الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة

الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

السّياسة الوطنيّة لأمن المعلومات

(NANS/ISC/NISP1.0)

هاتف:٣٩٣٧٠٣٢ ١١ ٩٦٣+، فاكس: ٣٩٣٧٠٧٩ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني : info@nans.gov.sy

العمليّات على الوثيقة

سجلُّ التّعديل

مرجعيّة التّعديل	النّسخة	تأليف	التّاريخ
	1.0	مركز أمن المعلومات	٢٠١٤/٦/٢٩

سجلُّ المراجعات

ملاحظات	الاسم	التّاريخ

جدول المحتويات

الفصل الأوّل :أحكام تمهيديّة

١-١ مقدّمة

ساهم التّطور العلميُّ التّكنولوجيُّ في تحسينِ حياة الأفراد، وباتت تكنولوجيا المعلومات والاتّصالات الرّافعة الأساسيّة في تعزيزِ التّنمية البشريّة والاقتصاديّة والاجتماعيّة والثّقافيّة، حيث أدّت إلى نشوءِ أشكالٍ جديدةٍ من التّفاعل الاقتصاديِّ والاجتماعيِّ، ويمكنُ قياس ذلك من خلالِ الانتشار الواسع وحجم المعلومات المتبادلة على الشّبكة، كلُّ ذلك بفضل ما تمتاز به من سرعة الأداءِ وسهولة الاستخدام وتنوّع الخدمات.

ومع تعاظم دور تكنولوجيا المعلومات والاتّصالات، وتزايد أثرها على المؤسساتِ الاقتصاديّةِ والاجتماعيّةِ، ازدادت المخاطر على المنظومات المعلوماتيّة وتنوّعت واختلفت أساليبُها، وتجاوز أثرها سرقة المعلومات والاختراق والتّجسس إلى تعطيلِ الخدمات العامّة وإيقاع خسائرَ ماديّةٍ ومعنويّةٍ كبيرةٍ بالأفرادِ والمؤسسات والحكومات، وعُرف ما يُسمّى بالحروبِ الإلكترونيّة.

ممّا سبق وبناءً على توجيهات الحكومة في الجمهوريّةِ العربيّةِ السوريّةِ بضرورة تأمين بنيةٍ تحتيّةٍ آمنةٍ وموثوقةٍ لتقديم الخدمات الإلكترونيّة، وتوفير البيئةِ الملائمة لتقليل خطر اختراق المنظومات المعلوماتيّة الحكوميّة، وكشف محاولات الاختراق واتّخاذِ الإجراءات اللّازمة بأسرع وقتٍ ممكنٍ في حال حدوثها، فقد أعدَّ مركز أمن المعلومات في الهيئة الوطنيّة لخدمات الشّبكة السّياسةَ الوطنيّة لأمن المعلومات؛ والّتي تتضمّنُ المتطلّبات الأساسيّة الواجب توفّرها لدى الجهات الحكوميّة لضمان عملِ المنظومات المعلوماتيّة بشكلٍ آمنٍ ومستمرٍ وموثوقٍ .كما تُعنىْ الهيئة بالتّوعية والتّأهيل والتّدريب لجميع الجهات الحكوميّةِ في مواضيع أمن المعلومات والتّوقيع الرّقميِّ.

هاتف:٣٢٠٣٩٣٧ ١١ ٩٦٣+، فاكس: ٣٩٣٧٠٧٩ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

١-٢ *تعريفات*

الجهة الحكوميّة :أيّة من الوزاراتِ والهيئاتِ والمؤسساتِ والشّركاتِ وغيرها التّابعة لحكومة الجمهوريّة العربيّة السوريّة.

الجهات الخارجيّة :الأشخاص والشّركات والمؤسسات والمجموعات وغيرها–لو كانت حكوميّة– الّتي تتعاقد معها الجهة الحكوميّة لتأديةِ خدمةٍ أو مشروعٍ أو عملٍ ما.

