وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Q-CERT

سياسات تأمين المعلومات الوطنية

الإرشادات الخاصة بكتيب تأمين المعلومات الوطنية

[IAG-NAT-GFGM]

المؤلف:	وزارة الموصلات والاتصالات بقطر
النسخة:	2,0
التصنيف:	عام
تاريخ الإصدار:	2011-05-01

جدول المحتويات

الفصل "أ"

نظرة عامة

تمثل هذه الوثيقة مجموعة من سياسات تأمين المعلومات الوطنية وقد تم إعدادها بهدف توفير الإرشادات إلى القراء كي يتمكنوا من فهم وتنفيذ كتيب تأمين المعلومات الوطنية.

وتركز الوثيقة على توفير تقييم موضوعي وعرض التوقعات الناجمة عن الضوابط المتعددة المحددة بكتيب تأمين المعلومات الوطنية.

يتم قراءة الوثيقة إلى جانب كتيب تأمين المعلومات الوطنية لتكون بمثابة مرجع ولا يتم قراءتها بصورة مستقلة.

الملكية والمحافظة

تمتلك وزارة المواصلات والاتصالات بقطر هذه الوثيقة. وتتولى الوزارة المسؤولية عن الحفاظ على هذه الوثيقة.

المراجع

[IAP-NAT-INFA] سياسة تأمين المعلومات الوطنية، وزارة المواصلات و الإتصالات بقطر، 2014

[IAP-NAT-DCLS] سياسة تصنيف المعلومات الوطنية، وزارة المواصلات و الإتصالات بقطر، 2014

[IAP-NAT-IAFW] إطار تأمين المعلومات، 2008

[AES] NIST FIPS PUB 197 "مواصفات التشفير المتقدمة" (AES)، نوفمبر 2001

[CC3-1] المعايير العامة لتقييم أمن تكنولوجيا المعلومات (CC)، النسخة رقم 2,0 (2006)

[CWA14167-1] المتطلبات الأمنية للأنظمة الجديرة بالثقة لإدارة شهادات التوقيعات الإلكترونية – الجزء الأول: متطلبات أمن الأنظمة، اتفاقية ورشة عمل CEN، CWA 14167-1، يونيو 2003

[FIP186-2] NIST FIPS PUB 186-2 "مواصفات التوقيع الرقمي (DSS)"، مع إخطار التغيير رقم 1، 1 أكتوبر 2001.

[FIPS-140-2] المعهد القومي للمعايير والتكنولوجيا، FIPS 140-2، المتطلبات الأمنية لوحدات التشفير، 24 يناير 2007

[Mitre] Mitre، 2009 CWE/SANS Top 25 أخطاء البرمجة الأكثر خطورة، http://cwe.mitre.org/top25/، يناير 2009

[RFC 4301] كينت & سيو Kent & Seo، أسلوب بناء الأمن لـIPJ، RFC 4301، ديسمبر 2005

[RFC3851] س. رامسدل/ MIME 3.1 مواصفات الرسالة، RFC 3851، يوليو 2004

[RFC4346] ديركس & ريسكورلا، بروتوكول TLS، RFC 4301، أبريل 2006

[RSA] معامل RSA، " PKCS#1 إصدار 2,1: مواصفات التشفير RSA"، يونيو 2002.

[SFTP] جالبريث & سارينما، بروتوكول نقل الملفات SSH، draft-ietf-secsh-filexfer، يونيو 2005

[SHA] NIST FIPS PUB 180-2، "مواصفات المزج الآمن"، المعهد القومي للمعايير والتكنولوجيا، وزارة التجارة الأمريكية، أغسطس 2001

[SP800-67] NIST SP 800-67 "التوصية الخاصة بلوغاريثم التشفير الثلاثي للبيانات (TDEA)"، مايو 2004

[ISO11770-1] تكنولوجيا المعلومات – تقنيات الأمن، الإدارة الرئيسية، ISO/IEC 11770-1:2006 (E) الجزء رقم 1: الإطار الرئيسي للإدارة، المنظمة الدولية للتوحيد القياسي واللجنة الدولية الكهروتقنية، 2006

[RFC4408] م. ونج، و. شليت، حول إطار سياسة المرسل (SPF) للتفويض باستخدام النطاقات في البريد الإلكتروني، النسخة رقم 1، فريق العمل الهندسي للشبكة الدولية (IETF)، RFC 4408، أبريل 2006.

يتم الإشارة إلى المصطلحات المعرفة بإطار تأمين المعلومات [IAP-NAT-IAFW]. ويتم استخدام المصطلحات المعرفة التالية ضمن هذه الوثيقة: **المؤسسة، المعلومات الشخصية، المواقع الساخنة/ الدافئة/ الباردة، فريق الاستجابة لطوارئ الحاسبات بقطر (Q-CERT)، وزارة المواصلات والاتصالات بقطر (MOTC)، علامات التصنيف القومي.**

الفصل "ب"

1- إرشادات حول هيكل الحوكمة [IG]

1-1 إرشادات حول السياسة والضوابط الرئيسية

IG 1 تعيين شخص يتولى مسؤولية وإدارة برنامج أمن المعلومات. وسوف يتم الإشارة إلى ذلك الشخص باعتباره "مدير أمن المعلومات" في إطار كتيب تأمين المعلومات الوطنية هذا.

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بتعيين مدير لأمن المعلومات يصبح مالكا لجميع البرامج ذات الصلة بأمن المعلومات.

سوف يتولى مدير أمن المعلومات المسؤولية عن وضع الموازنات (المالية والقوى العاملة) لبرنامج أمن المعلومات التابع للمؤسسة. ويضطلع مدير أمن المعلومات أيضا بالمسؤولية عن تخطيط وتنفيذ الأهداف لصالح إدارة أمن المعلومات.

IG 2 تخصيص الموازنة الملائمة للعاملين وإدارة برنامج أمن المعلومات.

ينص كتيب تأمين المعلومات الوطنية على أن تثبت المؤسسة التزامها بأمن المعلومات من خلال ضمان تخصيص الموارد الملائمة، بما في ذلك الموازنة والعاملين، لإدارة برنامج أمن المعلومات.

قد تؤدي ندرة التمويل إلى الحيلولة دون تطبيق الضوابط الأمنية المناسبة أو تنفيذ برامج أمن المعلومات. وفيما يتعلق بالموارد، سوف يخفق أفضل الأنظمة في حالة عدم توافر الموارد الكافية لإدارة عملياته.

IG 3 التأكد من قيام مدير أمن المعلومات بتقديم التقارير إلى إدارة المخاطر أو المراجعة الداخلية بالمؤسسات.

لضمان استقلالية وعدالة ممارسات مدير أمن المعلومات، فإنه من الحكمة أن يتولى تقديم التقارير بصورة مباشرة إلى مدير إدارة المخاطر أو المراجعة الداخلية بالمؤسسات أو إلى رؤساء المؤسسات ذاتهم.

سوف يؤدي قيام مدير أمن المعلومات بتقديم التقارير إلى مدير إدارة تكنولوجيا المعلومات إلى تعارض المسؤوليات والتعرض للمساءلة.

IG 4 ضمان قيام رؤساء المؤسسات بتقديم دعم موثق ومستمر لتطوير وتنفيذ عمليات الأمن والبنية الأساسية لتكنولوجيا المعلومات والاتصالات وصيانتها بصفة دائمة داخل المؤسسة.

يعد البرنامج الذي يحظى بتمويل ضعيف أسوأ من عدم وجود برنامج في الأساس، حيث يبث شعور بالرضا الزائف بين الأطراف الرئيسية.

يتمثل العنصر الرئيسي لنجاح أي من برامج أمن المعلومات في الدعم الدائم الذي يقدمه رؤساء المؤسسات من أجل تحقيق الأهداف المرجوة من خلال توفير الموارد الكافية والتمويل للبرنامج.

IG 5 حيثما يقوم رؤساء المؤسسات بتفويض سلطاتهم لاعتماد التعديلات على متطلبات هذا الكتيب، ينبغي أن يحظى المفوض بسلطات أعلى من سلطات مدير أمن المعلومات.

ينبغي أن يتم اعتماد أي تعديلات أو عدم تطابق مع هذا الكتيب من قبل رؤساء المؤسسات. وفي الحالات التي يستحيل معها القيام بذلك، يجوز أن يقوم رؤساء المؤسسات بتفويض هذه المسؤولية إلى شخص أو مسؤول يحظى بسلطة أعلى من سلطة مدير أمن المعلومات. ويهدف ذلك إلى منع سوء استغلال السلطة.

IG 6 تحديد مسؤوليات أمن المعلومات لمدير أمن المعلومات والإدارة والعاملين بالمؤسسة.

لنشر ثقافة فعالة لإدارة أمن المعلومات، يتحتم غرس مسؤوليات أمن المعلومات والتوعية بها داخل جميع العاملين والمتعاقدين وغيرهم..

ينبغي أن تكفل إدارة الموارد البشرية تعريف مسؤوليات أمن المعلومات ضمن كل توصيف وظيفي. وقد يختلف مستوى المسؤولية وفقا للدور المحدد وأنشطة العمل.

IG 7 ضمان أن يحظى مدير أمن المعلومات بما يلي:

أ. إمكانية الوصول إلى الإدارة التنفيذية والحصول على الدعم الكامل من قبلها.
ب. دراية كافية بأمن المعلومات و/أو أمن تكنولوجيا الاتصالات والمعلومات.
ج. معرفة عامة وخبرة كافية او توفر جميع المصادر الكافية المتعلقة بالأنظمة التي تستخدمها المؤسسة، وخاصة أنظمة التشغيل وأنظمة/ مرافق مراقبة الوصول والتفويض ومرافق المراجعة والتدقيق.
د. قدرة مناسبة لدعم دور مدير أمن المعلومات.

ينص كتيب تأمين المعلومات الوطنية على الحد الأدنى من الشروط الواجب توافرها بالمرشحين المحتملين لضمان أن يحظى مدير أمن المعلومات بالمهارات المناسبة اللازمة للوظيفة.

IG 8 إدراج المسؤوليات التالية ضمن دور مدير أمن المعلومات:

أ. تحديد والتوصية بإدخال تحسينات أمن تكنولوجيا الاتصالات والمعلومات على الأنظمة.
ب. ضمان دراسة جوانب أمن تكنولوجيا الاتصالات والمعلومات كجزء من عملية إدارة التغيير.
ج. ضمان تنسيق عمليات صياغة وصيانة وتنفيذ جميع وثائق أمن تكنولوجيا الاتصالات والمعلومات، بالتعاون مع مديري الوحدات الادارية. ضمان التحقيق وتقديم التقارير حول جميع حوادث أمن تكنولوجيا الاتصالات والمعلومات، بالتعاون مع فريق الاستجابة لطوارئ الحاسبات بقطر.
د. ضمان الإبلاغ في الوقت المناسب والمشاركة الكافية في التحقيق عن الحوادث الأمنية لتكنولوجيا المعلومات والاتصالات مع Q-CERT

IG 9 ضمان أن يتولى مدير أمن المعلومات المسؤولية عن:

أ. ضمان تطوير وحفظ وتحديث وتنفيذ خطط إدارة مخاطر الأمن وخطط أمن الأنظمة وأي إجراءات أمنية أخرى يتم تطبيقها.
ب. تقديم المشورة الأمنية التقنية حول تطوير وحيازة وتنفيذ وتعديل وإدارة ودعم وبناء الأنظمة.
ج. مساعدة مدير النظام في وضع وصياغة معايير وسياسات أمن الأنظمة.
د. اعتماد الأنظمة عند الاقتضاء.
هـ. ضمان أن ينظم الجهاز برنامج توعية وتدريب على أمن تكنولوجيا الاتصالات والمعلومات.
و. المراجعة المنتظمة لأمن الأنظمة وعمليات وسجلات تدقيق الأنظمة وسلامة إعدادات الأنظمة.

تنص الفقرتان IG 8 و IG 9 بكتيب تأمين المعلومات الوطنية على الحد الأدنى من المسؤوليات التي ينبغي أن يكون مدير أمن المعلومات عرضة للمساءلة بشأنها. ويمكن أن تتم إضافة أنشطة محددة وفقا لمتطلبات العمل بالمؤسسة.

IG 10 ضمان أن يكون مدير أمن المعلومات على دراية بجميع إجراءات التشغيل الأمنية ذات الصلة بالأنظمة، بما في ذلك الإجراءات المتعلقة بأدوار مديري وإداريي ومستخدمي الأنظمة.

يؤكد كتيب تأمين المعلومات الوطنية، بصفة محددة، على ضرورة أن يحظى مدير أمن المعلومات بمعرفة عملية حول الإجراءات الأمنية الخاصة بالأنظمة وأنشطة العمل. وسوف تمنح تلك المعرفة مدير أمن المعلومات فهما أفضل للنظام وتأثيره على العمليات والأنشطة. وسوف تساعد المعلومات أيضا في تحديد المسؤوليات الأمنية للأدوار المتعددة ذات الصلة باستخدام الأنظمة. وتصبح المراجعات المنتظمة لإجراءات التشغيل الأمنية جزءا من نظام إدارة أمن المعلومات.

2 - إرشادات حول إدارة المخاطر [RM]

2-1 إرشادات حول السياسة والضوابط الرئيسية

RM 1 تحديد إجراءات تنفيذ عملية تقييم مخاطرونقاط ضعف الأصول المعلوماتية الهامة (التي تم تحديدها في مستوى أمني متوسط أو مرتفع).

لا يوصي كتيب تأمين المعلومات الوطنية بأن تقر المؤسسة منهجية محددة لتقييم المخاطر ونقاط الضعف من أجل إدارة المخاطر.

هناك عدد من أطر ومعايير تقييم المخاطر ونقاط الضعف المتاحة من خلال المنظمة الدولية لتوحيد المقاييس (ISO 27005) وCobit والمواصفات الحكومية المتعددة مثل AS/NZS 4360:1999.

ينبغي أن تحدد الإجراءات مدى "تقبل المخاطر" لدى المؤسسة. ويحدد تقبل المخاطر، من حيث الجوهر، الحد الأدنى للمخاطر التي يمكن أن تتقبلها المؤسسة.

يمكن، على سبيل المثال، أن تحدد المؤسسة مستويات المخاطر باعتبارها منخفضة ومتوسطة ومرتفعة للغاية. وقد تحدد أيضا أن المخاطر عند المستوى "المنخفض" تكون مقبولة ولا يوجد ضرورة لاتخاذ إجراء بشأن التخفيف من حدتها.

ومن المتوقع أن يوفر التدريب للمؤسسة معارف ومدركات كافية من أجل:

- التأكد من المخاطر ونقاط الضعف الحقيقية التي تواجه النظام
- تحديد أولويات الموارد المتاحة لتنفيذ البنية التحتية الآمنة

RM 2 تحديد الضوابط الملائمة للتخفيف من حدة المخاطرونقاط الضعف المحددة، بناءً على عملية التقييم.

لا يوصي كتيب تأمين المعلومات الوطنية بأي إستراتيجية أو ضوابط أمنية محددة من أجل التخفيف من حدة المخاطر، بخلاف تحديد الضوابط الرئيسية. وقد تكون الضوابط التي تختارها المؤسسة تقنية أو إدارية وقد تؤكد على إحدى الاستراتيجيات التالية:

تجنب المخاطر: نتيجة للطبيعة المتأصلة للمخاطر، قد يكون من الحكمة تجنب "المخاطر" تماما. وعلى سبيل المثال، تعديل أو إنهاء العملية التي تشجع تلك المخاطر.

نقل وتحويل المخاطر: قد يوصى في بعض الحالات بتحويل المخاطر إلى كيان آخر. وعلى سبيل المثال، يتم مواجهة بعض مخاطر التشغيل عن طريق التعهيد. وقد يكون المثال الآخر عن طريق توفير تغطية تأمينية للتخفيف من حدة الخسائر المالية. ومع ذلك، تظل المجالات أو الخدمات التي يتم تعهيدها تتمثل في الحوكمة والالتزام ومسؤولية المؤسسة عن إدارة

المخاطر. يرجى النظر إلى TM1 بإدارة أمن الأطراف الأخرى للتعرف على المزيد من المعلومات حول الضوابط ذات الصلة بالتعهيد.

التخفيف من حدة المخاطر: قد يكون من المستحيل في معظم الأوقات تجنب أو تحويل المخاطر؛ وقد يكون هناك سيناريوهات تحتاج إلى إدارة العمليات الحرجة رغم المخاطر المرتبطة بها. ومن الضروري في تلك السيناريوهات الحد من المخاطر إلى مستوى مقبول. ويتضمن ذلك تطبيق ضوابط محددة للحد من العواقب (التأثير) أو من احتمالية وقوع المخاطر. وعلى سبيل المثال، يمكن أن يؤدي تركيب نظام إنذار فعال للكشف عن الحرائق، بالإضافة إلى نظام إخماد الحرائق، إلى الحد بفاعلية من العواقب ومن احتمالية نشوب الحرائق.

قبول المخاطر: تتمثل إحدى قواعد تصميم وتنفيذ الضوابط من أجل التخفيف من حدة المخاطر في ضمان ألا تتجاوز تكلفة التخفيف من حدة المخاطر تكلفة الأصول المعلوماتية و/أو الخدمات التي يتم تقديمها (إذا وضعنا الالتزامات القانونية والتعاقدية في الاعتبار). وقد لا تنخفض حدة المخاطر إلى المعدلات المقبولة (تقبل المخاطر) حتى بعد تطبيق الضوابط؛ وفي تلك الحالات، ينبغي أن تقرر السلطات المعنية بالمؤسسة ما إذا كانت مستعدة لقبول المخاطر.

