها لأغراض العمل المخصصة لأجله وعدم استخدامه لأغراض شخصية.
4. يتوجب على المستخدم عدم نسخ التطبيقات أو البرمجيات الخاصة بالجهة التي يعمل بها لصالح أي جهة ثانية وعدم محاولة التعديل عليها إلا في حالة كان يملك صلاحيات لعمل ذلك.
5. يجب أن يكون هناك سياسة مناسبة لتنصيب البرامج ضمن حواسب الجهة وعدم السماح للمستخدم العادي بتنصيب برمجيات عشوائية على الحاسب الذي يتسلمه.

6. يجب على المستخدم عدم تحميل الملفات المؤذية أو الفيروسات إلى الشبكة الخاصة بالجهة وأن تكون هناك سياسة مناسبة لوصل وسائط التخزين القابلة للإزالة من قبل المستخدم وذلك وفقاً لضرورة العمل وضرورة عمل مسح لها قبل استخدامها.
7. على المستخدم عدم احتكار الموارد الخاصة بالجهة التي يعمل بها كأن يقوم بتحميل حجم كبير من البيانات واستهلاك عرض المجال المتاح ضمن الجهة وحرمان المستخدمين الآخرين من الوصول للإنترنت.
8. على المستخدم عدم إغراق الشبكة بكم كبير من البيانات مما يتسبب ببطئ فيها سواء كان ذلك عن قصد أو من دون قصد.
9. ينبغي على المستخدم عدم استخدام صلاحياته من أجل تسريب معلومات سرية تخص الجهة التي يعمل بها.
10. على الجهة حذف جميع الحسابات الخاصة بالموظف في حال تركه العمل أو تغير موقعه الوظيفي بحيث لا يتطلب موقعه الجديد الصلاحيات المعطاة له سابقاً.
11. يحظر على المستخدم محاولة الوصول القسري للبيانات والمعلومات غير مخول بالوصول إليها أو محاولة الحصول على بيانات حساب مستخدم أخر أو إجراء مسح للشبكة أياً كان نوعه ما لم يكن مخولاً بإجراء ذلك.
12. يجب على أي جهة أن تقوم بالتحقق من الأصول الخاصة بها بشكل دوري كأن تقوم بذلك في نهاية كل سنة على سبيل المثال، ويجب على الجهة كذلك حفظ سجل يحتوي على جميع الأصول الخاصة بها وتحديثه بشكل دائم.
13. يجب أن يكون لدى الجهة سياسة مناسبة للتخلص من الأصول في حال تلفها أو انتهاء فترة استخدامها.

14. يجب أن يتم توثيق حركة الأصول ضمن الجهة بشكل كامل وذلك في حال الحاجة إلى نقلها من مكان لآخر لضرورة العمل.
15. في حال استقالة الموظف أو تركه العمل لأي سبب كان يجب توثيق جميع الأصول المُسَلمة له واستلامها منه بشكل أصولي.
16. يجب أن يحتوي كل قسم أو دائرة ضمن الجهة على شخص مسؤول عن مراقبة الأصول وصيانتها والاستخدام الأمثل لها.

3) **تحميل وتنصيب البرامج على تجهيزات الجهة:** يجب أن يكون لدى الجهة سياسة مناسبة لتثبيت التطبيقات والبرمجيات تحقق ما يلي:

1. عدم تنزيل أو تنصيب برمجيات أو تطبيقات غير معتمدة أو غير موثوقة بشكل عشوائي من قبل المستخدم سواء كان بتنزيلها عبر شبكة الإنترنت أو أي مصدر خارجي.
2. يجب على مسؤولي الشبكة في الجهة عدم النفاذ إلى تجهيزات الشبكة عن بعد إلا بموافقة الجهة وبوجود اتصالات شبكة افتراضية خاصة محمية VPN أو أي وسيلة حماية موثوقة معتمدة من قبل الجهة.
3. يجب على موظفي الجهة عدم استخدام البريد الإلكتروني الخاص بالجهة لأغراض شخصية أو خارج مجال العمل وعدم استخدام حسابه الخاص بالبريد الإلكتروني للجهة من أجل التسجيل ضمن منتديات أو مواقع تواصل وغيرها إلا بموافقة الجهة.
4. يجب أن يكون لدى الجهة سياسة مناسبة خاصة بالنفاذ إلى شبكة الإنترنت من خلال الشبكة الخاصة بها بحيث لا تعطي صلاحيات كاملة لجميع الموظفين بالنفاذ إلى شبكة الإنترنت وإنما تتناسب هذه الصلاحيات مع حاجة عمل الموظف.

5. يجب على المستخدم عدم تشفير البيانات الخاصة بالجهة لحرمان باقي المستخدمين في الجهة من الاستفادة منها إلا إذا كانت هذه البيانات سرية ولا يسمح لباقي الموظفين الاطلاع عليها وخاصة بعمله.
6. يجب على المستخدم استخدام كلمات مرور قوية للنفاذ إلى أي حساب خاص به ضمن أي منظومة ضمن الجهة.