الوزارة :وزارة الاتّصالاتِ والتّقانة.

الهيئة :الهيئةُ الوطنيّة لخدمات الشّبكة في وزارة الاتّصالات والتّقانة المُحدثَة بموجب قانون التّوقيع الرّقمي وخدمات الشّبكة ذي الرقم /4/ لعام ٢٠٠٩.

المركز :مركزُ أمن المعلومات في الهيئة الوطنيّة لخدماتِ الشّبكة.

المعلومات :العلامات أو الإشارات أو النّصوص أو الرّسائل أو الأصوات أو الصّور الثّابتة أو المُتحرِّكة الّتي تحمل معنىً قابلاً للإدراك، مُرتبطاً بسياقٍ محددٍ.

الأصول المعلوماتيّة :البيانات والمعلومات والبنية التّحتيّة والبيئة المُحيطة بها(من تجهيزاتٍ أو برمجيّات أو خدمات أو مستخدمين أو مرافق إلخ.).

المنظومة المعلوماتيّة :مجموعةٌ مُنّسقةٌ من الأجهزة والبرمجيات الحاسوبيّة والمُعدات المُلحقَة بها.

أمن المعلومات :الوسائل والتّدابير الخاصّة بالحفاظ على سريّة، وتوافريّة، وسلامة المعلومات، وحمايتها من الأنشطة غير المشروعةِ الّتي تستهدفُها.

أصالة المعلومات :خاصيّة كون الشيء حقيقياً ويمكن التّحقق منه والثّقة به، وضمان صحّةِ الإرسال، أو الرّسالة أو المُنشِئ داخل المنظومة المعلوماتيّة.

هاتف:٣٢ ٣٩٣٧٠ ١١ ٩٦٣+، فاكس: ٧٩ ٣٩٣٧٠ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

سريّة المعلومات :ضمان عدم الكشف عن المعلومات لأشخاصٍ أو عمليّاتٍ أو أجهزةٍ غير مصرّحٍ لها بذلك.

سلامة المعلومات :الحماية من التّعديل غير المرخّص للمعلومات أو تدميرها، وضمان أصالة المعلومات.

توافريّة المعلومات :ضمان النّفاذ إلى المعلومات واستخدامها في الوقت المناسب وبشكلٍ موثوقٍ من قبل المخوّلين بذلك.

التّشفير :تحويل البيانات (يُدعَى نصٌّ عاديّ) إلى شيفرات (يُدعَى نصٌّ مُشفّر) بشكلٍ يحافظُ على المعنى الأصلي للبيانات لمنع التّعرف عليها أو استخدامها.

المخاطر :احتمال وقوع حدثٍ من شأنه المساسُ بأمن المعلومات والآثار المترتّبة عن ذلك.

التّهديدات :ظرفٌ أو حدثٌ أو فعلٌ يمكن أن يسبب ضرراً على المعلومات من خلال تدميرها أو كشفها أو تعديلها أو إيقاف الخدمات الإلكترونيّة.

نقاط الضعف :خللٌ أو ضعفٌ يمكن أن تتعرّضَ له إجراءات أو تصميم أو تنفيذ أو الضّوابط الدّاخليّة لحماية النّظام (من الممكنِ أن تحدث بشكلٍ عرضيٍّ أو أن يتمَّ استغلالها بشكلٍ مقصودٍ)وينتجُ عنها خرقٌ أمنيٌّ أو انتهاك لسياسة حماية النّظام.

النّفاذ :القدرة على الاستفادة من أيِّ موردٍ من موارد منظومة المعلومات.

البرامج الخبيثة :برمجيّات حاسوبيّة مُصمّمة لإلحاق الضّرر بالأجهزةِ الحاسوبيّة أو المنظومات المعلوماتيّة أو المواقع الإلكترونيّة أو الشّبكة، أو تعطيل عملها أو تبطئته، أو تخريب محتوياتها أو مواردها، أو جمع معلوماتٍ عنها أوعن مالكيها أو مُستخدميها أو عن بياناتهم دون إذنهم، أو إتاحة الدّخول إليها أو استخدامها بصورةٍ غير مشروعةٍ.