RM 3 ضمان الفحص الدقيق للضوابط المختارة للأصول المعلوماتية المصنفة بمستوى أمني مرتفع، من قبل الإدارة العليا للمؤسسة.

يضمن كتيب تأمين المعلومات الوطنية اختيار الضوابط الفعالة أثناء فحص الأصول الهامة. وسوف تكفل السياسة أن تشارك الإدارة العليا للمؤسسة بفاعلية في عملية صنع القرارات ذات الصلة بأمن البنية الأساسية الحرجة.

تتضمن الإدارة العليا رئيس المؤسسة ومدير إدارة المراجعة الداخلية.

RM 4 ضمان المتابعة المنتظمة لفاعلية الضوابط المختارة بالفقرتين RM 1 وRM 2 .

ينص كتيب تأمين المعلومات الوطنية على وجود إجراءات فعالة لضمان فاعلية الضوابط التي يتم تنفيذها. ويتم متابعة الضوابط المنفذة لضمان تحقيق المستوى المرجو للتخفيف من حدة المخاطر.

يتغير سيناريو المخاطر وكذلك نقاط الضعف ذات الصلة؛ وينبغي أن تكفل العملية الحفاظ على دائرة مغلقة وتقييم أي تعديلات وتأثيرها على البنية الأساسية ودراستها بفاعلية. وتضمن العملية أن تظل الضوابط المنفذة ذات فاعلية في السيناريوهات المتغيرة وأن تتمكن من مواجهة التحديات الجديدة.

RM 5 ينبغي إدماج عمليات تقييم المخاطر في العمليات التجارية والمنقحة كلما كان هناك تغيير، او عند حدوث تغييرات مؤثرة في بيئة العمل قد تدعو إلى الحاجة بإجراء عملية تقييم البيانات..

يجب إدماج إدارة المخاطر في جميع العمليات بالمؤسسة. قد تغير بيئة العمل أيضا مخاطر المنظمة ولذا يجب مراعاتها في عملية تقييم المخاطر. كلما يتم تغيير عملية، ينبغي أن يتم إجراء تقييم للمخاطر لضمان أن التغييرات تتماشى مع قابلية المخاطرة للمنظمة أو يتم اتخاذ إجراءات تصحيحية للقيام بالمطلوب. وينطبق الشيء نفسه على أي تغييرات في بيئة الأعمال مثل التغييرات القانونية / التنظيمية، وفتح قنوات جديدة للتسليم (الأعمال عبر الإنترنت).

3 - إرشادات حول إدارة أمن الأطراف الأخرى [TM]

3-1 إرشادات حول السياسة والضوابط الرئيسية

TM 1 أن تظل المجالات أو الخدمات التي تم تعهيدها تتمثل في مسؤولية المؤسسةعن الحوكمة والالتزام وإدارة المخاطر.

ينص كتيب تأمين المعلومات الوطنية على أنه في حالة قيام المؤسسة بتعهيد بعض العمليات، فهي لا تنقل المسؤوليات الخاصة بالعملية إلى الأطراف الخارجية. وتتولى المؤسسة المسؤولية عن حوكمة والتزام وإدارة مخاطر العمليات التي يتم تعهيدها. وتكفل المؤسسة دعم جميع العمليات التي يتم تعهيدها من قبل اتفاقيات مستوى الخدمات المناسبة.

تحظى جميع اتفاقيات مستوى الخدمات بمؤشرات أداء رئيسية محددة، تتضمن على سبيل المثال لا الحصر سرية وسلامة وإتاحة العملية. وتكون إدارة الأمن متأصلة في العقد الذي يتم تعهيده.

ينبغي أن تبرم الأجهزة بعض الاتفاقيات المحددة التي يتم تخصيصها، على سبيل المثال، للوصول إلى الموارد الداخلية من خلال الأطراف الأخرى، مثل اتفاقية الاتصال بأي طرف آخر، والتي سوف تتضمن إشارات إلى السياسات الداخلية المعنية باستخدام موارد النظام والشبكة ومسؤوليات ومواصفات الأطراف المشاركة.

TM 2 أن تتفهم وتقر المخاطر المتعلقة بتعهيد خدماتها.

ينص كتيب تأمين المعلومات الوطنية على إجراء عملية تقييم المخاطر بأسلوب سليم والمقارنة بين جميع المزايا والعيوب قبل تعهيد الخدمات. ويتضمن ذلك تقييم عملية تقييم مخاطر أمن المعلومات. ويتم التخفيف من حدة جميع المخاطر المحددة بهذا التدريب وإقرار المخاطر المتبقية من قبل الإدارة العليا. على المؤسسة والاطراف الخارجية ان تقوم بإنشاء و تطوير جداول و رسوم RACI البيانية التي تقوم بتوضيح الاعتمادية و المسؤولية لتقديم ضوابط فعالة.

TM 3 أن يتم إدراج الضوابط الأمنية والسياسة الرئيسية المحددة بكتيب تأمين المعلومات الوطنية ضمن اتفاقيات أوعقود تقديم الخدمة المبرمة مع أي طرف آخر. ويسري ذلك أيضا على المتعاقدين من الباطن لدى الطرف الآخر.

ينص كتيب تأمين المعلومات الوطنية على أن يحظى المتعاقد مع الطرف الآخر أو مقدم الخدمة بإمكانية الوصول إلى سياسة تصنيف المعلومات الوطنية وكتيب تأمين المعلومات الوطنية. وسوف يكفل ذلك أن يكون ضليعا في السياسة ومتطلباتها ويضمن تحقيق المزيد من الالتزام بالسياسات.

TM 4 أن يتعهد الطرف الآخركتابياً بتقديم تقارير منتظمة حول الوضع الأمني للخدمة (الخدمات) الأمنية، بما في ذلك أي حوادث.

ينص كتيب تأمين المعلومات الوطنية على وجود آلية لضمان استمرار التواصل بين المؤسسة ومقدم الخدمة لدى الطرف الآخر. وتتضمن التقارير التي يقدمها مقدم الخدمة لدى الطرف الآخر أحدث الحوادث الأمنية ووضع البنية الأساسية الأمنية. ويستوعب مقدم الخدمة لدى الطرف الآخر العمليات التي ينص عليها كتيب تأمين المعلومات الوطنية، والتي تتضمن، على سبيل المثال لا الحصر، إدارة التغيير. ويتم إبلاغ جميع التعديلات ذات الصلة بالعملية التي يتم تعهيدها إلى المؤسسة واعتمادها من قبلها.

TM 5 أن يتم متابعة ومراجعة الخدمات والتقارير والسجلات التي يوفرها الطرف الآخر بصورة منتظمة، وأن يتم إجراء عمليات المراجعة والتدقيق بصورة منتظمة.

ينص كتيب تأمين المعلومات الوطنية على استخدام العناية الواجبة في متابعة الخدمات التي يتم تعهيدها إلى مقدم الخدمة لدى الطرف الآخر. وينبغي إجراء عمليات مراجعة وتدقيق منتظمة لضمان الالتزام باتفاقيات مستوى الخدمات والعقد. ويجب أيضا إجراء عمليات التدقيق على أمن، واستمرارية الأعمال، وإدارة المخاطر وأمثلية الاطرف الثالثة، ويعتمد عمق التدقيق على المخاطر التي يمكن ان يشكلها الطرف الثالث.

4 - إرشادات حول وضع البطاقات التعريفية للبيانات [DL]

4-1 إرشادات حول السياسة والضوابط الرئيسية

DL 1 أن تقوم المؤسسة بدور سلطة وضع البطاقات التعريفية للبيانات والمعلومات التي تجمعها أو تحتفظ بها.

ينص كتيب تأمين المعلومات الوطنية على أن تكون المؤسسة هي هيئة وضع البطاقات التعريفية للبيانات والمعلومات التي تجمعها وتحتفظ بها. ويعني ذلك أن يحظى المرشحون المحددون أو القائمون على إدارة الأعمال داخل المؤسسة المسؤولية عن تحديد وتصنيف المعلومات التي تجمعها أو تحتفظ بها.

DL 2 أن تصنف جميع الأصول المعلوماتية وفقا لسياسة تصنيف المعلومات الوطنية [IAP-NAT-DCLS]. ويتم وضع علامة البيانات الملائمة "داخلي" أو "تداول محدود" أو "مقيد" على التوالي على جميع الأصول المصنفة وفقا لتصنيف السرية C1 أو C2 أو C3.

ينص كتيب تأمين المعلومات الوطنية على أن تكفل المؤسسات تصنيف جميع المعلومات. ويتضمن ذلك المعلومات بجميع أنماطها، أي الرقمية والورقية والمسموعة والمرئية وغير ذلك.

يستند التصنيف على سياسة تصنيف المعلومات الوطنية. ويتم وضع العلامات الملائمة لتعريف جميع المعلومات المصنفة. ويتم أيضا وضع العلامات الملائمة على البيانات الرقمية؛ وتكفل الأجهزة الوطنية أن ينطوي النظام على الضوابط الملائمة لضمان أن يتماشى نشر المعلومات مع تصنيفات المعلومات C-I-A.

DL 3 أن تتولى تصنيف الأصول المعلوماتية الوطنية، بصورة افتراضية، باعتبارها أصول "داخلية"، ما لم تكن أصولا متاحة للعامة أو للاستهلاك.

ينص كتيب تأمين المعلومات الوطنية على توفير الحد الأدنى للحماية الأساسية لجميع الأصول المعلوماتية من أجل التخفيف من حدة المخاطر ذات الصلة بالرقابة على تصنيف الوثيقة. وقد يكون هناك حالات لا يتم بها وضع البطاقات التعريفية على الوثيقة، نظرا لكونها لا تزال في مرحلة المسودة أو لعدم الانتهاء منها بعد أو ربما تكون البطاقة التعريفية قد تعرضت للتلف أو العبث؛ وفي كل تلك الحالات، سوف تضمن الضوابط أعلاه أن تحظى جميع الأصول المعلوماتية، التي لم يتم وضع العلامات عليها أو تصنيفها، بتصنيف افتراضي C1، أي داخلي.

DL 4 أن تقر نظام وضع البطاقات التعريفية للبيانات من أجل دعم شرط "الحاجة إلى المعرفة"، حتى يتم حماية المعلومات من الإفصاح أو الاستخدام غير المصرح به.

يهدف كتيب تأمين المعلومات الوطنية إلى التأكيد على أن نظام وضع البطاقات التعريفية للبيانات يكمل شرط "الحاجة إلى المعرفة". وسوف يكفل تصنيف ووضع البطاقات التعريفية للمعلومات تبسيط عملية تحديد ومنح الحق في تداول المعلومات.

DL 5 أن تتولى تعليم وتوعية العاملين والموظفين والمتعاقدين بنظام وضع البطاقات التعريفية للبيانات.

ينص كتيب تأمين المعلومات الوطنية على أن يكون العاملون والجمهور المستهدف على دراية ووعي بمفهوم وضع البطاقات التعريفية للبيانات وآثاره على أمن المعلومات.

5 - إرشادات حول إدارة التغيير [CM]

5-1 إرشادات حول السياسة والضوابط الرئيسية

CM 1 تحديد والالتزام بعملية إدارة التغيير الموثقة التي تتضمن فئات التغيير التالية أو المماثلة:

أ- التغيير الرئيسي المخطط له. وتتضمن أمثلة التغيير الرئيسي المخطط له ما يلي:

- التغيير الذي يؤدي إلى توقف العمل أثناء ساعات العمل الرسمية
- التغيير الذي يؤدي إلى تغيير في ممارسات العمل أو التشغيل
- التغيير في أي نظام يؤثر على استعادة القدرة على العمل بعد الكوارث واستمرارية تصريف الأعمال
- استحداث أو قطع خدمة تكنولوجيا المعلومات

ب- الصيانة والتغييرات الصغرى. وتتضمن أمثلة هذا النمط من التغيير ما يلي:

- التغييرات/ التعديلات الأمنية على مستوى التطبيقات
- تعديلات نظام التشغيل (الهامة، الإصلاحات العاجلة، حزم الخدمات)
- الصيانة الدورية المنتظمة
- التغييرات التي من غير المحتمل أن تسبب انقطاع في الخدمة

ج. التغيير في حالات الطوارئ أو انقطاع الخدمات غير المخطط لها. وتتضمن أمثلة هذا النمط من التغيير ما يلي:

- تدهور شديد في الخدمة يتطلب اتخاذ إجراء فوري
- إخفاق النظام/ التطبيق/ المكون بما يؤدي إلى إحداث تأثير سلبي على أنشطة العمليات
- استجابة لأي كارثة طبيعية
- استجابة لاحتياجات حالات الطوارئ
- التغيير بناءً على طلب العاملين المسؤولين عن مواجهة والتصدي لحالات الطوارئ

ينص كتيب تأمين المعلومات الوطنية على وجود إجراءات محددة لإدارة التغيير داخل المؤسسة. ويهدف ذلك إلى ضمان توثيق ومداولة جميع التغييرات حول النطاق والآثار والمزايا والعيوب في إطار نشاط المؤسسة. وتكفل عملية إدارة التغيير أن تكون الإدارة والجمهور على دراية بالتغييرات الوشيكة وآثارها على أسلوب العمل. وينبغي أن يتم الاحتفاظ بسجلات إدارة التغيير في قاعدة البيانات الخاصة بإدارة التغيير ومراجعتها بصفة منتظمة.

ينص كتيب تأمين المعلومات الوطنية أيضا على تصنيف جميع التغييرات ضمن فئات، مثل الفئة المحددة أعلاه. ويمكن أن تحظى المؤسسة بأسلوبها الخاص في التصنيف الذي قد يكون مشتقا من الأسلوب المذكور أعلاه.

يركز التصنيف الملائم للتغيير على الموارد المناسبة التي قد تكون لازمة لإجراء مثل هذا التغيير.

CM 2 تأسيس لجنة لإدارة التغيير.

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بتشكيل لجنة إدارة التغيير، التي تتألف من ممثلين عن وحدات العمل/ الوظائف المتعددة والقائمين على إدارة العمل وغيرهم.

تتولى لجنة إدارة التغيير المسؤولية عن تقييم طلبات التغيير المقدمة إليها وتقييم أثر التغيير على إدارة الأعمال وجدواه التقنية والمالية والتأثير على الوضع الأمني للمؤسسة.

ضمان أن تتوافق الخطة مع إجراءات التشغيل النموذجية للمؤسسة.

CM 3 التصديق على التغييرات المقترحة من خلال لجنة إدارة التغيير المعنية.

ينص كتيب تأمين المعلومات الوطنية على عدم استحداث التغييرات المخصصة ضمن النظام/ العمل. وينبغي أن تتم مناقشة التغييرات المقترحة والتصديق عليها من قبل لجنة إدارة التغيير. وتتولى لجنة إدارة التغيير المسؤولية عن ضمان استحداث جميع التغييرات بأسلوب منهجي وإتباع إجراءات التشغيل النموذجية ودعمها من خلال آليات احتياطية.

CM 4 التأكد من تقييم حاجة النظام إلى إعادة الاعتماد فور تنفيذ أي تعديل مقترح قد يؤثر على أمن نظام تكنولوجيا الاتصالات والمعلومات.

ينص كتيب تأمين المعلومات الوطنية على أنه في حالة وجود تأثير كبير للتغيير المستحدث (سواء كان كبيرا أو صغيرا) على الوضع الأمني للمؤسسة، يتعين على لجنة إدارة التغيير تقييم ما إذا كان النظام يتطلب إعادة التصديق؛ وفي تلك الحالة بدء وتنفيذ خطة من أجل إجراء اعلدة المصادقة.

CM 5 يتم تحديث جميع الوثائق المتعلقة بالنظام كي تعكس عملية التغيير.

ينبغي أن تكفل لجنة إدارة التغيير تحديث عمليات ما بعد تنفيذ التغيير وجميع العمليات ذات الصلة والمعلومات ذات الصلة بالنظام. ويتم الاحتفاظ بسجلات إدارة التغيير في قاعدة بيانات خاصة بإدارة التغيير.

CM 6 ضمان تطبيق هذه المعايير على حد السواء على التغييرات العاجلة. وينبغي أن تحدد عملية إدارة التغيير الإجراءات الملائمة الواجب إتباعها قبل تنفيذ التغييرات العاجلة وبعدها.

من الممكن أن يكون هناك وقت أو حالات يكون بها حاجة إلى إجراء تغيير عاجل دون اللجوء إلى إجراءات إدارة التغيير الواجبة. وينبغي أن تضع لجنة إدارة التغيير معيارا لهذه الحالات يحدد الشروط التي يتم في ظلها إجراء التغييرات وكيفية القيام بذلك.

ينبغي أن تضمن لجنة إدارة التغيير أيضا أن يلتزم القائمون على تنفيذ التغيير، في مرحلة ما بعد حالات الطوارئ واستكمال إدارة التغيير، ببذل العناية الواجبة وإعادة عمل التغيرات المقترحة من خلال إجراءات وعمليات قياسية وموحدة.

ينبغي أن يتم استيفاء جميع أعمال التوثيق ذات الصلة.

6 - إرشادات حول أمن العاملين [PS]

6-1 إرشادات حول السياسة والضوابط الرئيسية

PS 1 ضمان أن تتفق عمليات إدارة الموارد البشرية مع سياسات ومبادرات أمن المعلومات بالمنظمة.

يعد الإنسان أضعف حلقة ضمن سلسلة الأمن. ولإقامة وضع أمني فعال، يتحتم ضمان وجود الضوابط المناسبة من أجل التخفيف من المخاطر البشرية. ويوطد كتيب تأمين المعلومات الوطنية أساس تلك الضوابط من خلال ضمان دمج أفضل الممارسات الأمنية ضمن جميع عمليات الموارد البشرية.