4) تأمين المستخدمين للحواسب المكتبية أو المحمولة الخاصة بعملهم:

1. يجب على الجهة تأهيل موظفيها وتوعيتهم للمخاطر الخاصة بسرقة البيانات وأساليبها وكيفية الحماية منها.
2. يجب على المستخدم عدم ترك الحاسب الخاص به من دون تسجيل خروج خلال فترات تركه له وذلك لمنع سرقة البيانات.
3. يعتبر الموظف مسؤول عن البيانات الموجودة لديه أو ضمن حاسبه مسؤولية كاملة فيجب عليه منع الوصول غير الشرعي إليها والعبث بها أو نسخها أو تعديلها.
4. يجب على الموظفين الحفاظ على التجهيزات التي تم تسليمها لهم نظيفة من الغبار وعدم الأكل أو الشرب بجانبها.
5. يجب على المستخدم اجراء نسخ احتياطي للملفات والبيانات المهمة على حاسوبه الشخصي والحفاظ عليها من التلف أو السرقة.
6. يجب على المستخدم عدم فتح أي مرفقات من البريد الإلكتروني إذا كانت ضمن بريد من جهة غير معروفة أو غير موثوق بها.
7. عدم تثبيت أو تحميل برامج أو تطبيقات بدون تصريح من الجهة التي يعمل لديها.

8.في حال تسلم المستخدم حاسب محمول ينبغي عليه حمايته من السرقة على سبيل المثال عدم تركه في السيارة أو الابتعاد عنه في الأماكن العامة وغيرها.

ملحق (10)

سياسة التشفير

1) معلومات السياسة:

الهدف من السياسة	الجهة المسؤولة عن التنفيذ	الجهة المسؤولة عن مراقبة التنفيذ	المدة الزمنية اللازمة للتنفيذ	المرجع في السياسة الوطنية لأمن المعلومات
تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	تحدد من قبل الجهة.	NANS/ISC/NSP1.0 (3-1)

2) يجب على أي جهة اعتماد سياسة خاصة بالتشفير لديها تتضمن ما يلي:

1. أن يتم تشفير جميع البيانات الحساسة أو المهمة التي يتم إرسالها خارج الجهة.
2. يجب أن تكون جميع الاتصالات البعيدة إلى تجهيزات الجهة مشفرة بوسائل تشفير قوية.
3. يجب تشفير جميع اتصالات الشبكة اللاسلكية عن طريق بروتوكولات حماية قويةً تتوافق مع السياسة الخاصة بحماية الشبكة اللاسلكية.
4. يتوجب حماية رسائل البريد الإلكتروني ومرفقاتها وتشفيرها في حالة كانت البيانات المرفقة مهمة، بالإضافة إلى ضرورة استخدام وسائل التوقيع الرقمي للحفاظ على سلامة الرسائل وضمان عدم تغيرها أثناء الإرسال.
5. على أي جهة أن تقوم بتصنيف البيانات ووسائط التخزين لديها على أساس أهمية البيانات التي تحتوي عليها.
6. توعية الموظفين ضمن الجهة إلى المخاطر التي تهدد البيانات لديهم وبضرورة تشفيرها وحمايتها من النفاذ غير الشرعي لها وبشكل رسائل البريد الإلكتروني التي يقوم المستخدم بإرسالها.

7. يجب تحديد مستوى التشفير وخوارزمية التشفير المطلوبة بالاعتماد على تقييم المخاطر وأهمية البيانات المراد حمايتها.
8. يجب على الجهة تحديد القواعد والمسؤوليات الخاصة بالسياسة كتحديد الجهات المسؤولة عن متابعة تنفيذ والتقيد بالسياسة بالإضافة إلى إدارة المفاتيح وتوليدها وغير ذلك.
9. يجب أن تحقق السياسة الخاصة بالتشفير المفاهيم التالية:

- السرية: استخدام التشفير لحماية البيانات المخزنة أو المرسلة لضمان عدم الاطلاع عليها من قبل الأشخاص غير المخولين بذلك.
- سلامة المحتوى: استخدام وسائل التوقيع الرقمي أو توابع البصمة لضمان سلامة محتوى البيانات سواء كانت مرسلة أو مخزنة.
- عدم الإنكار: استخدام تقنيات التشفير للتأكد من قيام شخص ما بنشاط محدد في وقت محدد.
- المصادقة: استخدام تقنيات التشفير في المصادقة على نفاذ المستخدم إلى منظومة معينة.

3) إدارة المفتاح:

1. وجود آلية محمية لتبادل مفاتيح التشفير مع إمكانية استعاد البيانات المشفرة في حالات ضياع مفتاح التشفير أو تسربه وغيرها.
2. أن يتم استخدام خوارزمية تشفير جيدة بالإضافة إلى مفتاح تشفير بطول مناسب وتوفير آليات محمية من أجل إدارة المفتاح من توليد وتبادل وغيرها.
3. يجب حماية مفاتيح التشفير من الفقدان أو التسرب أو التعديل بالإضافة إلى توفير حماية فيزيائية عالية لتجهيزات توليد أو تخزين مفاتيح التشفير.

4. يجب أن يتميز نظام توليد وإدارة المفاتيح بالمواصفات التالية:

- إمكانية توليد مفاتيح تشفير لمختلف أنظمة التشفير والتطبيقات.
- القدرة على إصدار شهادات رقمية للمفاتيح عامة.
- تخزين المفاتيح مع تأمين آليات للنفاذ إلى المفاتيح من قبل المخولين بذلك.
- إمكانية تعديل أو تحديث المفاتيح بالإضافة إلى قواعد تنظم عملية تغيير أو تجديد المفاتيح وتوقيتها.
- إمكانية إلغاء المفاتيح في حالات الحصول عليها من قبل المخترقين لأي سبب كان والعمل على إصدار مفاتيح جديدة.
- إمكانية استعادة المفاتيح في حالات ضياعها أو تلفها.
- القدرة على النسخ الاحتياطي للمفاتيح وأرشفتها.
- إمكانية تسجيل جميع الأحداث التي تجري ضمن منظومة إدارة المفاتيح ضمن ملفات تسجيل أحداث خاصة ومتابعتها باستمرار.