هاتف:٣٢ ٣٩٣٧٠ ١١ ٩٦٣+، فاكس: ٧٩ ٣٩٣٧٠ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

إدارة المخاطر :العمليّة الكليّة لتحديد ومراقبة المخاطر ذات الصّلة بمنظومات المعلومات والحدّ من آثارها. وتتضمّنُ تقييم المخاطر، ومقارنة المزايا والسيئات، وانتقاء وتنفيذ واختبار الإجراءات الوقائيّة وتقييم الحماية. تأخذ هذه المراجعة الشّاملة لحماية النّظام الفعاليّة والكفاءَة بعين الاعتبار، مُتضمّنةً الأثر على المُهمّة والقيود الّتي تفرضها السّياسة والقوانين والأنظمة.

هاتف:٣٢٠٣٩٣٧ ١١ ٩٦٣+، فاكس: ٣٩٣٧٠٧٩ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

الفصل الثّاني: مدخل للسّياسة الوطنيّة لأمن المعلومات

٢-١ الأهداف

وضع الإطار العامّ للسّياسة الوطنيّة لأمن المعلومات بحيث تكونُ المرجع الرئيسي لجميع الجهات الحكوميّة في الجمهوريّة العربيّة السوريّة أثناء إعداد خطّة أمن المعلومات، وتهدف هذه السّياسة إلى:

١. تحديد المتطلّبات الأساسيّة لأمن المعلومات وما يجبُ القيام به لحماية الأصول المعلوماتيّة في الجهات الحكوميّة.
٢. توفير البيئة الآمنة لتقديم وتطوير الخدمات الإلكترونيّة.
٣. تحديد المهام والمسؤوليّات لتنفيذِ هذه السّياسة في الجهاتِ الحكوميّة.
٤. توفير مرجعيّة وطنيّة لكافّة النّواحي المُتعلّقة بأمن المعلومات.

سيقوم المركز بإصدار مجموعة من اللّوائحِ التّنظيميّة كأدلّة عملٍ ومعاييرَ وغيرها من الوثائق اللّازمة للمساعدة على تنفيذ هذه السّياسةِ.

٢-٢ الغاية

تأمين مرجعية وطنيّة لسياسات أمن المعلومات لدى الجهات الحكوميّة، بما يضمنُ حماية المعلومات والبيانات (المُخزّنة أو المنقولة) والخدمات الإلكترونيّة، بحيث تشملُ البرمجيّات والتّجهيزات وشبكات الاتّصال والأفراد وأماكن تواجدها، والّتي تمَّ تضمينها في أربعةَ عشْرَ مجالاً:

١. سياسات أمن المعلومات.
٢. تنظيم أمن المعلومات.
٣. أمن الموارد البشريّة.
٤. أمن المتعاقدين.

هاتف: ٣٩٣٧٠٣٢ ١١ ٩٦٣+، فاكس: ٣٩٣٧٠٧٩ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

٥. التّوعية والتّأهيل.

٦. إدارة الأصول المعلوماتيّة.

٧. الأمن الفيزيائيُّ والبيئة المحيطة.

٨. إدارة وسائل النّفاذ.

٩. تصميم وتطوير واختبار منظومات المعلوماتيّة.

١٠. التّشفير.

١١. أمن عمليّات التّشغيل.

١٢. إدارة الحوادث الأمنيّة.

١٣. إدارة استمراريّة العمل.

١٤. الامتثال.

٢-٣ مجال تطبيق السّياسة

تُعد هذه السّياسة المرجع الأساسيَّ لجميع الجهات الحكوميّة في الجمهوريّة العربيّة السوريّة فيما يخصُّ أمن المعلومات.

تقوم الجهات الحكوميّة بدعم وتخصيص فريق أمن معلومات ضمن الجهة للقيام بالمهام اللّازمة لضمان أمن المعلومات فيها.