PS 2 ضمان أن تحتفظ إدارة الموارد البشرية بكتيب موارد بشرية يكون متاحا لجميع العاملين لضمان وعيهم بالتزاماتهم تجاه أمن المعلومات.

ينص كتيب تأمين المعلومات الوطنية على توثيق مسؤوليات أمن المعلومات وإتاحتها للعاملين في جميع الأوقات. ويكفل دمج مسؤوليات أمن المعلومات ضمن كتيب الموارد البشرية إتاحة جميع المعلومات التي يحتاج إليها العاملون (القواعد ومدونة السلوك والإجراءات التأديبية والمسؤوليات...الخ) من خلال مصدر معلومات واحد. ويضمن ذلك سهولة تحديث المعلومات والمحافظة عليها وتوزيعها (لا يوجد مصادر متعددة يتم تعديلها وتحديثها وتوزيعها).

PS 3 تخزين وإدارة المعلومات ذات الصلة بالعاملين من خلال العناية الواجبة بما يتفق مع متطلبات التعامل مع المعلومات الشخصية وفقا لما هو محدد بسياسة حماية البيانات والخصوصية [IAP-NAT-DPRP].

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بصياغة إجراءات داخلية لمعالجة المعلومات الشخصية التي تجمعها عن طريق العاملين و/أو كجزء من أنشطة العمل لمنع إساءة استخدامها من قبل عناصر المتعاملين معها. ويمكن أن تكون هذه العناصر داخلية أو خارجية بالنسبة للمؤسسة. وعلاوة على ذلك، ينبغي أن تكفل المؤسسة التزام الإجراءات باللوائح ذات الصلة أثناء إجراءات التعامل مع المعلومات الشخصية. وقد اقترحت وزارة المواصلات الإتصالات بقطر وضع سياسة حماية البيانات والخصوصية [IAP-NAT-DPRP]، التي يتم حاليا صياغتها، كي تنص على كيفية جمع تلك المعلومات ومعالجتها والاحتفاظ بها لتجنب إساءة استخدامها.

PS 4 ضمان إدراج مسؤوليات أمن المعلومات كجزء من المسؤوليات والتوصيفات الوظيفية للعاملين وتطبيقها على عملية توظيف الأفراد داخل المنظمة.

علاوة على ذلك، ينص كتيب تأمين المعلومات الوطنية على تعريف مسؤوليات أمن المعلومات باعتبارها جزء من مسؤوليات العاملين وجزء من التوصيفات الوظيفية القياسية. ويهدف ذلك إلى ضمان فهم العاملين لمسؤوليات أمن المعلومات المنوطة بهم منذ يوم تقدمهم لشغل الوظيفة. ويكفل ذلك التركيز بالصورة الواجبة على أمن المعلومات.

وينص كتيب تأمين المعلومات الوطنية أيضا على الالتزام بهذه المسؤوليات ومتابعتها طيلة فترة عمل العاملين بالمؤسسة.

وهناك مثال بسيط على التنفيذ من خلال ضمان أن يكون ذلك جزءا من منهجية تقييم أداء العاملين. وينبغي أن يتم تحديد معايير الأداء ذات الصلة بأمن المعلومات وربطها إذا أمكن بتقييم طبقاً لنظام SMART.

PS 5 إجراء الفحص الملائم للتأكد من نزاهة المرشحين المحتملين للتوظيف والمتعاقدين (بما في ذلك العاملين المتعاقدين من الباطن). ويمكن أن تتوسع المؤسسة في تطبيق هذه الممارسة لتشمل العاملين الحاليين وفقا للضرورة من أجل الوفاء بالشروط الناجمة عن عوامل تشتمل، على سبيل المثال لا الحصر، على "تغيير مسؤوليات العاملين" أو "الشبهة الناجمة عن سلوكيات أي عامل".

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بإجراء الفحص الملائم للمعلومات الأساسية من أجل إقرار سلامة المعلومات التي يقدمها العامل المحتمل. وتؤكد فحوص المعلومات الأساسية على ملاءمة العامل للوظيفة. وقد يختلف مستوى فحص المعلومات الأساسية بناءً على طبيعة وحساسية العمل. ويمكن أن تتضمن فحوص المعلومات الأساسية بعض من أو كل ما يلي:

فحص الوثائق والسجلات: يتضمن ذلك فحص السجلات التي يقدمها العامل المحتمل، وعلى سبيل المثال: المؤهلات العلمية والتاريخ الوظيفي وعضوية المنظمات والفحوص المرجعية وغير ذلك. ويمكن أن تكون الشبكة الدولية (الإنترنت) أداة فعالة للغاية في هذا الصدد. ويمكن أن توفر عمليات فحص مواقع الشبكات الاجتماعية (تتضمن الأمثلة مواقع Facebook وLinkedIN) والمدونات والمنتديات بعض المعلومات حول المرشح. ومع ذلك، ينبغي أن يتم استخدام كل هذه المعلومات بحذر شديد، نظرا لأن هناك حالات يتم بها الكشف عن الهوية الفعلية للأشخاص أو الخضوع لرقابة جهاز المراجعة والتدقيق بقطر من قبل الأشخاص المخولين بذلك لأسباب قوية ومبررة.

الفحص الجنائي: يتضمن ذلك عملية فحص لضمان ألا يكون للعامل أي تاريخ جنائي أو خلفية جنائية. ومع ذلك، تحظى المؤسسة بالحق في اتخاذ القرار بشأن المرشحين ذوي سجل جنائي غير خطير، مثل المخالفات ذات الصلة بقيادة السيارات.

يتم تمديد عمليات الفحص لتشمل المتعاقدين والمتعاقدين من الباطن اعتمادا على طبيعة وحساسية العمل الذي يشاركون به.

سوف تحظى المؤسسة بالحق في تمديد هذا الفحص ليشمل العاملين الحاليين في حالة إثارة مواقف مثل تغيير المسؤوليات أو الشبهات حول سلوك أحد العاملين. ومع ذلك، تعتمد المؤسسة على العناية الواجبة لضمان ألا تكون تلك الشبهات جزءا من الكشف عن المخالفات أو نتيجة له.

PS 6 ضمان أن يوقع العاملون على اتفاقية للانضمام إلى المؤسسة تنص على الالتزامات والمسؤوليات الأمنية المنوطة بهم. وتتضمن ما يلي:

أ- التزامات السرية وعدم الإفصاح

ينبغي أن تتولى المؤسسة إخطار المرشحين المحتملين فيما يتعلق بالتزامهم بالإطار الأمني المقرر للمؤسسة. ويتضمن ذلك، على سبيل المثال لا الحصر، ما يلي:

1- اتفاقية السرية وعدم الإفصاح
2- فهم وقبول سياسة تأمين المعلومات

تعد الوثيقة الموقعة بمثابة دليل قانوني يضمن موافقة العامل على الالتزام بلوائح المؤسسة.

ينبغي أن تفحص المؤسسة الخيارات الخاصة بمراجعة الالتزامات واللوائح الأمنية على فترات منتظمة. ويمكن أن تتم تلك المراجعة سنويا أو أثناء تجديد العقد.

PS 7 ضمان وجود ضوابط ملائمة لمنع العاملين (الموظفين والموردين والمتعاقدين والزوار) من الإفصاح عن المعلومات دون تصريح أو سوء استعمالها أو إفسادها بمقتضى السياسات الأمنية الخاصة بالمؤسسة.

ينبغي أن تدرك المؤسسة أن التوعية حول مسؤوليات أمن المعلومات وتوقيع اتفاقية عدم الإفصاح وغيرها تمثل ضوابط إدارية قد تمنع العامل من خرق الأمن. ومع ذلك، غني عن القول أنه يمكن دائما أن تكون تلك الضوابط فعالة؛ ومن ثم، فمن الضروري أن تستعين المؤسسة بأنماط أخرى للرقابة التقنية من أجل التعامل مع المخاطر الناجمة عن خرق أمن المعلومات.

يمكن أن تتضمن الضوابط على المستوى التقني تقنيات إدارة المضمون، وتتضمن على المستوى الإداري منع أي عاملين باستثناء "المتحدثين الرسميين" حينذاك من الإدلاء بتصريحات إلى جمهور العامة.

PS 8 ضمان أن تقتصر حقوق المستخدمين في الوصول إلى المعلومات على تلك المعلومات التي يحتاجون إليها من أجل الالتزام بمتطلباتهم الوظيفية وفقا للمبادئ الأقل امتيازا.

ينشأ أحد الأسباب المحتملة لخرق المعلومات (بصورة متعمدة أو غير متعمدة) في السيناريوهات التي يحظى من خلالها العامل أو المتعاقد بإمكانية الوصول إلى المعلومات دون وجه حق. وهناك أسطورة عامة تنص على أنه "إذا حظيت بالوصول إلى المعلومات، يمكنني استخدامها".

ينص كتيب تأمين المعلومات الوطنية على اقتصار المعلومات التي يتم تقديمها إلى العاملين أو المتعاقدين بالمؤسسة على التفويض الفعال لمسؤولياتهم وتستند بصورة مشددة إلى قاعدة "الحاجة إلى المعرفة".

PS 9 توزيع المسؤوليات على عمليات ومهام الأمن الحساسة، باستخدام مبادئ الرقابة من قبل شخصين لضمان تبادل المعلومات وتجنب وجود شخص واحد يتولى السيطرة الكاملة على العمليات أو المهام الرئيسية.

تتولى المؤسسة تنفيذ الضوابط لضمان عدم هيمنة شخص واحد بمفرده على العملية بالكامل. وينبغي أن يكفل القائمون على العملية عدم قيام نفس الشخص بالاضطلاع بأنشطة المعالجة والتفويض أو المعالجة وتدقيق الحسابات. وسوف يضمن ذلك ضرورة أن يتواطئ أكثر من شخص حتى يتم الاختراق.

وعلاوة على ذلك، فيما يتعلق بالأنظمة والتطبيقات بالغة الأهمية والسرية، ينبغي اقتسام كلمات المرور أو الوصول بين كيانين كحد أدنى. وعلى سبيل المثال، قد يتطلب الوصول إلى النظام مستوى ثنائي من الرقابة على الوصول؛ ويتم توزيع هذه الرقابة بين شخصين؛ وفي حالة عدم إمكانية ذلك، يتم تقسيم كلمة المرور إلى النظام إلى قسمين، دون أن يحظى أي شخص بمفرده بإمكانية الوصول إلى هذين الجزأين.

ومع ذلك، ينبغي أن تتوخي المؤسسة الحذر الواجب لضمان تطبيق تلك الضوابط على العمليات الأكثر حساسية، نظرا لأن هذا التوجه قد يكون في حد ذاته سببا لرفض الخدمة في الأوقات الحرجة.

PS 10 وضع عملية تأديبية وضمان توعية العاملين بتلك العملية. وينبغي أن يتم توثيق العملية التأديبية ضمن كتيب الموظفين أو كتيب الموارد البشرية.

تحدد المؤسسة العملية التأديبية وتكفل توعية العاملين بتلك العملية من خلال جلسات التوعية الأمنية المناسبة. ويمكن أن يتم توثيق تلك العملية التأديبية ضمن كتيب الموظفين أو كتيب الموارد البشرية وإتاحتها للعاملين المعنيين من خلال وسائل مثل الشبكة الداخلية أو النسخ المطبوعة أو المكتبة أو غير ذلك.

PS 11 ضمان أن يكون الموردون أو المتعاقدون أو الممثلون أو زوار مقار المؤسسة:

- **أ- مسجلون وفقا لبيانات تعريفية**
- **ب- يحصلون على شارة الزوار**
- **ج- يرتدون لافتة ملحوظة توضح وضعهم كزوار**
- **د- على دراية بالتزاماتهم المتعلقة بالامتثال لسياسات الأمن الخاصة بالمؤسسة**
- **هـ- يرافقهم موظفو المؤسسة أثناء دخول المناطق المؤمنة**

قد تقتضي طبيعة العمل الذي تضطلع به المؤسسة أو متطلبات ذلك العمل قيام الزوار من الموردين أو المتعاقدين أو الممثلين أو الضيوف بزيارة مقر المؤسسة. ورغم أنه من الصعب التعرف على دوافع كل شخص، فمن الحكمة أن تتوخى المؤسسة الحذر وأن تطبق تلك الضوابط من أجل تنظيم دخول هؤلاء الزوار.
ينص كتيب تأمين المعلومات الوطنية على أن يكون هناك من يرافق كل هؤلاء الزوار والموردين والمتعاقدين والممثلين وغيرهم داخل المناطق الإدارية. وينبغي أن يتم تعريف الزوار بإيجاز بالوضع الأمني والضوابط القائمة. وعادة ما يمكن

القيام بذلك من خلال التأكد من أن شارة الزائر مرفقة بكتيب أو منشور يوفر المعلومات الأساسية للزوار ويحذرهم من كونهم مراقبين ويتولى توعيتهم بشأن المسؤوليات المنوطة بهم.

ينبغي أن يتم توعية العاملين وتشجيعهم على توقيف واعتراض والإبلاغ عن الأغراب الذين يتجولون بمقر المؤسسة دون وضوح هوياتهم، أي دون بطاقة الموظف أو شارة الزائر.

PS 12 ضمان صدور طلب التغيير من قبل إدارة الموارد البشرية عند تغيير مهام أو فسح عقد أي موظف أو متعاقد أو أي طرف آخر. ويكفل ذلك أن يعيد العاملون أو المتعاقدون أو الأطراف الأخرى أصول المؤسسة وأن يتم تعديل/ إلغاء الوصول المادي والافتراضي حسب الاقتضاء.

ينص كتيب تأمين المعلومات الوطنية على الدمج الفعال للموارد البشرية وإدارة المرافق وتكنولوجيا المعلومات ضمن العمليات ذات الصلة بالقوى العاملة. ويتم متابعة عمليات تعيين الموظفين الجدد أو أي عمليات فسخ تعاقد أو تغيير مسؤوليات باستخدام الأسلوب الملائم لإدارة التغيير.

يهدف ذلك إلى ضمان إطلاع جميع الأطراف الرئيسية المعنية، أي الموارد البشرية وإدارة المرافق وتكنولوجيا المعلومات على أحدث التطورات عندما يطلب شخص جديد دخول مرافق المؤسسة (سواء كان دخولاً ماديا أو افتراضيا) وحينما يغادر ذلك الشخص المنظمة بسبب التقاعد أو فسخ التعاقد أو الاستقالة أو انتهاء الخدمة.

سوف يكفل ذلك تعديل جميع قواعد الرقابة على الدخول (المادي والافتراضي) بصورة ملائمة بما يضمن عدم دخول أطراف سابقة إلى النظام. وينبغي أن يتم إتباع عملية مماثلة عندما يتم تغيير المسؤوليات عن طريق النقل أو الترقية أو تخفيض الدرجة الوظيفية.

7 - إرشادات حول التوعية الأمنية [SA]

7-1 إرشادات حول السياسة والضوابط الرئيسية

SA 1 تنظيم برنامج توعية أمنية وتخصيص الموازنات اللازمة لتنفيذه.

تعد التوعية الأمنية هامة لضمان فهم جميع الأطراف ذات الصلة للمخاطر وقبول وإقرار الممارسات الأمنية الجيدة. ويمكن أن يوفر التدريب والتوعية للمستخدمين والمطورين وإداريي النظام وإداريي الأمن وأي أطراف ذا صلة المهارات والمعارف اللازمة لتنفيذ التدابير الأمنية.

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بتخصيص الموازنات اللازمة لبدء وتنفيذ والحفاظ على برنامج التوعية الأمنية داخل المؤسسة.

SA 2 يتضمن هذا التدريب كحد أدنى:

المتطلبات الرئيسية المحددة بكتيب تأمين المعلومات الوطنية هذا.

المتطلبات الأمنية للمؤسسة.

المسؤوليات القانونية.

ضوابط العمل.

الاستخدام الصحيح لمرافق معالجة البيانات (على سبيل المثال: إجراءات الدخول واستخدام حزم البرمجيات ...إلخ).

معلومات حول عملية التنفيذ.

معلومات حول من ينبغي الاتصال به للحصول على المزيد من النصائح الأمنية والقنوات المناسبة للإبلاغ عن حوادث أمن المعلومات.

ينص كتيب تأمين المعلومات الوطنية على تصميم التوعية الأمنية لتغطية الموضوعات ذات الصلة بنشاط المؤسسة بالصورة الملائمة.

1- تتضمن مواد التدريب، كحد أدنى، مضمون من شأنه أن:

أ. يساعد الفرد على فهم معنى أمن تكنولوجيا المعلومات وسبب الحاجة إليه ومسؤوليته الشخصية عن الأمن، بالإضافة إلى أهمية الالتزام بالسياسات والمعايير الأمنية المحددة للمؤسسة. وحيثما تكون متطلبات أمن تكنولوجيا المعلومات بالمؤسسة أكثر تشددا من السياسات والمعايير الوطنية لأمن تكنولوجيا المعلومات، ينبغي توضيح هذه العناصر.

ب. يتضمن أو يشير إلى القوانين واللوائح الوطنية.

ج. يساعد الفرد على تحقيق فهم أفضل لتقنيات أسلوب الهندسة الاجتماعية التي يمكن استخدامها في خداع شخص من أجل الكشف عن معلومات سرية أو خاصة أو متميزة بهدف تعريض سرية وسلامة وتوافر بيانات ومعلومات المؤسسة وموارد تكنولوجيا المعلومات للمخاطر.