٢-٤ المراجع والسّلطات

أ. المراجع الرئيسيّة المعتمدة عند وضع هذه السّياسة:

١. قانون التّوقيع الالكتروني وخدمات الشّبكة رقم ٤ للعام ٢٠٠٩.

٢. قانون تنظيم التّواصل على الشّبكة ومكافحة الجريمة المعلوماتيّة للعام ٢٠١٢.

٣. تم وضع هذه السّياسة وفق المعايير العالميّة لأمن المعلومات، ومنها: ISO27001:2013, COBiT 5, NIST SP 800-53 Rev. 4, ISA 62443.

هاتف:٣٢ ٣٩٣٧٠ ١١ ٩٦٣+، فاكس: ٧٩ ٣٩٣٧٠ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

ب. يعتبر مركز أمن المعلومات في الهيئة الوطنيّة لخدمات الشّبكة الجهة المعنيّة بوضع وتطوير ومتابعة حسن تنفيذ هذه السّياسة وما يليها من لوائحَ ومعايير وتعليمات وغير ذلك من الوثائقِ المعنيّة بأمن المعلومات.

٢-٥ متطلّبات أمن المعلومات

إنَّ تحديد متطلّبات أمن المعلومات في الجهات الحكوميّة يختلفُ باختلاف أهميّة تلك المعلومات والبيانات والخدمات الإلكترونيّة المُعتمدَة، ويجري تحديد هذه المتطلّبات في الجهات الحكوميّة اعتماداً على ثلاثة مصادر أساسية:

أ. تقييم المخاطر الّتي قد تهدّد الجهة الحكوميّة، مع الأخذ بعين الاعتبار أهداف الجهة الحكوميّة والخدمات الّتي تقدّمُها ومدى الضّرر الحاصل من هذه المخاطر.

ب. القوانين والأنظمة والتّعليمات وغيرها ممّا يتعلّقُ بعمل الجهة الحكوميّة، أو المُتعلّقة بالخدمات الإلكترونيّة (كقانونِ التّوقيع الإلكتروني وخدمات الشّبكة وغيره).

ت. متطلّبات نجاح الجهة الحكوميّة في تحقيق أهدافها وتنفيذ مهامها.

٢-٦ خطّة إدارة أمن المعلومات

لإعداد وتحديث خطة إدارة أمن المعلومات في الجهات الحكومية يجب أن تكون هذه الخطة موثقة وتتضمّن الإجراءات والتّعليمات والسّياسات الدّاخليّة الواجب تنفيذها من قبلِ العاملين والمتعهّدين لديها، ويجب أن تحظىْ هذه الخطّة بدعم الإدارة وتتوافق مع السّياسة والمعايير والتّعليمات الوطنيّة لأمن المعلومات.

هاتف:٣٢ ٣٩٣٧٠ ١١ ٩٦٣+، فاكس: ٧٩ ٣٩٣٧٠ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

٢-٧ تقييم ومعالجة المخاطر

لتقييم وإدارة المخاطر المتعلّقة بأمن المعلومات في الجهات الحكومية، يجب تحديد وتقييم المخاطر الّتي قد تواجهها تلك الجهات، وتحليلها والتّعامل معها وتحديد الأكثر خطورة منها على أمن المعلومات، ووضع الحلول المناسبة لها، وذلك بما يتوافقُ مع أهميّة تلك المعلومات والبيانات واستمراريّة الخدمات، بحيث تكون هذه الحلول متوافقة مع سياسة ومعايير أمن المعلومات الوطنيّة.

هاتف:٣٩٣٧٠٣٢ ١١ ٩٦٣+، فاكس: ٣٩٣٧٠٧٩ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

الفصل الثّالث: مجالات أمن المعلومات

لضمان حماية المعلومات الحكوميّة بطريقةٍ تتناسب مع قيمة تلك المعلومات وحجم الضّرر النّاجم عن فقدانها أو إساءة الاستخدام أو السّرقة أو التّعديل بطرقٍ غير قانونيّة، لا بدَّ من وجود خطّة شاملة وواضحة لحماية أصول المعلومات الحكوميّة، بما يضمنُ استخدامها وتخزينها ونقلها وإدارتها بطريقة فعّالة تتوافق مع هذه السّياسة، بحيث تتضمّن الخطّة عدّة مجالاتٍ وفق التّالي:

٣-١ سياسات أمن المعلومات:

يجب أن تتضمن خطة إدارة أمن المعلومات لدى الجهات الحكومية تعريفاً لمجموعة من سياسات أمن المعلومات وذلك وفق متطلّبات أمن المعلومات الواردة في البند (٢-٥)، وفي هذه الحالة يجب أن تصادقَ الإدارة على هذه اللّوائح وتضمن نشرها لجميع المعنيين بتنفيذها، ويجب أن تتضمّن كل سياسة البنود التّالية:

أ. تعريف السّياسة والغرض منها وأهدافها.

ب. تحديد الجهات أو الأفراد الملتزمين بتنفيذِ هذه السّياسة.

ت. تحديد المسؤولين عن الإشراف على تنفيذ السّياسةِ والرّقابة على الالتزام بها.

ث. إجراءاتٌ واضحةٌ لحالات عدم الامتثال للسياسة.

فيما يلي على سبيل المثال لا الحصر بعض لوائح سياسات أمن المعلومات الّتي يجب أن تُعرف وتُوثّق وتُطوّر بشكلٍ مستمرٍ:

- إدارة التّحكم بالنّفاذ (الوصول واستخدام الأصول المعلوماتيّة).
- تصنيف المعلومات واستخدامها.
- الأمن الفيزيائيُّ وأمن البيئة المُحيطة بالأصولِ المعلوماتيّة.

هاتف:٣٢٠٣٧٣٧٠٣٢ ١١ ٩٦٣+، فاكس: ٣٧٠٧٩ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

- سياسات المستخدم (تعليمات استخدام الأصول المعلوماتيّة).
- سياسة النّسخ الاحتياطيِّ.
- سياسة أمن الشّبكات.
- سياسة الحماية من البرامج الخبيثة.
- سياسة التّعامل مع الجهات الخارجيّة (متعهدين وغيرهم).
- سياسة استخدام التّشفير.
- سياسة التّعامل مع شبكة الانترنت وشبكات التّواصل الاجتماعيّة.

٣-٢ تنظيم أمن المعلومات:

لتنفيذ خطّة أمن المعلومات، يجب أن تقوم الجهات الحكومية بوضع إطار عملٍ لإطلاق الخطة والتّحكم بآليات التنفيذ، وذلك من خلال فريقٍ مُتخصّصٍ وبصلاحيّات مُعرّفةٍ وواضحةٍ ومددٍ زمنيّةٍ مُحدّدةٍ وتطويرها بشكلٍ مستمرٍ بما يشملُ:

أ. تحديد فريق العمل المسؤول عن تنفيذ السّياسة (أو مجموعة السياسات) وإعداد تقارير عن حسن الالتزام للإدارة العليا، مع المدد الزمنيّة للتّنفيذ.

ب. تحديد الجهات الدّاخليّة (مديريّات أو دوائر أو أقسام أو غيرها)، أو الجهات الخارجيّة (متعهدين أو غيرهم) الملتزمين بتنفيذ السّياسة.

ت. توضيح المهام والأدوار بين الأقسام الإدارية الدّاخليّة بحيث لا تتعارض أو تتقاطع مهامها وبما يضمنُ تحديد الجهة المسؤولة عن عدم تنفيذ السّياسة أو عندَ حدوث مشكلةٍ ما.