د. يشتمل على سبيل المثال لا الحصر على:

1- مسؤولية الأفراد عن الإبلاغ عن القضايا ذات الصلة بأمن تكنولوجيا المعلومات وآلية القيام بذلك.
2- حقيقة إمكانية خضوع أنشطة الفرد للمراجعة والتدقيق.
3- المتطلبات القانونية لسرية وحماية البيانات (*القانون المقترح لسرية وحماية البيانات).
4- ملكية البيانات ووضع العلامات على البيانات.
5- قضايا الاستخدام في غير نطاق العمل.
6- متطلبات كلمة المرور الخاصة بوحدة الموازنة من أجل الاستخدام والإدارة.
7- الحماية من الفيروسات والبرامج المضرة والمدمرة.
8- سياسة الاستخدام المقبول للأصول المعلوماتية والبريد الإلكتروني واستخدام الشبكة الدولية (الإنترنت).
9- ترخيص البرمجيات.
10- حساسية الأنظمة التابعة للمؤسسة للتهديدات ومخاطر ونقط الضعف.
11- تقنيات الهندسة الاجتماعية الشائع استخدامها في خداع المستخدمين لإقناعهم بالتخلي عن إمكانية الوصول للمعلومات أو الكشف عن المعلومات السرية أو المتميزة.
12- الأمن المادي.
13- إمكانية تطبيق المتطلبات الأمنية على جميع موارد تكنولوجيا المعلومات، بما في ذلك أجهزة تكنولوجيا المعلومات المحمولة، مثل الحاسبات المحمولة وغير ذلك.

2- ينبغي أن يتم توفير مواد التدريب على التوعية الأمنية (الكتيبات والوثائق وغير ذلك)، بالإضافة إلى سياسات ومعايير وإجراءات أمن تكنولوجيا المعلومات، سواء بصورة إلكترونية أو عن طريق النسخ الورقية إلى جميع العاملين والمتعاقدين والعمال المؤقتين بالمؤسسة، حسب الاقتضاء.

SA 3 يحصل جميع موظفي المؤسسة، بالإضافة إلى المتعاقدين والمستخدمين لدى الأطراف الأخرى حيثما كان ذلك مناسبا، على التدريب والتوعية الملائمين فيما يتعلق بسياسات وإجراءات المؤسسة حسب الاقتضاء بشأن مهامهم الوظيفية وأدوارهم ومسؤولياتهم ومهاراتهم.

ينبغي أن يكون مستوى التوعية الأمنية والتدريب متناسبا مع مستوى الوصول والخبرات اللازمة فيما يتعلق بمكونات النظام وموارد المعلومات التي يتولى الموظف بالمؤسسة أو المتعاقد معها أو المستخدم لدى أي طرف آخر المسؤولية عنها.

1- ينبغي أن يحصل الموظف بالمؤسسة أو المتعاقد معها أو المستخدم لدى أي طرف آخر على تدريب أمني قبل أن يحظى بإمكانية الوصول إلى أنظمة وموارد تكنولوجيا المعلومات. وقبل الوصول إلى تطبيقات البرمجيات المحددة الخاصة بالمؤسسة، يحصل العاملون على أي تدريب أمني متخصص يركز، حسب الاقتضاء، على أدوارهم ومسؤولياتهم ذات الصلة بنظام تطبيقات البرمجيات.

2- يتم تعزيز التوعية الأمنية بصفة مستمرة. وينبغي أن يتم تحديث التدريب على التوعية الأمنية الذي يحصل عليه العاملون بالمؤسسة بصورة سنوية أو بمجرد وقوع حدث محدد، مثل تغير المسؤوليات الوظيفية أو الحالة الوظيفية أو غير ذلك.

SA 4 ينبغي تدريب الموظفين في التعرف على محاولات استخراج المعلومات عن طريق الهندسة الاجتماعية عليهم، وعدم إفشاء أي من المعلومات التي يمكن أن تهدد امن المؤسسة أثناء المناسبات الاجتماعية والدورات التدريبية..

يهدف كتيب تأمين المعلومات الوطنية إلى التأكيد على مخاطر الهندسة الاجتماعية التي قد تؤدي إلى الإفصاح عن المعلومات. وغالبا ما تتمثل تلك المخاطر في السلوك البشري للمناقشات القائمة على الخبرات الشخصية. فمن الممكن أن يخوض العاملون الحكوميون أثناء التدريب مناقشات ومداولات حول المعلومات الداخلية للمؤسسة (عملية أو تقنية). وقد يؤدي ذلك إلى الإفصاح غير المتعمد عن معلومات حساسة.

SA 5 يتم مراجعة وتحديث مضمون التدريب والتوعية الأمنية بصورة منتظمة كي يعكس التوجهات والمخاطر والتغييرات الجديدة بالبنية الأساسية لتكنولوجيا المعلومات في المؤسسة.

ينص كتيب تأمين المعلومات الوطنية على تقديم دورات تدريبية على التوعية الأمنية ومراجعة وتحديث محتوى التدريب بصورة منتظمة لضمان تناوله لأهداف وثقافة ونشاط وتكنولوجيا وأنظمة المؤسسة ومتطلبات البيانات والمعلومات الخاصة بها.

SA 6 يحصل العاملون الجدد على التدريب والتوعية بأمن المعلومات كجزء من عملية تحفيز العاملين.

ينص كتيب تأمين المعلومات الوطنية على دمج أمن المعلومات ضمن أنشطة العمل المختلفة للمؤسسة. ويساعد دمج برنامج التدريب على التوعية الأمنية وبرنامج التدريب التوجيهي على خلق التعاون بين الموارد البشرية وإدارة أمن المعلومات.

وعلاوة على ذلك، تؤكد عملية الدمج للموظف الجديد على أهمية أمن المعلومات.

SA 7 يتم تقييم التدريب للتأكد من فاعلية البرنامج، بما في ذلك الحفاظ على سجلات حضور برامج التوعية الأمنية.

ينبغي أن تدرج المؤسسة آليات التقييم والنتائج الرسمية لقياس مدى ملاءمة وفاعلية برامج وتقنيات ومواد التوعية الأمنية والتدريب.

ينبغي أن تحتفظ المؤسسة بسجلات حول جهود التوعية بأمن المعلومات. ويجب أن يتم توثيق حضور برامج التدريب على التوعية الأمنية ضمن ملف الموظف بشؤون العاملين، مع إقرار الموظف بالحصول على التدريب وفهمه له.

ينبغي أن تحدد المؤسسة معايير الأداء الرئيسية التي تساعد على توضيح فاعلية جهود التوعية الأمنية.

SA 8 يتم استخدام الوسائط غير المباشرة مثل الملصقات والشبكات الداخلية والبريد الإلكتروني ...الخ بصورة فعالة من أجل دعم برنامج التوعية.

تحدد المؤسسة الأساليب الملائمة المستخدمة في التوعية والتعليم، والتي قد تتضمن على سبيل المثال لا الحصر ما يلي:

- الملصقات
- التدريب القائم على الحاسوب
- مواد وموارد الشبكة الداخلية
- أفلام الفيديو
- الرسائل الإخبارية
- النشرات
- البيانات الموجزة
- التعليمات الرسمية بالفصل الدراسي
- التدريب أثناء العمل
- المؤتمرات

8 - إرشادات حول إدارة الحوادث [IM]

8-1 إرشادات حول السياسة والضوابط الرئيسية

IM 1 تعيين شخص لتولى المسؤولية وإدارة برنامج إدارة الحوادث، بما في ذلك نقطة اتصال لجميع اتصالات الأمن المعلوماتية.

ينص كتيب تأمين المعلومات الوطنية على أن تحدد المؤسسة المسؤول عن إدارة الحوادث. وينبغي أن يتولى ذلك الشخص المسؤولية الكاملة عن إدارة برنامج إدارة الحوادث، الذي يتضمن إدارة الموازنات وتعريف البرنامج وتنفيذه وغير ذلك.

IM 2 بناء القدرة على التصدي لحوادث أمن المعلومات، اعتمادا على سياسة تصنيف المعلومات الوطنية القادرة على إجراء تقييم دوري لمخاطر (من خلال المخاطرونقاط الضعف وقيمة الأصول) البيانات والعمليات والأنظمة والشبكات وفقا لكتيب تأمين المعلومات هذا.

يتولى المسؤول عن عملية إدارة الحوادث (مدير إدارة الحوادث) تقييم المتطلبات الخاصة بالقدرة على الاستجابة للحوادث في إطار متطلبات عمل المؤسسة. ويقوم مدير إدارة الحوادث بمراجعة هذه المتطلبات بصفة دورية استنادا إلى تحليل المخاطر ونقاط الضعف.

IM 3 تحديد إجراءات الكشف عن الحوادث وتقييمها والتصدي لها.

تتولى المؤسسة تحديد الإجراءات الخاصة بالكشف عن الحوادث وتقييمها والتصدي لها. وتتضمن الإجراءات، كحد أدنى، ما يلي:

1) الكشف عن الحوادث.

أ. تتضمن إجراءات الكشف متابعة الحوادث والإبلاغ عنها.

ب. يتم تشجيع جميع المستخدمين على الإبلاغ عن حوادث الأمن التي يرصدونها. ويتضمن ذلك أي أخطاء عرضية تحدث ويمكن أن تتسبب في تعريض الأمن للمخاطر.

ج. يمكن ضبط أدوات متابعة نظام المعلومات، مثل متابعة الشبكات ونظام الكشف عن التدخل ومنعه وغير ذلك، بحيث تنذر أو تبلغ بصورة أوتوماتيكية عن أي أحداث أو وأحداث مريبة.

د. تتألف الحوادث الأمنية من كل من حوادث تكنولوجيا المعلومات والحوادث غير المتعلقة بتكنولوجيا المعلومات.

- الإصابة بالفيروسات
- عدم مصاحبة الأشخاص أو التعرف عليهم (من غير العاملين) أثناء الانتقال داخل المقر.

- المشكلات الخاصة بأقفال الأبواب (بوابات المداخل)

2) تقييم الحوادث

أ. تقييم ما إذا كان التقرير يمثل حادثا أو إنذار كاذب أو خدعة.

ب. تقييم نوع وحجم المشكلة.

ج. تحديد مستوى الأولوية وبالتالي خطة العمل.

د. تحديد ما إذا كان نشاط الحادث لا يزال قائما أو قد توقف؛ وفي حالة توقفه، تحديد ما إذا كان من المحتمل أن يبدأ نشاطه من جديد.

هـ. تحديد الأنظمة والبيانات التي تأثرت أو من المحتمل أن تتأثر بالفعل وعددها؛ وأيضا تقييم ما إذا كان نشاط الحادث قد وقع داخل نطاقك فقط أو أن هناك نشاط خارجي أيضا (كمصدر أو هدف نهائي).

1- تقييم الخسائر في حالة حدوث خرق فعلي.

2- وضع جدول تقديري لاستعادة قدرة النظام أو إجراءات السيطرة على الموقف.

3) التصدي للحوادث

أ. إخطار السلطات المعنية

- إخطار الإدارة والرؤساء حول الحادث والطريق إلى المستقبل.
- التأكد من إخطار الإدارة في المراحل الحرجة.
- تحديد الأهداف الفورية وفقا لموافقة الإدارة. ويمكن أن يتضمن ذلك استعادة قدرة النظام أو تقليل زمن التعطل أو محاولة تعقب المتعدين وغير ذلك.
- إخطار فريق الاستجابة لطوارئ الحاسبات بقطر وأجهزة تطبيق القانون وطلب المساعدة إذا لزم الأمر.

ب. جمع الأدلة.

- توثيق الخسائر الناتجة.
- عمل نسخة اختياطية كاملة لجميع السجلات والنظام برمته.
- عمل نسخة احتياطية للسجلات من الجدار الناري وأجهزة الراوتر وأنظمة الكشف عن التدخل والأجهزة الأمنية الأخرى التي قد تساعد في تشخيص الخرق الأمني.
- توثيق الإجراءات التي يتم إجراؤها لمراقبة واحتواء والقضاء على الحادث.

ج. مراقبة/ احتواء/ إلغاء الخسائر

- تحديد مصدر المشكلة (التهديد أو الخطر).

- تحديد نقطة الضعف التي تسببت في تعرض النظام للمخاطر (نقطة ضعف)
- التأكد من التخلص من نقطة الضعف والتخفيف من حدتها والسيطرة على الخرق الأمني.
- إدراك أن الدخلاء ربما قاموا بتنصيب فيروس طروادة أو التجسس على لوحة المفاتيح أو تنصيب مثل تلك البرامج على الأنظمة المعرضة للمخاطر.

د. استعادة الخدمات

- التأكد من تشغيل النظام بعد التخلص من نقاط الضعف بالنظام والتأكيد على فرض الرقابة على النظام.
- فحص جميع الخدمات المباشرة التي يوفرها النظام.
- متابعة النظام للتعرف على أي مشكلات أخرى أو على تدهور الخدمات.
- إجراء اختبارات أمنية (اختبار/ مسح الاختراق) لضمان أداء النظام حسب الاقتضاء.
- إصدار النظام لاستخدامه من قبل جمهور العامة.

IM 4 تحديد إجراءات الإبلاغ عن حوادث أمن المعلومات وإدارتها واستعادة القدرة على العمل داخليا بالتعاون مع فريق الاستجابة لطوارئ الحاسبات بقطر والمؤسسة الأخرى.

يتولى مدير إدارة الحوادث بناء القدرة على التصدي للحوادث داخل المؤسسة. وفي هذه الحالة، يلعب فريق الاستجابة لطوارئ الحاسبات في قطر دور المكتب الحكومي للتصدي للحوادث ويوفر التنسيق المركزي والدعم لعملية قدرة التصدي للحوادث في المؤسسة.

تتولى إدارات القدرة على التصدي للحوادث المعنية بالمؤسسة المسؤولية عن عمليات التعامل مع الحوادث التي تقع في أنظمة أو شبكات المعلومات المحددة أو خدمات الحاسبات أو المجالات الوظيفية داخل نطاق المؤسسة التي تعمل بها.

يتم وضع خطط وقنوات الاتصالات لتبادل المعلومات مع فريق الاستجابة لطوارئ الحاسبات بقطر وأجهزة تطبيق القانون والمؤسسة الأخرى (إذا لزم الأمر) أثناء الأوضاع العادية والأزمات.

IM 5 خلق الوعي بين العاملين من أجل الإبلاغ عن الحوادث.

ينص كتيب تأمين المعلومات الوطنية على أن تكون إدارة الحوادث جزء من التدريب على الوعي الأمني. وينبغي أن يتم توعية جميع المستخدمين بكيفية الإبلاغ عن الحوادث. ويمكن أيضا توعية المستخدمين حول كيفية الاستجابة لحوادث محددة، مثل الحرائق والكوارث الطبيعية وغير ذلك.

تنشئ المؤسسة قنوات صديقة للمستخدم من أجل الإبلاغ عن الحوادث.

IM 6 تصنيف جميع الحوادث وفقا لتصنيف خطورة الحادث المنصوص عليه بالملحق "ج".

لضمان الاتساق والتوافق بين الموارد المختلفة، فمن الحكمة أن يتم تصنيف الحوادث الأمنية وفقا لجدول تصنيف مدى خطورة الحادث، المنصوص عليه بالملحق المرفق بكتيب تأمين المعلومات الوطنية.

IM 7 التنسيق مع فريق الاستجابة لطوارئ الحاسبات بقطر لوضع سجل حوادث في المؤسسة.

ينص كتيب تأمين المعلومات الوطنية على توثيق جميع الحوادث الأمنية. وعقب التأكد من استعادة النظام، تسعى إدارة القدرة على التصدي للحوادث إلى تسجيل المعلومات التالية:

- توثيق وجمع جميع المعلومات المتعلقة بالحادث بأكمله.
- فتح القضية مع الجهاز المعني بتطبيق القانون، اعتمادا على نوع الحادث وحجم الخسائر ومدى حدتها.
- تحديد الدروس المستفادة أثناء الحادث. وتقييم ما إذا كان من الممكن تحسين أسلوب العمليات من أجل التعامل مع الموقف بصورة أفضل. وتبادل الدروس مع المؤسسة الأخرى من خلال فريق الاستجابة لطوارئ الحاسبات في قطر من أجل منع أي هجمات مماثلة.

IM 8 إبلاغ فريق الاستجابة لطوارئ الحاسبات بقطر عن جميع حوادث المستوى الأول من الخطورة خلال ساعة واحدة من اكتشاف وقوع الحادث.

ينص كتيب تأمين المعلومات الوطنية على توافر الموارد الحكومية المثلى من أجل تسوية الحوادث التي قد تحظى باهتمام هائل من جانب الأمة. ويتم تعريف حوادث المستوى الأول للأهمية باعتبارها تلك الحوادث التي قد تتضمن جزءا من البنية الأساسية الحرجة للأمة.

IM 9 منسق إدارة الحوادث مسؤول عن وضع وتطوير وتنفيذ خطة سنوية لضمان أمن المعلومات. ويمكن أن تشمل بعض الأنشطة مثل اختبار الاختراق، ومراجعة الإجراءات الأمنية، واختبار سيناريو الحادث.

يجب على منسق إدارة الحوادث وضع خطة سنوية لمحاكاة كيفية إستجابة المؤسسة للحوادث. يمكن إجراء اختبارات للتحقق من فعالية العمليات والتحذيرات الموضوعة. وتشمل هذه الاختبارات ولكن لا يقتصر على مراجعة الجداول من قبل الجهات العليا بالمؤسسة ، والاختبارات العملية، والتدقيق، الخ. الغرضمن كل ما سبق هو ضمان حفاظ المؤسسة علىالعمليات الحالية والضوابط والنظم وأنها جاهزة للعمل كما تم تصميمها خلال حادث أو أزمة. وينبغي أن يتضمن الاختبار أيضا سلسلة من الاحتجاز، والتعامل مع سجلات، والطب الشرعي، والدروس المستفادة.