هاتف:٣٢٠٣٧٣٧٠٣٢ ١١ ٩٦٣+، فاكس: ٣٢٠٣٧٣٧٠٧٩ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

ث. تحديد آليّةٍ واضحةٍ لإبلاغ المعنيين داخل أو خارج الجهة الحكومية عند حدوث أيِّ طارئٍ يتعلّق بأمن المعلومات، كحدوث هجومٍ إلكترونيٍّ على الموقع الإلكترونيِّ أو فقدانٍ للخدمات أو المعلومات.

٣-٣ أمن الموارد البشريّة:

يجب أن تضمنَ خطّة أمن المعلومات والسّياسات المعرّفة ضمنها ما يلي:

أ. تقيّد جميع الموظّفين والمتعهّدين بتطبيق السّياسات والتّعليمات الواردة في خطّة أمن المعلومات.

ب. تعريف واضح للواجبات والمسؤوليات وتطبيق الفصل بينها، بما يتلاءم مع مجال تنظيم أمن المعلومات (الفقرة ٣-٢، البند ت).

ت. التّأكد من حصول الموظفين على المعلومات اللّازمة والوعي والتّدريب بما يضمنُ توفّر المهارات والكفاءات الضروريّة لحماية المعلومات الحكوميّة على نحو يتلاءم مع تصنيفها من حيث الأهميّة والخطورة.

ث. وضع عقوبات إداريّة رادعة للموظفين أو المتعهّدين المخالفين لخطّة أمن المعلومات.

ج. التّأكد من مدى تأثير الإجراءات الإدارية الخاّصة بالعاملين (نقل، تقاعد، فصل...) على إدارة الأصول المعلوماتيّة واستمراريّة العمل.

٣-٤ أمن المتعاقدين (الجهات الخارجيّة):

أ. يجب أن تتضمّن خطّة أمن المعلومات ضمان حماية الأصول المعلوماتيّة الّتي تسمح للجهات الخارجيّة النّفاذ إليها أو تعديلها أو تطويرها أو نقلها بموجب العقود المبرمة لهذه الغاية.

هاتف:٣٢٠٣٧٣٧٠٣٢ ٩٦٣+، فاكس: ٣٢٠٣٧٣٧٠٧٩ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

ب. يجب أن تتضمّن العقود الّتي تتعلّق بشكلٍ مباشرٍ أو غير مباشرٍ بالأصول المعلوماتيّة:

- إلزام الجهة الخارجيّة تقديم شرحٍ موثّقٍ لآليات العمل والمراحل المتعلّقة بإحداث تغيراتٍ على الأصول المعلوماتيّة، مما يتيحُ للجهة الحكوميّة توثيق المراحل الّتي تمر بها هذه الأصول ومعالجة الصّعوبات الطّارئة بسرعةٍ وفعاليّةٍ.
- تقديم كافة الوثائق المتعلّقة بآليات التّركيب والتّنصيب والتّشغيل والصيانة والنّسخ الاحتياطيِّ والحماية لمواد العقد.
- تعهّد الجهة الخارجيّة بالالتزام بسياسات أمن المعلومات الخاصة بالمتعاقدين المعتمدة من الجهة الحكوميّة.
- اقتراح أيّة منظومات خاصة بحماية وأمن المعلومات لمخرجات العقد، مع بيان السبب ومدى الحاجة إليها.

٣-٥ التّوعية والتّأهيل:

يجب أن تتضمّنَ خطّة أمن المعلومات آلياتٍ واضحةٍ لنشر الوعي وتقديم التّدريب اللازم لمُستخدمي أصول المعلومات في الجهة، بما يتلاءم مع الأدوار والمسؤوليّات، وعليها ضمان نشر مزايا الالتزام بخطّة أمن المعلومات المطبّقة لديها، وذلك بهدف بناء الوعي بأهداف وإجراءات أمن المعلومات والتّفاعل معها.

٣-٦ إدارة الأصول المعلوماتيّة:

تعتبر البيانات والمعلومات والبنية التحتيّة والبيئة المحيطة (من تجهيزات أو برمجيات أو خدمات أو مستخدمين أو مرافق أو غير ذلك مما يؤثّر على أمن المعلومات) الأصول المعلوماتيّة الّتي يجب تحديدها وإدارتها كما يلي:

أ. تحديد الأصول المعلوماتيّة والمكلفين بحماية كلِّ أصلٍ معلوماتيٍّ:

هاتف:٣٢ ٣٩٣٧٠ ١١ ٩٦٣+، فاكس: ٧٩ ٣٩٣٧٠ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

- جرد الأصول :يجب تحديد الأصول وجردها وتوثيق ذلك ضمن جداولَ وتحديثها لتتضمّنَ أهمَّ المعلومات عنها.
- يجب أن تتضمّن جداول الأصول الأفراد أو الجهات (مديريّة أو دائرة أو قسم أو غيرها) المسؤولة عن الأصول المعلوماتيّة.
- يجب تعريف وتوثيق قواعد الاستخدام الآمن للأصول المعلوماتيّة.
- ضمان إعادة الأصول إلى أماكنِها الأصليّة بعد استخدامها.

ب. تصنيف المعلومات بحسب أهميتها ممّا يسهّلُ وضع آليّات حمايتها.

ت. وضع آليّات وإجراءات التّخزين والنّقل والإتلاف الآمن للأصول بحسب تصنيفها.

٣-٧ الأمن الفيزيائي والبيئة المحيطة:

يجب تأمين البيئة الفيزيائيّة المحيطة بالأصول المعلوماتيّة بما يضمنُ الاستخدام الآمن والأمثل لهذه الأصول، بما يشملُ:

أ. حماية المرافق المستخدمة في معالجة وحفظ المعلومات من الاختراق والكوارث الطبيعيّة أو الصناعيّة أو الدخول غير المُصرّحِ به، وذلك بما يتناسب مع أهميّة تلك المعلومات وحساسيتها.

ب. حماية كافّة التّجهيزات ووسائط حفظ المعلومات من التّهديدات الماديّة كالتّلف أو السّرقة أو غيرها.

٣-٨ إدارة وسائل النّفاذ:

يجب أن تضمن خطّة أمن المعلومات ما يلي:

هاتف:٣٢ ٣٩٣٧٠ ١١ ٩٦٣+، فاكس: ٧٩ ٣٩٣٧٠ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

أ. آليّات واضحة للتحكم في النّفاذ إلى منظومات المعلومات وأصول المعلومات.

ب. التّحقق من هويّة المُصرَّح لهم بالنّفاذ إلى منظومات المعلومات أو المرافق المستخدمة في معالجة المعلومات بما يتوافقُ مع متطلّبات العمل.

ت. المراجعة الدّوريّة لملفات النّفاذ إلى منظومات المعلومات والمرافق وإلغاء الصّلاحيات الّتي لم تعدْ لازمةً لمتطلّبات العمل، مع ضرورة إبلاغ المستخدمين بالتزاماتهم ومسؤولياتهم اتّجاه أمن المعلومات.

ث. التّأكد من وضع وتنفيذ سياسة تتعلّق بالنّفاذ لمعلومات وخدمات الجهة من خارج أماكن العمل الرسميّة.

ج. التّأكد من وضع وتنفيذ سياسة تتعلّق بالنّفاذ من خلال الأجهزة الإلكترونيّة المحمولة (حاسب محمول، هواتف ذكية، وغيرها).

٣-٩ تصميم وتطوير واختبار المنظومات المعلوماتيّة:

يجبُ ضمان أنّ أيَّ تصميمٍ أو تطويرٍ أو تطبيقٍ أو اختبارٍ لمنظومات المعلومات يتلائمُ مع متطلّبات أمن المعلومات وخطّة أمن المعلومات.

٣-١٠ التّشفير:

في حال تبادل المعلومات الحساسة عبر الشبكات يجب أن تُعتمد تقنيات التّشفير وذلك لضمانِ سريّة وسلامة ومصداقيّة هذه المعلومات وذلك باستخدام تقنيات التّوقيع الرّقمي، وفي هذه الحالة يجبُ استخدام شهادات التّصديق الالكتروني الصّادرة عن الهيئة الوطنيّة لخدمات الشّبكة.