9 - إرشادات حول إدارة استمرارية تصريف الأعمال [BC]

9-1 إرشادات حول السياسة والضوابط الرئيسية

BC 1 يتم تعيين شخص يتولى مسؤولية وإدارة برنامج استمرارية تصريف الأعمال.

تولى المؤسسة تعيين شخص (يعرف باسم مدير استمرارية تصريف الأعمال) لإدارة برنامج استمرارية تصريف الأعمال. وينبغي أن تضمن المؤسسة أيضا التزام مدير برنامج استمرارية تصريف الأعمال وحصوله على الدعم من قبل الإدارة، بالإضافة إلى الحصول على الموازنات المعتمدة والمخصصة لإدارة استمرارية تصريف الأعمال. ويمكن أن يتولى مدير برنامج استمرارية تصريف الأعمال بدوره تشكيل فريق يتضمن محترفين من شعب العمل الفردية لإدارة برنامج استمرارية تصريف الأعمال.

يضطلع مدير أو فريق استمرارية تصريف الأعمال بالمسؤوليات التالية:

- تنظيم واعتماد برنامج إدارة استمرارية تصريف الأعمال (بالتشاور مع إدارة المؤسسة).
- إدارة أنشطة استمرارية تصريف الأعمال الملائمة داخل المؤسسة.
- دعم استمرارية تصريف الأعمال في أنحاء المؤسسة وخارجيا متى أمكن ذلك.
- إدارة موازنة إدارة استمرارية تصريف الأعمال.
- المحافظة على توثيق برنامج إدارة استمرارية تصريف الأعمال.
- إجراء البحوث حول وضع الاستعداد الحالي للمؤسسة والمستوى الذي يتطلبه التشريع واللوائح.
- تقديم التقارير حول وضع الاستعداد الحالي لإدارة المؤسسة بصفة منتظمة وتحديد موضع الفجوات المحددة.
- قد يحدد فريق إدارة استمرارية تصريف الأعمال (بالتشاور مع مديري الأعمال) ممثلي استمرارية تصريف الأعمال بإدارات العمليات أو بالمواقع الأخرى ويتولى تدريبهم من أجل:
  - القيام بدور نقطة اتصال في قضايا استمرارية تصريف الأعمال التي تؤثر على الإدارة أو الموقع.
  - مساعدة الإدارة في تحديد آثار التغيير في العمليات على استمرارية تصريف الأعمال.
  - إخطار فريق إدارة استمرارية تصريف الأعمال بالتغيير في العمليات.
  - المساعدة في أو قيادة عملية استعادة القدرة على العمل بالإدارة أو الموقع في حالة توقف العمل.

BC 2 يتم إعداد خطة استمرارية تصريف الأعمال لضمان استمرارية العمليات الرئيسية وتقديم الخدمات بالمستوى المقبول. وتتضمن هذه الخطة وتعتمد على الوقت المستهدف ومرحلة الاسترجاع المستهدفة لاستعادة القدرة على العمل فيما يتعلق بكل عملية من عمليات المؤسسة.

ينبغي أن تتبع المؤسسة إجراءً محددا عند إعداد خطة استمرارية تصريف الأعمال. وتتمثل الخطوة الرئيسية لإعداد خطة استمرارية تصريف الأعمال في إجراء تحليل أثر النشاط من أجل تحديد العمليات والوظائف الهامة للمؤسسة. ويعد التدريب امتدادا لتدريب تصنيف المعلومات الذي تجريه المؤسسة.

1- تحديد العمليات الرئيسية والقائمين على إدارتها داخل المؤسسة.
2- تحديد تبعيات العمليات: المعلومات والتطبيقات والأنظمة والشبكات وغيرها.
3- تحديد متطلبات التوافر. ويمثل هذا المرحلة "A" من الثلاثي C-I-A (السرية / السلامة / التوافر).
4- حساسية زمن توثيق العمليات الرئيسية. وعلى سبيل المثال: يعد شرط التوافر لتطبيق جدول الرواتب مرتفعا للغاية في نهاية الشهر، أثناء إعداد الرواتب.
5- تقييم الآثار الملموسة (المالية وغير المالية) وغير الملموسة الناجمة عن تعذر تشغيل كل وظيفة أو خدمة هامة.
6- تحديد الحد الأقصى المسموح به لتعطل العملية*.
7- تحديد المرحلة المستهدفة لاستعادة القدرة على العمل**.
8- حساب الوقت المستهدف لاستعادة القدرة على العمل بناءً على ما سبق.

ينبغي أن تستفيد المؤسسة من نتائج تحليل أثر العمل وتقييم المخاطر ونقاط الضعف في صياغة وتنفيذ خطة استمرارية تصريف أعمال تكنولوجيا المعلومات التي سوف تساعد على استمرار عمليات تكنولوجيا المعلومات الهامة وتقديم الخدمات الضرورية بمستوى مقبول في حالة تعطل العمل. وينبغي أن تهتم الخطة أيضا باستعادة مرافق وقدرات تكنولوجيا المعلومات لدى المؤسسة في حالة إخفاق تلك العمليات أو الخدمات.

تساعد نتائج تحليل أثر العمل، بالإضافة إلى نتائج تقييم المخاطر ونقاط الضعف (تقييم المخاطر)، المؤسسة في تطبيق الضوابط لضمان توافر العملية من خلال التخفيف من حدة المخاطر، وبالتالي، وضع خطة مناسبة لاستمرارية العمل .

* الحد الأقصى المسموح به لتعطل العمل: يتم تعريفه باعتباره المدة الزمنية التي تتعرض بعدها جدوى المنظمة (سواء المالية أو من خلال فقدان السمعة الطيبة) للمخاطر دون رجعة، في حالة عدم القدرة على تسليم منتج محدد أو خدمة محددة.

** الوقت المستهدف لاستعادة القدرة على العمل: يتم تعريفه باعتباره الإطار الزمني لاستعادة القدرة على العمل أو تقديم الخدمة عقب حدوث تعطل في العمل. وينبغي أن يكون الوقت المستهدف لاستعادة القدرة على العمل أقل من الحد الأقصى المسموح به لتعطل العمل.

** المرحلة المستهدفة لاستعادة القدرة على العمل: يتم تعريفها باعتبارها المرحلة التي ينبغي عندها استعادة المعلومات للمساعدة على إدارة النشاط بمجرد استئناف العمل.

BC 3 تشمل خطة استمرارية تصريف الأعمال سيناريوهات الكوارث وتتضمن أحكام استعادة القدرة على العمل في حالات الكوارث.

ينص كتيب تأمين المعلومات الوطنية على ضرورة أن تضع المؤسسة في الاعتبار أثناء إجراء تحليل أثر العمل السيناريوهات المختلفة لتعطل العمل، سواء كانت طفيفة أو حادة. وينبغي أن تتوقع خطة استمرارية تصريف الأعمال مجموعة متنوعة من الكوارث وأن تضع سبل حماية مشتركة لأكبر عدد ممكن من السيناريوهات.

BC 4 يتم الحفاظ على خطة استمرارية تصريف الأعمال وتحديثها لتعكس الوضع الحالي والمتطلبات الحالية وإتاحتها لجميع أعضاء الفريق.

ينبغي أن تضمن المؤسسة انعكاس وتحديث أي تغيير أو تحسين رئيسي في عملياتها أو بنيتها الأساسية ضمن خطة استمرارية تصريف الأعمال للمؤسسة. وينبغي أن تكفل أيضا اختبار جميع تلك التغييرات خلال الاختبار التالي المزمع إجراؤه بصفة منتظمة.

BC 5 يتم تخزين نسخة من الخطة المستحدثة لاستمرارية تصريف الأعمال بالإضافة إلى وسائط تخزين النسخ الإحتياطية للبيانات اللازمة والمعلومات بخزينة مقاومة للحرائق والعبث إلى جانب تخزين نسخة إضافية خارج موقع العمل. بحسب أفضل الممارسات يجب ان يبعد مركز البيانات الخارجي 25 كلم في منطقة مختلفة جغرافياً من مركز البيانات الرئيسي.

تضمن المؤسسة تأمين وتوزيع خطط استمرارية تصريف الأعمال بالصورة الملائمة.

تحتفظ المؤسسة بنسخ من خطة استمرارية تصريف الأعمال الخاصة بالمؤسسة وأي وثائق ومواد أخرى هامة ذات صلة في مكان آمن ومحدد سلفا بعيدا عن موقع العمل. وينبغي أن يحصل فريق العمل المحدد بقائمة مسؤولي الاتصال على معلومات حول ذلك المكان وأسلوب الوصول إليه.

ينبغي أن تضمن المؤسسة، حيثما يكون ذلك مناسبا، نقل مضمون خطة استمرارية تصريف الأعمال بالمؤسسة إلى المؤسسة الأخرى.

ينبغي أن تضع المؤسسة إجراءات لضمان توافر أحدث وسائل الدعم (وفقا لسياسة المؤسسة وبموجب الوقت المستهدف لاستعادة القدرة على العمل والمرحلة المستهدفة لاستعادة القدرة على العمل) بأحد الأماكن البعيدة عن موقع العمل.

BC 6 تحديد مواقع بديلة لاستعادة القدرة على العمل في حالات الكوارث، ويتم تحديد مدى جاهزيتها وفقا لمتطلبات الوقت المستهدف لاستعادة القدرة على العمل. وقد تكون هذه المواقع ساخنة/ دافئة/ باردة وفقا لمتطلبات المؤسسة.

بناءً على نتائج تحليل أثر العمل وعلى المتطلبات التنظيمية الأخرى، ينبغي أن تحدد المؤسسة حاجتها إلى موقع بديل. وينبغي أن يخضع اختيار موقع بديل لعوامل الوقت المستهدف لاستعادة القدرة على العمل والمرحلة المستهدفة لاستعادة القدرة على العمل.

الموقع الساخن:

يعد الموقع الساخن نسخة طبق الأصل من الموقع الأصلي للمنظمة يتضمن أنظمة حاسبات كاملة بالإضافة إلى دعم شبه كامل لبيانات المستخدمين. ويمكن استخدام التزامن في الوقت الفعلي بين الموقعين كي يعكس بيئة بيانات الموقع الأصلي بالكامل باستخدام روابط شبكية واسعة النطاق وبرمجيات متخصصة. وعقب توقف العمل بالموقع الأصلي، يتواجد الموقع الساخن كي تستطيع المنظمة الانتقال إلى تنفيذ العمليات الطبيعية دون تكبد أدنى خسائر. ويتم تشغيل الموقع الساخن، من الناحية المثالية، خلال ساعات أو أقل. وربما ينبغي انتقال العاملين إلى الموقع الساخن؛ ومن ثم، فمن الممكن تشغيل الموقع الساخن من منظور معالجة البيانات قبل انتقال العاملين إليه. وقد تكون قدرة الموقع الساخن متطابقة أو غير متطابقة مع قدرة الموقع الأصلي اعتمادا على متطلبات المنظمة. ويعد تشغيل هذا النمط من مواقع الدعم هو الأكثر تكلفة. وتعتبر المواقع الساخنة شائعة بين المنظمات التي تدير العمليات في الزمن الفعلي، مثل المؤسسة المالية والأجهزة الحكومية ومقدمي خدمات التجارة الإلكترونية.

الموقع الدافئ:

يعد الموقع الدافئ بمثابة موقع تستطيع المنظمة الانتقال إليه عقب توقف أو تعطل العمل ويكون مزودا بالفعل بأجهزة حاسابات مماثلة لأجهزة حاسبات الموقع الأصلي ولكنه لا يتضمن نسخ دعم للبيانات والمعلومات. وقد يحظى أو لا يحظى بنفس قدرات الموقع الأصلي اعتمادا على متطلبات المنظمة. وينبغي أن يتم استعادة البيانات على الأجهزة في ذلك الموقع قبل إمكانية بدء الأنشطة.

الموقع البارد:

يعد الوقع البارد أقل أنماط مواقع الدعم التي تتولى المنظمات تشغيلها من حيث التكلفة. ولا يتضمن نسخا احتياطية من البيانات والمعلومات الخاصة بالموقع الأصلي للمنظمة، كما لا يتضمن أجهزة منصبة بالفعل. ويساهم الافتقار إلى البرمجيات في خفض تكاليف بدء تشغيل الموقع البارد إلى حدها الأدنى، ولكنه يتطلب وقتا إضافيا عقب وقوع الكارثة لإدارة العمليات بقدرة تقترب بقدرة إدارة العمليات قبل وقوع الكارثة.

BC 7 النص على ضوابط قوية بالعقود تتضمن تعهيداً لجزء من أنشطتها أو مهام تكنولوجيا المعلومات أو خدمات استمرارية تصريف الأعمال الخاصة بها.

ينبغي أن تضع المؤسسة ضوابط قوية بعقود تكنولوجيا المعلومات تتضمن تعهيدا لجزء من أنشطتها أو مهام تكنولوجيا المعلومات أو خدمات استمرارية تصريف الأعمال. ويجب أن تدرس المؤسسة ما إذا كانت المخاطر المتعلقة بالحفاظ على بيانات الأجهزة تحول دون الاستعانة بأحد المتعاقدين في تنفيذ المهام التي يتم تعهيدها. وينبغي أن تشارك إدارة استمرارية تصريف الأعمال في توفير العاملين لتنفيذ عقود التعهيد.

ينبغي أن تتولى المؤسسة تقييم ما إذا كان لدى المتعاقدين الضوابط التالية لاستمرارية تصريف الأعمال:

أ. خطة استمرارية تصريف الأعمال استنادا إلى تحليل أثر العمل وتقييم المخاطر.

ب. اختبار خطة استمرارية تصريف الأعمال التي يتم ممارستها بصفة منتظمة.

ج. التأكيد على تقديم إخطار بانقطاع الخدمة بموجب اتفاقيات مستوى الخدمة.

BC 8 يتم اختبار خطة استمرارية تصريف الأعمال (Business Continuity Plan) بانتظام لمرة واحدة سنويا على الأقل أو عندما تطرأ تغييرات ذات اهمية في الأعمال التجارية أو المتطلبات القانونية / التنظيمية.

ينبغي أن تختبر المؤسسة خطة استمرارية تصريف الأعمال لمرة واحدة سنويا على الأقل. وكحد أدنى، ينبغي أن يكون الاختبار للسيناريو الأكثر احتمالا، بينما يتم إجراء اختبارات السيناريوهات الأقل احتمالا حسب الاقتضاء. وسوف يعتمد نمط وحجم الاختبار على مدى أهمية النشاط بدعم من تكنولوجيا وتعقد عملياته ومكوناته.

قد تتضمن اختبارات استمرارية تصريف الأعمال أي من أو جميع ما يلي:

تدريبات المحاكاة: تدريبات المحاكاة هي أحد أساليب اختبار خطة استمرارية تصريف الأعمال التي لا تؤثر تأثيرا كبيرا على العمليات اليومية. ويتولى أفراد فريق استمرارية تصريف الأعمال مراجعة ومناقشة الإجراءات التي يتخذونها حيال السيناريوهات المحددة لتوقف العمل وفقا لما هو محدد ضمن الخطط الخاصة بهم، ولكنهم لا يقومون بالفعل بأداء أي من هذه الإجراءات. ويمكن إجراء التدريب من خلال فريق واحد أو مجموعة من الفرق حسب الاقتضاء.

عمليات المحاكاة/ ورش العمل: يتم إعداد سيناريو الاختبار اعتمادا على الظروف الواقعية التي تضع في الاعتبار النشاط/ الموقع والمخاطر المحتملة. ويتم بعد ذلك مطالبة أعضاء الفريق بالتحدث عن الخطط (بموجب خطة استمرارية تصريف الأعمال) وأداء أدوارهم من أجل استعادة القدرة على العمل من خلال السيناريو.

اختبارات استعادة القدرة الجزئية على العمل: في هذا السيناريو، يتم دراسة سيناريو تعطل العمل وإجراء محاولة مباشرة لاستعادة القدرة على العمل. ومع ذلك، يتم اختبار جزء واحد فقط من العملية أو المهمة أو البنية الأساسية.

وفي بعض البدائل، قد يتضمن ذلك استعادة مهام وبنية رئيسية محددة وغير ذلك، وعادة ما يكون ذلك بعيدا عن موقع العمل دون التأثير على العمليات الفعلية.

اختبارات استعادة القدرة الكاملة على العمل: في هذا السيناريو، يتم دراسة توقف العمل؛ وعادة ما يتم استعادة النظام أو العملية أو البنية الأساسية بالكامل في موقع بديل بموجب الخطة المحددة لاستمرارية تصريف الأعمال. وعادة ما يتضمن ذلك تعبئة كاملة للقوى العاملة وتفويضات من الإدارة كما يتضمن مخاطر كبيرة مما يؤثر العمليات المعتادة. ومع ذلك، يعد نجاح هذا الاختبار بمثابة دليل حقيقي على فاعلية خطة استمرارية تصريف الأعمال التي وضعها الفريق.

BC 9 يتم توعية العاملين بخطة استمرارية تصريف الأعمال.

تبذل المؤسسة جهودا للتوعية باستمرارية تصريف الأعمال كجزء من برنامج التوعية الأمنية بالمؤسسة. وكحد أدنى، ينبغي أن يتناول برنامج التوعية ما يلي:

أ. تعريف جميع العاملين بأسباب وأهمية خطة استمرارية تصريف الأعمال.

ب. تعريف العاملين بأدوارهم ومسؤوليات وتوقعات المؤسسة في حالة حدوث أزمة أو تعطل العمل.

ج. توعية العاملين حول قنوات وعمليات الاتصال المختلفة التي سوف يتم استخدامها في حالة وقوع أزمة أو تعطل العمل. وعلى سبيل المثال: توضيح كيفية استخدام "شجرة الاتصالات" في التواصل مع الزملاء والوسائل البديلة للاتصال، مثل الهواتف التي تتصل بالأقمار الاصطناعية والاتصالات اللاسلكية وغير ذلك، حسبما يكون متاحا داخل المؤسسة.

10 - إرشادات حول تسجيل الأداء والمتابعة الأمنية [SM]

10-1 إرشادات حول السياسة والضوابط الرئيسية

SM 1 وضع مجموعة من الإجراءات والضوابط لضمان متابعة الوصول إلى المعلومات وحمايتها.

تكفل المؤسسة وجود إجراءات تنص على متابعة الوصول إلى المعلومات وحمايتها. وينبغي أن تحدد الإجراءات الأصول والعمليات التي ينبغي أن تتم متابعتها.

SM 2 إقرار ممارسات المتابعة وفقا لمدى أهمية البنية الأساسية. وينصح بتوفير متابعة لمدة 24 ساعة يوميا على مدار الأسبوع للبيانات، التطبيقات والبنيات الأساسية المصنفة C3 و I3 و A3 وضمان تخصيص مسؤوليات المتابعة وفقا لما تحدده الفقرة PS9 الفصل B-6 بعنوان "أمن العاملين" [PS].

ينبغي أن تكفل المؤسسة إقرار ممارسات المتابعة وفقا لأهمية المعلومات والعملية والبنية الأساسية. ويهدف ذلك إلى ضمان استهلاك موارد ملائمة في عملية متابعة الموارد والرقابة عليها.

ويؤكد كتيب تأمين المعلومات الوطنية أيضا على حقيقة أن تقسيم المسؤوليات أو مبدأ الرقابة من قبل شخصين ينبغي أن يكونا قائمين من أجل عملية المتابعة أيضا.

SM 3 أن يتماشى نشاط المتابعة مع الأطر الرقابية والقانونية مثل سياسة حماية البيانات والخصوصية المقرح ويشمل استخدام الأنظمة أو الوصول إليها.

ينبغي أن تكفل المؤسسة أن تتماشى جميع أنشطة المتابعة وتسجيل الأداء مع الأطر الرقابية والقانونية المتعددة. وينبغي أن تشمل المتابعة وتسجيل الأداء استخدام النظام والوصول إليه.

SM 4 تمكين الدخول على جميع أجهزة معالجة البيانات أو حماية المعلومات المصنفة وفقا لمستوى السرية C2 أو أكثر.

ينبغي أن تكفل المؤسسة أن يتم تزويد جميع أجهزة البيانات التي تحمي أو تعالج المعلومات المصنفة بمستوى السرية C2 وأكثر بإمكانية تسجيل الأداء.

SM 5 تصنيف جميع السجلات الأمنية بمستوى سرية C3، بينما يتم تصنيف سجلات التطبيقات والأنظمة وفقا لتصنيف السرية الخاص بالنظام.

ينبغي أن تكفل المؤسسة تصنيف السجلات الأمنية الخاصة بالنظام بمستوى سرية C3، بينما ينبغي أن تحظى سجلات التطبيقات والأنظمة بتصنيفات وفقا لمستوى السرية الخاص بالنظام. ويجب أن يتم تعريف ضوابط الوصول إلى النظام لضمان حماية السجلات الأمنية من إمكانية الوصول غير المصرح به أو العبث.

SM 6 أن تحظى السجلات التي تتضمن معلومات شخصية بالتدابير الملائمة لحماية الخصوصية وفقا لسياسات حماية البيانات والخصوصية المقترحة.

ينبغي أن تكفل المؤسسة حماية السجلات التي تتضمن معلومات شخصية بالصورة الملائمة بما يتماشى مع سياسة حماية البيانات والخصوصية.

SM 7 أن يتم الاحتفاظ بهذه السجلات لمدة تسعين يوما كحد أدنى، وكد اقصى يعتمد على القوانين واللوائح الخاصة بتلك بالقطاع ومدى اهمية تلك السجلات.

يتم الاحتفاظ بالسجلات لمدة تسعين يوما. وليس ضروريا أن تكون السجلات متاحة عبر الإنترنت من خلال النظام ويمكن الاحتفاظ بذات السجلات بالأرشيف أو إتاحتها دون الاتصال بشبكة الإنترنت. ومع ذلك، في حالة الاحتفاظ بالسجلات بالأرشيف أو دون الاتصال بشبكة الإنترنت، فلابد من وجود وسيلة للوصول إلى تلك السجلات بسهولة نسبية.

SM 8 أن يتم تسجيل الأحداث ذات الصلة لتوفير معلومات كافية تسمح بإعادة محاكاة الحوادث.

ينبغي أن تكفل المؤسسة الاحتفاظ بالسجلات المناسبة والملائمة داخل النظام للمساعدة على إعادة محاكاة الحوادث إذا لزم الأمر. ويكون ذلك هو الحال حينما يرى الإداريون ضرورة تعديل كمية السجلات الناجمة من خلال تسجيل أحداث أو إنذارات محددة فقط.

SM 9 أن يتم زيادة تقارير الاستثناء وفقا لسياسة التعامل مع الحوادث، كما هو محدد بالفصل B-8 بعنوان "إدارة الحوادث" [IM].

ينبغي أن تكفل المؤسسة تكامل العمليات بشكل جيد. وفي هذه الحالة، ينبغي دمج متابعة النظام مع التعامل مع الحوادث. ويجب أن يتم تسجيل الاستثناءات التي يتم رصدها بالنظام من خلال سجلات نظام المتابعة والإنذارات وغيرها واتخاذ الإجراءات من خلال عملية إدارة الحوادث. وقد يكون التكامل أو الدمج أتوماتيكيا أو يدويا.

11 - إرشادات حول حفظ وأرشفة البيانات [DR]

11-1 إرشادات حول السياسة والضوابط الرئيسية

DR 1 أن تحدد وتوثق فترات الاحتفاظ بالأصول المعلوماتية الهامة التي في حوزتها. وتخضع فترات الاحتفاظ بالبيانات كحد أدنى لما يلي:

أ- سياسات واحتياجات المؤسسة
ب- المتطلبات الرقابية والتنظيمية
ج- المتطلبات القانونية

يتمثل أحد التحديات الكبرى اليوم في تخزين البيانات والمدة الزمنية لتخزينها. وينص كتيب تأمين المعلومات الوطنية على صياغة سياسة تحدد فترة الاحتفاظ بالمعلومات التي يتم جمعها أو إصدارها أو حيازتها. ويجب أن تقرر المؤسسة فترة الاحتفاظ بالبيانات اعتمادا على العوامل المذكورة أعلاه بصفة رئيسية. وقد يكون هناك عوامل أخرى يمكن دراستها استنادا إلى المتطلبات الخاصة بالمؤسسة.

لابد من وجود إجراءات لتدمير المعلومات وفقا لسياسة تطهير الوسائط بالمؤسسة بمجرد الانتهاء من إمكانية استخدامها.

DR 2 أن يتم تخزين البيانات الواجب الاحتفاظ بها بما يضمن سريتها وسلامتها وإتاحتها وإمكانية الوصول إليها لأغراض مستقبلية محددة.

ينبغي أن تكفل المؤسسة التزام البيانات، التي يتم الاحتفاظ بها لأغراض العمل، بمتطلبات السرية والسلامة والتوافر الخاصة بتصنيف البيانات. ويجب ألا يتم تطبيق الضوابط على البيانات المتوفرة عبر شبكة الإنترنت فحسب، بل على البيانات التي يتم أرشفتها أو تخزينها دون الاتصال بشبكة الإنترنت بما يتماشى مع سياسة الأرشفة الخاصة بالمؤسسة.

DR 3 ألا يتم الاحتفاظ بالمعلومات الشخصية لفترة أطول مما هو ضروري بمقتضى سياسة حماية البيانات والخصوصية [IAP-NAT-DPRP].

يود كتيب تأمين المعلومات الوطنية إعادة التأكيد على أهمية الالتزام بالقوانين التي قد تسري على المعلومات التي تكون في حوزة المؤسسة. وينبغي أن يتم الاحتفاظ بالمعلومات الشخصية، التي تحتفظ بها المؤسسة، بمقتضى سياسة حماية البيانات والخصوصية [IAP-NAT-DPRP].

لابد من وجود إجراءات لتدمير المعلومات الشخصية بعدما لا يكون هناك أي ضرورة للاحتفاظ بها بما يتماشى مع سياسة حماية البيانات والخصوصية [IAP-NAT-DPRP].

DR 4 أن يكون لدى عمليات الدعم والأرشفة واستعادة القدرة على العمل إجراءات مقابلة تضمن الحفاظ على سلامة وسرية البيانات.

تحدد المؤسسة إجراءات العمل القياسية الخاصة بالدعم والأرشفة واستعادة المعلومات. ويتم توخي الحذر لضمان عدم تعريض سرية وسلامة البيانات لأي أخطار أثناء هذه العمليات. ويتم تفعيل الضوابط وفقا لأعلى تصنيف للبيانات المختزنة أو المعالجة أو المستعادة.

DR 5 أن تحتفظ البيانات الأرشيفية بعلامات التصنيف الخاصة بها وأن يتم تأمينها وفقا لذلك.

تعد عبارة "البعيد عن العين بعيد عن القلب" قولا مأثورا، ولكنه يبرز إلى حد ما طريقة تفكير العقل البشري. ومن المعتاد أن يميل خبراء التكنولوجيا إلى التركيز على البيانات الموجودة على شبكة الإنترنت والبيانات التي يتم استخدامها بصفة دائمة. ومع ذلك، ينبغي أن تكفل المؤسسة وجود ضوابط أمنية للبيانات التي يتم أرشفتها وإعداد نسخة احتياطية منها على الوسائط غير المباشرة أومواقع استعادة القدرة على العمل عقب الكوارث أو المناطق البعيدة عن موقع العمل وفقا لتصنيف المعلومات التي في حوزتها. وينبغي وضع العلامات المناسبة على كل تلك الوسائط وتأمينها وفقا لذلك. ولابد من وجود إجراءات تحدد كيفية وضع علامات على هذه الوسائط وكيف سيتم التعامل معها.

DR 6 أن يتم مراجعة أرشيف التكنولوجيا المطبقة لضمان ألا يكون قد عفا عليه الزمن والحفاظ على البيانات الأرشيفية في حالة تسمح باستعادتها بنجاح.

يتمثل أحد الاهتمامات الرئيسية أثناء أرشفة البيانات في الحفاظ على وثاقة الصلة بالتكنولوجيا. فقد خطت تكنولوجيا تخزين والوصول إلى البيانات خطوات هائلة على مدار العقود القليلة الماضية. وأفسحت شرائط البيانات الممغنطة الكبيرة المجال أمام وسائط DAT وDLT و CD و DVD وغير ذلك. ومن الضروري أن يتم ضمان الاحتفاظ بالبيانات أثناء دورة حياتها حتى يمكن الوصول إليها؛ وفي حالة السيناريوهات التي تغير بها المؤسسة التكنولوجيا المستخدمة، فلابد أن تضمن انتقال جميع البيانات ذات الصلة بالأرشيف بالصورة الملائمة إلى التكنولوجيا الجديدة.

12 - إرشادات حول التوثيق [DC]

12-1 إرشادات حول السياسة والضوابط الرئيسية

DC 1 إصدارسياسة أمنية للمؤسسة تتضمن متطلبات كتيب تأمين المعلومات الوطنية هذا.

تتولى المؤسسة إعداد سياسة لأمن المعلومات يتم تعديلها وفقا لاحتياجات ومتطلبات وأهداف المؤسسة وبما يتماشى مع سياسة تأمين المعلومات الوطنية.

تمثل سياسة تأمين الأجهزة الوطنية الأساس الرئيسي لتنفيذ نظام إدارة أمن المعلومات داخل المؤسسة.

DC 2 ضمان أن يحظى كل نظام تتقرر أهميته للمؤسسة بخطة/مواصفات أمنية. ويجب أن تكفل المؤسسة صياغة وتوثيق إجراءات الإدارة الأمنية حسب الاقتضاء.

ينص كتيب تأمين المعلومات الوطنية على أن تبذل المؤسسة العناية الواجبة في المحافظة على توثيق نظام المعلومات. وعلى مستوى أدنى، يتم تقييم كل نظام يحظى بأهمية لدى المؤسسة وتضمينه ضمن خطة أمنية.

تكفل المؤسسة، كحد أدنى، أن يتم تحديد العمليات الهامة وصياغة إجراءات العمل القياسية للحفاظ على تلك العمليات. ويجب أن تتضمن إجراءات العمل القياسية ضوابط أمن المعلومات المتفق عليها.

لا يهدف كتيب تأمين المعلومات الوطنية إلى توثيق كل عملية في صيغة كتابية شريطة أن يكون جميع العاملين (ذوي الصلة بالعملية) ملمين بالإجراءات وأن تكون هناك آلية لضمان تدفق ووصول المعارف إلى العاملين الجدد.

ومع ذلك، ينبغي أن تشير المؤسسة إلى أن الإجراءات الكتابية توفر قيمة كبيرة خلال حالات الطوارئ والكوارث.

DC 3 ضمان أن تتوافق معاييروإجراءات أمن النظام مع السياسات والأهداف الأمنية للمؤسسة.

يهدف كتيب تأمين المعلومات الوطنية إلى إعادة التأكيد على ضرورة أن تتماشى معايير وإجراءات أمن المعلومات بالمؤسسة مع السياسات والأهداف الأمنية للمؤسسة، التي يتعين بدورها أن تتفق مع كتيب تأمين المعلومات الوطنية.

سوف يكفل الالتزام باتباع الإعلان السابق توافق جميع العمليات مع سياسات وإجراءات المؤسسة وكتيب تأمين المعلومات الوطنية.

DC 4 تصنيف الوثائق الأمنية لتكنولوجيا الاتصالات والمعلومات بصورة افتراضية كحد أدنى C3/ محظور.

يتم تصنيف جميع الوثائق الأمنية لتكنولوجيا الاتصالات والمعلومات كحد أدنى C3/ محظور. ويتم تطبيق الضوابط الأمنية ذات الصلة وفقا لهذا التصنيف.

DC 5 فحص الوثائق بصورة دورية للتأكد من تحديثها وكونها موجودة وفي حالة جيدة.

تحظى المؤسسة بإجراءات محددة كجزء من منهجية إدارة الوثائق الخاصة بها من أجل إجراء فحص دوري لضمان تحديث وثائق تكنولوجيا الاتصالات والمعلومات وكونها في حالة جيدة.

تكفل المؤسسة أن تتضمن إجراءات إدارة التغيير أحكاما لتحديث وثائق النظام ذات الصلة كجزء من العملية.

تحظى الوثائق بدورة مراجعة محددة ينبغي المحافظة عليها كجزء من سمات إدارة الوثائق.

13 - إرشادات حول التدقيق وإصدار الشهادات [AC]

13-1 إرشادات حول السياسة والضوابط الرئيسية

AC 1 ضمان وضع برنامج للحوكمة وتحسين الأمن بما يتفق مع سياسة تصنيف المعلومات الوطنية وكتيب تأمين المعلومات الوطنية هذا. [IAP-NAT-DCLS]

تكفل المؤسسة وضع نظام لإدارة أمن المعلومات يتوافق مع سياسة تصنيف المعلومات الوطنية وكتيب تأمين المعلومات الوطنية المرفق.

تتولى المؤسسة تعيين مدير أمن المعلومات؛ وحيثما تكون المؤسسة منتشرة في العديد من المواقع الجغرافية وتكون هناك أصول معلوماتية هامة بمواقع نائية، يجوز أن يتم تعيين مدير محلي لأمن معلومات الموقع.

ومع ذلك، سوف يحتفظ مدير أمن المعلومات بالمؤسسة بجميع مسؤوليات أمن المعلومات.

تكفل المؤسسة ما يلي:

1- أن يكون مدير أمن المعلومات مؤهلا بالصورة المناسبة وأن يحظى بالخبرة المطلوبة والمتخصصة.
2- يحظى مدير أمن المعلومات بتصريح أمني من أجل الوصول إلى أعلى تصنيف للمعلومات المعالجة من قبل المؤسسة.
3- يحظى مدير أمن المعلومات بدعم وثقة وإمكانية الوصول إلى الإدارة العليا للمؤسسة.
4- لا يتولى مدير أمن المعلومات أي أدوار أو مسؤوليات أخرى متعارضة.
5- يقدم مدير أمن المعلومات التقارير، بصورة مباشرة، إلى رئيس المؤسسة أو مدير إدارة تدقيق الحسابات الداخلية.
6- في حالة تعهيد مهام أمن المعلومات، يظل مدير أمن المعلومات مستقلا عن الجهة التي تتولى تعهيد المهام.

AC 2 الالتزام بأحكام قوانين ولوائح الدولة ذات الصلة المعمول بها حاليا وتلك القوانين واللوائح التي يمكن تعديلها و/أو إضافتها في مرحلة زمنية لاحقة.

تلتزم المؤسسة بالأحكام المعنية من قوانين ولوائح الدولة المعمول بها حاليا وتلك التي يمكن تعديلها أو إضافتها في مرحلة زمنية لاحقة.

تكفل المؤسسة، بصفة خاصة، الالتزام بالقوانين التالية (* الحالية والجديدة المقترحة)

1- سياسة البنية الأساسية للمعلومات الهامة.
2- سياسة حماية البيانات والخصوصية.
3- قانون التجارة الإلكترونية.
4- قانون جرائم الإنترنت.