٣-١١ أمن عمليّات التّشغيل:

يجب أن تضمن خطّة أمن المعلومات، إجراءات واضحة لإدارة المنظومات في مرحلة التّشغيل، بحيث تحقّقُ ما يلي:

هاتف:٣٢٠٣٧٣٧٠٣٢ ١١ ٩٦٣+، فاكس: ٣٢٠٣٧٣٧٠٧٩ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

أ. وجود تعليمات وإجراءات واضحة وموثّقة لمستخدمي المنظومات المعلوماتيّة خلال مرحلة التّشغيل.

ب. المراقبة الدّوريّة للمنظومات المعلوماتيّة لضمان وجود الحدِّ الأدنى لمستوى أمن المعلومات المُتفق عليه في الجهة لتحقيق الأداء المطلوب والامتثال للمعايير الأمنيّة.

ت. مسك السّجلات اللّازمة لتسجيلِ وتوثيقِ كافّةِ التّغيرات والأعطال الّتي تطرأُ على منظومات المعلومات أثناء التّشغيل لاستخدامها في المستقبل.

ث. إجراء عمليات النسخ الاحتياطي بشكلٍ دوريٍّ على وسائطَ يتمُّ حفظها بشكلٍ آمن، بما يضمن استعادة المعلومات والخدمات وفق الحاجة.

٣-١٢ إدارة الحوادث الأمنيّة:

يجب أن تضمنَ خطّة أمن المعلومات إجراءاتٍ واضحةً لإدارة الحوادث المرتبطة بأمن المعلومات ومعالجتها بطريقة فعّالة وفي الوقت المناسب .ويجب توقّع الحوادث الأمنيّة المُحتملَة والتّخطيط للاستجابة لها وذلك بما يتلائم مع دراسة تقييم المخاطر المُحتملة .ويتعيّن على المعنيين إبلاغ مركز أمن المعلومات في الهيئة الوطنية لخدمات الشبكة عن حوادثَ أمن المعلومات الهامّة (المتعلقة بالهجمات الإلكترونيّة ومحاولات الإختراق) الّتي تتعرّض لها منظوماتهم حتى يتسنّى للمركز تقديم الدّعم الفنّي المُناسب.

٣-١٣ إدارة استمراريّة العمل:

يجبُ إعداد خطّة لإدارة استمراريّة عمل المنظومات المعلوماتيّة بما يتوافقُ مع برنامج إدارة استمراريّة الأعمال في الجهة الحكوميّة في حال وجوده.

ويتعين أن تراعي عمليّة تخطيط استمراريّة عمل منظومات المعلومات تحقيق أهداف النّقطة المستهدفة للاسترجاع والوقت المُستهدَف للاسترجاع وذلك في ظلِّ مجموعة من الظروف التّشغيليّة والاستثنائيّة المُحتملَة.

هاتف:٣٢ ٣٩٣٧٠ ١١ ٩٦٣+، فاكس: ٧٩ ٣٩٣٧٠ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy

٣-١٤ الامتثال:

الالتزام والامتثال للقوانينِ والأنظمةِ النّافذة في الجمهوريّة العربيّة السوريّة عندَ وضع أية خطّة أو سياسة أو مُتطلّبات أو عقود أو غيرها بما يخصُّ أمن المعلومات.

كذلك حماية الوثائق (الورقيّة والإلكترونيّة) الخاصّة بأمن المعلومات وكافّة الأصول المعلوماتيّة والاحتفاظ بها بحسب الحاجة وبما يتوافق مع القوانينِ والأنظمةِ النّافذة.

هاتف:٣٢ ٣٩٣٧٠ ١١ ٩٦٣+، فاكس: ٧٩ ٣٩٣٧٠ ١١ ٩٦٣+، ص.ب: قدسيا-٤٧، بريد إلكتروني: info@nans.gov.sy