AC 3 أن تخضع للمراجعة والتدقيق من قبل جهة المصادقة أو أي هيئة مستقلة تحددها وزارة المواصلات والإتصالات بالدولة.

يتولى جهاز المراجعة والتدقيق بقطر المسؤولية عن مراجعة وتدقيق مدى التزام المؤسسة بسياسة تصنيف المعلومات الوطنية وكتيب تأمين المعلومات الوطنية. وبدلا من ذلك، يجوز أن يقوم جهاز المراجعة والتدقيق بقطر بتعيين مدققين آخرين مستقلين ومعتمدين لدى المؤسسة لإجراء عمليات المراجعة والتدقيق.

AC 4 ضمان إجراء مراجعة وتدقيق لنظام المعلومات الخاص بها (البنية الأساسية والأشخاص والعمليات) مرة واحدة سنويا على الأقل أو متى يتم إجراء تغيير قد يؤثر على أمن المؤسسة.

تسري عملية المراجعة والتدقيق التي يجريها جهاز المراجعة والتدقيق بقطر أو الهيئة لمدة عام واحد. وتتولى المؤسسة المسؤولية عن ضمان أن تكون معتمدة في جميع الأوقات. وهكذا يتم إجراء تدريب سنوي لمراجعة وتدقيق الوضع الأمني بالمؤسسة.

في حالة حدوث تغيير كبير يؤثر على البنية الأساسية أو الأشخاص أو العمليات، يتعين إعادة إجراء المراجعة والتدقيق من قبل جهاز المراجعة والتدقيق بقطر أو الهيئة.

AC 5 ضمان أن يشتمل نطاق عملية المراجعة والتدقيق على جميع الأصول المعلوماتية والأشخاص والعمليات.

ينبغي أن يكفل جهاز المراجعة والتدقيق بقطر أن يتضمن نطاق عملية المراجعة والتدقيق جميع الأصول المعلوماتية والأشخاص والعمليات.

ينص كتيب تأمين المعلومات الوطنية على أن تدرج المؤسسة جميع عناصر بنيتها الأساسية وعملياتها وأشخاصها كجزء من نطاقها؛ ومع ذلك، قد لا يكون من الحكمة أو الممكن إجراء الاعتماد الكامل من خلال محاولة واحدة. ورغم ذلك، لابد من تحريك العجلة لتحقيق الهدف النهائي.

يقدم جهاز المراجعة والتدقيق بقطر المشورة للمؤسسة حول كيفية وضع هدف محدد وقابل للقياس ويمكن تحقيقه ومحدد المدة الزمنية. تقدم المؤسسة، من جانبها، خارطة طريق إلى جهاز المراجعة والتدقيق بقطر من أجل تحقيق الالتزام الكامل.

AC 6 ضمان إعادة المصادقة حينما يؤدي أي تغيير أو أي نتائج جديدة إلى إثبات عدم صحة الاعتماد الحالي أو التشكك في صحته. وهناك حاجة إلى مصادقة كاملة للتغييرات الرئيسية التي تؤثر على التصميم الأمني الأساسي لأي نظام وهناك حاجة أيضا إلى اعتماد جزئي حينما يكون التغيير متوسطا أو يؤثر على اثنين أو أكثر من المتطلبات الأمنية.

في حالة حدوث تغيير كبير أو حادث أمني يؤثر على البنية الأساسية أو الأشخاص أو العمليات أو يبطل أو يتشكك في الاعتماد الحالي، فمن الضروري أن تتم مراجعة المصادقة من قبل جهة المصادقة بقطر أو الهيئة التي يحددها خلال الفترة الزمنية المحددة.

يتم تحديد زمن المراجعة من قبل جهة المصادقة بقطر بمجرد إخطاره بالتغيير. ويجب أن تكفل المؤسسة التعاون مع جهة المصادقة بقطر في حالة التغيير المخطط له و/أو إخطاره على الفور في حالة التغيير غير المخطط له أو الحادث الأمني.

AC 7 ضمان إصلاح أي تباينات خلال فترة زمنية محددة.

تكفل المؤسسة إصلاح أي تباينات تظهر خلال عمليات المراجعة والتدقيق وفقا لجدول زمني محدد. ويتولى جهاز المراجعة والتدقيق بقطر أو الهيئة التي يحددها المسؤولية عن ضمان إجراء المراجعة من قبل المؤسسة خلال الفترة الزمنية المحددة.

يتم تحديد المهلة الزمنية من قبل جهاز المراجعة والتدقيق بالدولة أو الهيئة التي يحددها من خلال التشاور مع المؤسسة.

AC 8 ضمان حصول المؤسسة على موافقة جهة المصادقة بالدولة على أي اعفاء تود القيام به.

تكفل المؤسسة أن تكون البنية الأساسية والأشخاص والعمليات جزءا من عملية المراجعة والتدقيق. وفي حالة الرغبة في الحصول على إعفاء، يتم إحالة الأمر إلى جهة المصادقة بالدولة مع تحديد نطاق الإعفاء وسببه وتحديد مخاطر الاستثناء والحصول على موافقة رئيس المؤسسة أو مدير إدارة المخاطر الداخلية.

تتخذ جهة المصادقة بقطر القرار بشأن الإعفاء ويوافق عليه بناءً على مدى الأحقية لحالة الإعفاء.

الفصل "ج"

1 - إرشادات حول أمن الاتصالات [CS]

1-1 أهداف السياسة

2-1 إرشادات حول السياسة والضوابط الرئيسية – تمديد الكابلات

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** القيام بما يلي:

CS 1 أن يتم استخدام أنابيب (قنوات أو مواسير أو مجاري) لحماية الكابلات من العبث أو التخريب أو الأضرار العرضية عند نقل البيانات المصنفة عند المستوى C4 أو أكثر. وينصح بهذه الضوابط فيما يتعلق بالبيانات المصنفة عند المستوى C2 أو أكثر.

يعد التصنت على المكالمات الهاتفية من بين الوسائل الأكثر شيوعا لسرقة المعلومات. وتصبح المهمة أيسر في حالة ترك الكابلات دون حماية أو تغطية. ويمكن أن تؤدي الضوابط الأساسية مثل تمديد الكابلات خلال القنوات أو المواسير أو المجاري إلى توفير الحماية للكابلات والمعلومات المتدفقة داخلها ضد العبث أو الإضرار (المتعمد أو العرضي) والخضوع لرقابة جهاز المراجعة والتدقيق بقطر. وينبغي أن تعتمد وسيلة الحماية المختارة على تصنيف المعلومات والتقييم المناسب للمخاطر.

ينص كتيب تأمين المعلومات الوطنية على فرض هذه الضوابط على المعلومات المصنفة عند المستوى C4 وينصح بها للمعلومات المصنفة عن المستوى C2.

CS 2 أن يتم استخدام شبكة تمديد كابلات مستقلة للأنظمة التي تتعامل مع المعلومات المصنفة عن المستوى C4 أو أكثر.

للحد من مخاطر التصنت على المكالمات الهاتفية، ينبغي أن تكفل المؤسسة وجود شبكة كابلات متخصصة لتوزيع المعلومات المصنفة عند المستوى C4 أو أكثر. ويتم إجراء ذلك من خلال ضوابط الوصول المناسبة (الوصول المادي ووصول فريق العمل).

CS 3 ألا يتم وضع علامات على الأنابيب المنصبة بالأماكن العامة أو أماكن الزوار بأسلوب يجتذب اهتمام لا داعي له من قبل أشخاص قد لا يكون لديهم تصريحات أمنية مناسبة أو لا ينبغي أن يعرفوا بوجود مثل هذه الكابلات.

يهدف كتيب تأمين المعلومات الوطنية إلى دعم مفهوم "تحقيق الأمن من خلال الغموض"، ولو كان ذلك على نطاق ضيق. ومن الحكمة أن تكفل المؤسسة قدرا من الغموض أثناء وضع العلامات على الكابلات والأنابيب، وخاصة في المناطق العامة أو مناطق الزوار، ما لم تكن خاضعة للرقابة والإشراف.

CS 4 أن تحتفظ بسجل للكابلات. وينبغي أن ينطوي السجل على الأقل على ما يلي:

أ. رقم تعريف الكابل
ب. التصنيف
ج. المصدر
د. المقصد
هـ. الرسم التخطيطي للموقع

ينص كتيب تأمين المعلومات الوطنية على احتفاظ المؤسسة بالوثائق المناسبة الخاصة بنقاط الشبكة (البيانات والصوت) في حوزتها. وتساعد الوثائق التفصيلية لنقاط الشبكة فريق الدعم على استكشاف مشكلات الشبكة وتحديد الأجهزة التالفة المتصلة بشبكات المؤسسة وتخطيط القدرة.

CS 5 فحص الكابلات للتعرف على أي تباين مع سجل الكابلات بصفة منتظمة.

تتولى المؤسسة صياغة الإجراءات لضمان اتساق الكابلات والنقاط المتصلة مع الوثائق الخاصة بها. ويساعد التدقيق/ الفحص المنتظم المؤسسة على تحديد الأجهزة التالفة المتصلة بشبكات المؤسسة والتلفيات التي قد تسبب تدهور خدمات الشبكة، ضمن أمور أخرى.

3-1 إرشادات حول السياسة والضوابط الرئيسية – الهواتف والفاكسات

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسة القيام بما يلي:

CS 6 إخطار المستخدمين بالحد الأقصى لمستوى التصنيف المسموح به فيما يتعلق بالمحادثات باستخدام كل من خطوط الهاتف الداخلية والخارجية، وفقا لما يحدده اختبار نظام الهاتف الداخلي ومستوى التشفير، إن وجد، بالخطوط الخارجية.

يعد التحدث بمثابة أحد السبل المحددة بالهندسة الاجتماعية لتسريب المعلومات. ويتحدث الأشخاص معا كوسيلة رئيسية للتواصل وتبادل الأفكار. وتعد أنظمة الهاتف (المحمول/ الخط الأرضي/ الهاتف المتصل بالأقمار الاصطناعية) أكثر الوسائط التكنولوجية التي يستخدمها الإنسان شيوعا للتغلب على عقبة المسافات. ورغم كونها وسيط فعال، إلا أنها تكون عرضة للمخاطر مثل التصنت على المكالمات الهاتفية وسوء الاتصالات (الأرقام الخاطئة) وإدارة الهوية (لا يمكنك التعرف على شخص على الجانب الآخر بأسلوب يمنع الخداع). ومن ثم، فمن الضروري أن تتولى المؤسسة تنفيذ الضوابط التي تتضمن توعية المستخدمين بالمستويات المصرح بها من المحادثات المصنفة واستخدام القنوات المشفرة وغير ذلك.

CS 7 ضمان تعطيل خاصية مكبر الصوت خلال المحادثات الهاتفية المسموعة/ المرئية، حيث من المحتمل أن يتم مناقشة المعلومات المصنفة عند المستوى C3 والاستماع إليها خلسة.

التأكد من أن العاملين على دراية بمخاطر استخدام أنظمة مكبر الصوت أو خاصية المحادثات الجماعية أثناء مناقشة المعلومات المصنفة. وقد يؤدي ذلك إلى تسريب المعلومات نتيجة للاستماع إليها خلسة. وإذا ما سمح موقف ما باستخدام تلك الوسائط، فلابد من وجود ضوابط لكتم الصوت من خلال المكاتب المانعة لتسريب الصوت.

CS 8 ضمان تعطيل خاصية تشغيل أجهزة المحادثات الجماعية عن بعد حيثما يتم تنصيبها في أحد المواقع الحساسة.

ينص كتيب تأمين المعلومات الوطنية على استحالة سرقة أو تخريب أجهزة المحادثات الجماعية عن بعد. وسوف يؤدي ذلك إلى التخفيف من حدة مخاطر القدرة على التجسس على المحادثات من خلال تشغيل أجهزة المحادثات الجماعية عن بعد.

ينبغي أن تدرس المؤسسة خيارات حظر استخدام الهواتف المحمولة في مثل تلك المواقع الحساسة، وخاصة حينما يتم مناقشة معلومات حساسة.

CS 9 ضمان عزل الغرف المخصصة لتبادل المواد الحساسة بالصورة الملائمة من أجل منع تسرب الصوت.

ينص كتيب تأمين المعلومات الوطنية على عدم الكشف عن المعلومات أثناء مناقشتها في الغرف المخصصة نتيجة لتسرب الصوت أو اختلاس السمع بصورة متعمدة أو غير متعمدة من قبل العاملين. ويمكن التخفيف من حدة تلك المخاطر إلى مستوى مقبول من خلال التأكد من تنفيذ ضوابط ملائمة، مثل استخدام المواد الكاتمة للصوت.

CS 10 ضمان تأمين أجهزة الفاكس لدى كلا الطرفين باستخدام أجهزة التشفير أثناء إرسال المعلومات المصنفة عند المستوى C2 أو أكثر.

ينص كتيب تأمين المعلومات الوطنية على ضرورة استخدام أجهزة التشفير لدى كلا الطرفين أثناء استعمال الفاكس في إرسال المعلومات المصنفة عند مستوى السرية C2 أو أكثر. ويهدف ذلك إلى التخفيف من حدة مخاطر التجسس عن طريق تشفير قنوات الإرسال.

CS 11 ضمان الوفاء بجميع معايير استخدام أجهزة الفاكس لدى كلا الطرفين عند مستوى التصنيف الواجب إرساله؛ ويجري المرسل الترتيبات للمستقبل كي:

أ. يجمع المعلومات من جهاز الفاكس بأسرع ما يمكن عقب استلامه.

ب. يخطر المرسل في حالة عدم وصول الفاكس خلال الفترة الزمنية المتفق عليها، على سبيل المثال: 10 دقائق.

ينص كتيب تأمين المعلومات الوطنية على أن يتولى العاملون بالمؤسسة المنوط بهم إرسال الفاكسات المسؤولية عن ضمان تطبيق جميع الضوابط الرئيسية للتأكد من سرية الإرسال. ويشمل ذلك ضمان الوفاء بجميع المعايير المعمول بها لدى كلا الطرفين، بما في ذلك استخدام أجهزة التشفير في إرسال المعلومات المصنفة عند المستوى C2 أو أكثر. وينبغي أن يقوم المرسل بإخطار المستقبل قبل إرسال الفاكس وترتيب إجراءات استلام الفاكس بأسرع ما يمكن. وينبغي أن يقوم المستقبل بدوره بإخطار المرسل في حالة عدم تسلم الفاكس في الوقت المحدد، على سبيل المثال: 10 دقائق.

2 - إرشادات حول أمن الشبكات [NS]

2-1 هداف السياسة

2-2 إرشادات حول السياسة والضوابط الرئيسية – إدارة الشبكات

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

NS 1 لا يتم الإفصاح عن تفاصيل الشبكة الداخلية وإعدادات النظام وخدمات الدليل ذات الصلة بالعاملين والأجهزة ووسائل التكنولوجيا الحساسة الأخرى أو إحصاؤها أمام جمهور العامة من قبل أشخاص غير مصرح لهم.

تتولى المؤسسة تصنيف الإعدادات ذات الصلة بالشبكة الداخلية والنظام وخدمات الدليل وغير ذلك، عند المستوى C2 كحد أدنى، أي "الوصول المحدود".

وتقوم بتطبيق الضوابط الكافية لضمان عدم الوصول إلى المعلومات من قبل أشخاص غير مصرح لهم. وقد يتضمن ذلك ضوابط لحماية محيط الشبكة، مثل الجدران النارية. ويتم تدمير النسخ الورقية والوثائق الإلكترونية لإعدادات أجهزة الشبكة والرسم التخطيطي للشبكة وغير ذلك، عند استبدالها أو عدم وجود حاجة إليها. وينبغي أن تلتزم المؤسسة بسياسة التخلص من البيانات/ الوسائط المنصوص عليها بكتيب تأمين المعلومات الوطنية أثناء التخلص من تلك المستندات.

يتم توعية العاملين/ فريق العمل الذي يتم تعهيد الأعمال إليه/ العاملين لدى الموردين بسياسات المؤسسة من خلال دورات التوعية الأمنية الملائمة.

NS 2 أن تلغي أو تعطل جميع الحسابات الافتراضية مثل (root) أو (admin) ...الخ أو أن تغير كلمة المرور وفقا لما هو محدد بالفصل C-6 بعنوان "أمن البرمجيات" [SS].

يتضمن النظام الأساسي لمراقبة الوصول ضوابط لتحديد وتوثيق المستخدم. ويوفر اسم المستخدم الهوية وتوثق كلمة المرور الهوية المزعومة. وعلى العكس من الكشف عن إمكانية الدخول على النظام، يحتاج المستخدم الخبيث أيضا إلى معرفة اسم المستخدم وكلمة المرور. ومن خلال ضمان تعطيل أو إلغاء أسماء المستخدم الافتراضية من النظام، يصبح من الصعب للغاية اختراق النظام من قبل المستخدم الخبيث.

في حالة استحالة القيام بذلك نتيجة للقيود التقنية، يتم تأمين حساب المستخدم من خلال كلمة مرور وفقا لما هو محدد بالفصل B-62 "أمن البرمجيات".

يتم مراجعة وتدقيق جميع أنشطة المستخدم من أجل تتبع الأنشطة المريبة والمشبوهة.

NS 3 يتم الاحتفاظ بإعدادات الشبكة تحت رقابة وسيطرة مدير الشبكة أو ما شابه وتخضع جميع التغييرات بالإعدادات إلى:

أ. التصديق من خلال عملية رسمية لمراقبة التغيير وفقا لما هو محدد بالفصل B-5 "إدارة التغيير" [CM].

ب. التوثيق والالتزام بسياسة أمن الشبكات والخطة الأمنية وفقا لما هو محدد بالفصل B-12 بعنوان "التوثيق" [DC].

ج. المراجعة المنتظمة. يتم الاحتفاظ بالإعدادات القديمة المتبعة وفقا لإجراءات المؤسسة كجزء من مراجعة التغيير، معدل تكرار المراجعة يعتمد على مخاطر وعمليات المؤسسة.

تحدد المؤسسة المسؤولية عن تشغيل وصيانة الشبكات. ويتم تعيين شخص كمدير للشبكة أو ما شابه بحيث يحظى بالمسؤولية عن تشغيل إدارة الشبكة.

يتولى مدير الشبكة الوصاية على جميع الإعدادات ذات الصلة بالشبكة. ويحتفظ بمستندات مستحدثة حول الشبكة بالكامل. وينبغي أن يتولى المسؤولية أيضا عن الإدارة الداخلية التي تتضمن تدمير النسخ القديمة لإعدادات الشبكة بخلاف تلك النسخ التي يتم الاحتفاظ بها لأسباب محددة، مثل التاريخ أو التحليل التقني أو النسخ الاحتياطية.

يتم اعتماد جميع التعديلات بإعدادات الشبكة من خلال عملية رسمية لمراقبة التغيير وفقا لما هو محدد بالفصل B-5 "إدارة التغيير".

يتولى مدير الشبكة المسؤولية عن ضمان التزام التغيير المقترح بسياسة أمن الشبكات والخطة الأمنية للمؤسسة وفقا لما هو محدد بالفصل B-12 "التوثيق".

يتولى مدير الشبكة مراجعة إعدادات الشبكة على فترات منتظمة.

NS 4 لكل شبكة خاضعة للإدارة، تحتفظ المؤسسة بما يلي:

أ. رسم تخطيطي رفيع المستوى يوضح جميع توصيلات الشبكة.

ب. رسم تخطيطي للشبكة المنطقية يوضح جميع أجهزة الشبكة.

ج. عمليات تحديث NS4 (أ) و(ب)، مع حدوث تغييرات بالشبكة.

د. وضع ملصق "حالي <بتاريخ>"على كل صفحة.

يهدف كتيب تأمين المعلومات الوطنية إلى إعادة التأكيد على أهمية الوثائق الكاملة والمستحدثة. وينص الكتيب على أن تحظى المؤسسة بالعمليات اللازمة للحفاظ على الوثائق وتوفر المشورة حول الوثائق التي ينبغي الحفاظ عليها.

NS 5 يتم تصميم وتهيئة الشبكات بحيث تحد من فرص الوصول غير المصرح إلى المعلومات التي تنتقل عبر البنية الأساسية للشبكة. وينبغي أن تستخدم المؤسسة التكنولوجيات التالية للوفاء بهذا الشرط:

أ. بدالات بدلاً من التوصيل المباشر.
ب. أمن منافذ قنوات سير البيانات على أجهزة التحويل للحد من إمكانية الوصول إلى المعلومات وتعطيل جميع المنافذ غير المستخدمة.
ج. أجهزة الراوتر والجدران النارية التي تعزل أجزاء الشبكة على أساس الحاجة إلى المعرفة.
د. أمن بروتوكول الإنترنت/ الإصدار 6 من بروتوكول الإنترنت.
هـ. التشفير على مستوى التطبيقات.
و. أداة آلية تقارن الإعدادات الحالية لأجهزة الشبكة بالإعدادات الموثقة.
ز. تقييد وإدارة إتصال مستخدمي النظام بشبكة المؤسسة من خلال عدة تقنيات متوفرة, متال: MAC Address Filtering.
ح. تفعيل انظمة منع الإختراق وكشف الإختراق بالشبكة.
ط. تقييد الدخول إلى الشبكة عن طريق السماح فقط بأيام وأوقات محددة.

يوفر كتيب تأمين المعلومات الوطنية ضوابط أمنية أساسية يتم تطبيقها على هيكل شبكات المؤسسة. وينبغي توخي العناية الواجبة من أجل ضمان تصميم وتهيئة الشبكات بحيث تحد من فرص الوصول غير المصرح إلى المعلومات أثناء انتقالها داخل الشبكة. ويحد التصميم والتطبيق من فرص اختلاس الحزم أو سرقة الجلسات أو التجسس على الشبكات أو غير ذلك.

NS 6 تتبنى شبكات الإدارة تدابير الحماية التالية:

أ. يتم استخدام الشبكة المخصصة لأجهزة الإدارة، أي تنفيذ شبكة محلية افتراضية VLAN مستقلة للإدارة أو بنية أساسية مادية مستقلة
ب. قنوات آمنة، على سبيل المثال: عن طريق استخدام الشبكات الافتراضية الخاصة VPNs و SSH ...الخ.

تكفل المؤسسة تطبيق الحد الأدنى من الضوابط المحددة من أجل تأمين شبكات الإدارة. ويتم إدارة الأجهزة من خلال قنوات داخل النطاق وخارج النطاق. وفي حالة القنوات داخل النطاق، تحدد تلك القنوات الفصل المنطقي من خلال الشبكات المحلية الافتراضية. ويتم تشفير جميع تلك القنوات بالصورة المناسبة، حيث تحمل معلومات سرية مثل اسم المستخدم وكلمات المرور التي تحظى بامتيازات إدارية ومعلومات تخضع للمراقبة والمعاينة من قبل المنافذ الأخرى وغير ذلك.

3-2 إرشادات السياسة والضوابط الرئيسية – الشبكات المحلية الافتراضية VLAN

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسة أن تكفل ما يلي:

NS 7 في الشبكات الهامة والأساسية يتم استخدام الشبكات المحلية الافتراضية لفصل وتحديد مرور هواتف بروتوكول الإنترنت.

يوصي كتيب تأمين المعلومات الوطنية بتطبيق الضوابط الأساسية، مثل استخدام الشبكات المحلية الافتراضية، في الفصل بين مرور البيانات وغير البيانات (الصوت، الصورة) داخل شبكة المؤسسة. ويتطلب مرور الصوت جودة محددة للخدمة من أجل تأمين مرور الصوت من سلسلة مرور البيانات التي ينبغي إعدادها للتشغيل في الشبكة المحلية الافتراضية المستقلة من خلال جودة محددة للخدمة. ويؤدي الفصل في المرور أيضا إلى الحفاظ عليه من الهجمات المحتملة على الشبكة المحلية.

NS 8 أن يُمنح حق الدخول الإداري خلال الشبكة المحلية الافتراضية ذات التصنيف الأعلى إلى شبكة أخرى تحظى بنفس مستوى التصنيف أو تصنيف أقل.

يتم تهيئة إعدادات الشبكة كحد أدنى لمستوى تصنيف المعلومات C2. وينص كتيب تأمين المعلومات الوطنية على ضرورة أن يتم الوصول لإدارة البدالات إلى البدالات (مما يعني بالفعل الوصول إلى إعدادات الشبكة) من خلال الشبكة المحلية الافتراضية التي تحظى بنفس مستوى التصنيف أو مستوى أعلى. وسوف يضمن ذلك وجود الضوابط المناسبة للوصول إلى هذه المعلومات.

NS 9 تنفيذ جميع التدابير الأمنية التي تنصح بها عملية تقييم المخاطر في المؤسسة وإرشادات التأمين الصادرة عن مورد أجهزة البدالات.

ينص كتيب تأمين المعلومات الوطنية على تقوية أجهزة التحويل بالشبكات (عملية تأمين نظام التشغيل وإعدادات جهاز التحويل) وفقا لأفضل الممارسات التي يوصي بها المورد. وعلاوة على ذلك، يتم تطبيق الضوابط الأمنية الإضافية التي تنصح بها عملية تقييم المخاطر بالمؤسسة.

NS 10 ألا يتم استخدام مراكز تحويل البيانات بأجهزة التحويل التي تدير الشبكات المحلية الافتراضية للتصنيفات المختلفة.

ينص كتيب تأمين المعلومات الوطنية على عدم استخدام مراكز تحويل البيانات بأجهزة التحويل التي تدير الشبكات المحلية الافتراضية للتصنيفات المختلفة من أجل منع الكشف المحتمل عن المعلومات.

4-2 إرشادات حول السياسة والضوابط الرئيسية – الأجهزة متعددة الوظائف (MFDs)

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

NS 11 ألا يتم استخدام الأجهزة متعددة الوظائف المتصلة بالشبكة لنسخ الوثائق المصنفة أعلى من مستوى الشبكة المتصلة.

ينص كتيب تأمين المعلومات الوطنية على أن تقوم الأجهزة متعددة الوظائف المتصلة بالشبكة بمعالجة المعلومات المصنفة عند مستوى تصنيف اتصالها بالشبكة أو أقل من ذلك المستوى. وعلى سبيل المثال، إذا تم تصنيف أي شبكة تحمل المعلومات المصنفة عند المستوى C2، فلا يمكن أن تقوم الأجهزة متعددة الوظائف المتصلة بتلك الشبكة بمعالجة أي معلومات مصنفة عند المستوى C3.

NS 12 حيثما يكون لدى الأجهزة متعددة الوظائف المتصلة بالشبكة القدرة على نقل المعلومات عبر بوابة ما إلى شبكة أخرى، يتعين على المؤسسة أن تكفل ما يلي:

أ. أن يطبق كل من الأجهزة متعددة الوظائف مهام تعريف المستخدم والتوثيق والتدقيق على جميع المعلومات التي ينقلها المستخدمون من خلال تلك الأجهزة متعددة الوظائف.

ب. أن تكون هذه الآليات تماثل من حيث القوة تلك الآليات اللازمة لمحطات العمل بتلك الشبكة.

ج. يمكن أن تحدد البوابة المعلومات وتتولى تنقيتها وفقا للمتطلبات الخاصة بتصدير البيانات.

ينص كتيب تأمين المعلومات الوطنية على وجوب أن تطبق جميع الأجهزة متعددة الوظائف المتصلة بالشبكة، والتي تحظى بالقدرة على نقل المعلومات عبر بوابة ما إلى شبكة أخرى، الحد الأدنى للضوابط المنصوص عليها بكتيب تأمين المعلومات الوطنية.

تعد الضوابط المنصوص عليها مماثلة لتلك الضوابط المطبقة على محطة عمل المستخدم وتتضمن هوية المستخدم والتوثيق وأسلوب المراجعة والتدقيق. وينبغي أن تحظى كلمات المرور المستخدمة بقوة كافية بمقتضى الفصل 9-3 بعنوان "إدارة الوصول إلى المعلومات" بكتيب تأمين المعلومات الوطنية. وتعد الأجهزة متعددة الوظائف، بصفة رئيسية، بمثابة أجهزة مشتركة بالشبكة؛ ومن ثم، فمن الضروري تحديد القائمين على إدارة المهام فيما يتعلق بالمعلومات التي تتولى الأجهزة متعددة الوظائف معالجتها. وفي حالة وقوع أي حادث، فمن الضروري أن يتم نسب الخرق إلى شخص ما. وسوف توفر مهام التوثيق والتدقيق الأدوات اللازمة لتسوية مثل هذا الخرق.

ينبغي أن يتم تنقية المضمون لتحديد وترشيح البيانات وفقا لمتطلبات تبادل المعلومات. وينبغي أن يتم وضع العلامات على البيانات وفقا لتصنيف الوثائق الخاصة بها.

NS 13 لا يوجد اتصال مباشر من أي من الأجهزة متعددة الوظائف بشبكة هاتف ذات تصنيف أقل ما لم يتم تقييم الجهاز متعدد الوظائف ويتضمن نطاق التقييم ما يلي:

أ. مهام التحكم في تدفق المعلومات لمنع تدفق البيانات غير المتعمد وغير المصرح به.
ب. ضوابط تصدير البيانات القادرة على حصر المعلومات بناءً على تصنيف المعلومات.
ج. التوثيق وإصدار وحماية بيانات التدقيق.

ينص كتيب تأمين المعلومات الوطنية على عدم اتصال الأجهزة متعددة الوظائف بشبكات الهاتف المصنفة بمستوى سرية أقل من تصنيف المعلومات التي يتم معالجتها من قبل الأجهزة متعددة الوظائف. ويهدف ذلك إلى منع تسرب المعلومات الذي قد يحدث عن طريق نقل المعلومات المصنفة على شبكة لا تحظى بضوابط كافية.

يمكن توفير التوصيلات بموجب عملية تقييم تكفل وجود ضوابط كافية داخل الأجهزة متعددة الوظائف من أجل التحكم في تدفق البيانات اعتمادا على تصنيف المعلومات.

NS 14 أن تتولى نشر الأجهزة متعددة الوظائف عقب وضع مجموعة من السياسات والخطط والإجراءات التي تحكم استخدام الأجهزة.

ينبغي أن تضع المؤسسة مجموعة محددة من السياسات والإجراءات التي تحكم استخدام الأجهزة متعددة الوظائف داخل المؤسسة و/أو شبكاتها. ويجب أن تحدد السياسات الضوابط التقنية والإدارية والتشغيلية.

وفيما يلي نستعرض بعض الضوابط الأمنية الإدارية والتقنية من أجل وضعها في الاعتبار:

<u>الضوابط الإدارية والتشغيلية</u>

1- توعية المستخدمين بشأن استخدام وحماية الأجهزة متعددة الوظائف بالصورة الملائمة.
2- تنفيذ الضوابط الكافية للأمن المادي ضد السرقات.
3- إجراء عملية تقييم دوري لمخاطر أمن تكنولوجيا المعلومات تشمل استخدام الأجهزة متعددة الوظائف في بيئة حاسبات المؤسسة.

<u>الضوابط التقنية</u>

1- تشغيل خاصية توثيق المستخدم/ حماية كلمة المرور بالأجهزة متعددة الوظائف من أجل الحماية من الاستخدام غير المصرح به.
2- تشفير البيانات المصنفة قبل نقلها.

3- تعطيل خدمات الشبكة غير الضرورية، مثل منافذ الأشعة تحت الحمراء والبلوتوث من أجل تجنب الكشف عنها باعتبارها نقاط هجوم.

NS 15 ألا يتم الاحتفاظ بالمعلومات المصنفة عند المستوى C1 أو أكثر بصفة دائمة بالأجهزة متعددة الوظائف. حيثما تحظى الأجهزة متعددة الوظائف بخصائص لجدولة المهام، تبقى الضوابط أو الإعدادات اليدوية/ الأوتوماتيكية الكافية قائمة لإلغاء المعلومات من ذاكرتها بمجرد انتهاء المهمة.

نظرا لأن الأجهزة متعددة الوظائف هي أجهزة مشتركة في الأساس، ينبغي ألا يتم الاحتفاظ بأي معلومات مصنفة عند المستوى C1 أو أكثر بصفة دائمة بتلك الأجهزة متعددة الوظائف. ويجب أن تتوافر الضوابط لإخلاء الذاكرة من المهام المكتملة وأي معلومات متصلة بها قد تساعد في إعادة معالجة أو عرض المعلومات. ويهدف ذلك، في الأساس، إلى ضمان الحيلولة دون سرقة البيانات.

NS 16 تلتزم الأجهزة متعددة الوظائف بالإجراءات المحددة بالفصل C 8-3 بعنوان "السياسة والضوابط الرئيسية – تطهير الوسائط".

يتم حذف جميع البيانات المختزنة بالأجهزة متعددة الوظائف عقب استكمال المهمة. وفي حالة حاجة الأجهزة متعددة الوظائف للإصلاح (خارج المكتب) أو في حالة إخراجها من الخدمة، يتم التعامل مع وسائط التخزين وفقا لإجراءات تطهير الوسائط الموصى بها. ويمكن أن تضع المؤسسة في الاعتبار الضوابط/ الإجراءات، مثل ضمان مصاحبة الفنيين العاملين لدى المورد أثناء إصلاح الأجهزة بموقع العمل.

5-2 إرشادات حول السياسة والضوابط الرئيسية – خوادم أسماء النطاقات (DNS)

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسة أن تكفل ما يلي:

NS 17 أن يتم تأسيس خادم داخلي مستقل لأسماء النطاقات داخل الشبكة الداخلية من أجل معلومات النطاق الداخلي التي لا يتم الإفصاح عنها على شبكة الإنترنت.

ينص كتيب تأمين المعلومات الوطنية على عدم الإفصاح عن معلومات بروتوكول الإنترنت الداخلية الخاصة بالشبكات لجمهور العامة. ويكفل فصل خادم أسماء النطاقات لتسوية بروتوكول الإنترنت الداخلي والخارجي عدم الإفصاح عن معلومات بروتوكول الإنترنت ذات الصلة بالشبكات الداخلية أو الوصول إليها من خلال الشبكات الخارجية.

NS 18 أن يكون لمعلومات خادم أسماء النطاقات التي يتعين الإعلان عنها خادم محلي مضيف وآمن (خادم حصين) أو أن تستخدم تلك المعلومات خادم أسماء النطاقات الحكومي الذي يمثل جزءا من الشبكة الحكومية مثل خادم أسماء النطاقات الرئيسي.

يعد خادم أسماء النطاقات مكونا أساسيا بالشبكة ويتولى المسؤولية عن رسم تفاصيل أسماء المضيف بعناوين بروتوكول الإنترنت. وينص كتيب تأمين المعلومات الوطنية على تأمين ومراقبة هذا المكون الهام بالصورة الملائمة. ويؤكد الكتيب على الحاجة على إدارة واستضافة الخدمات محليا في خادم آمن (متصلب/ حصين) أو استخدام خادم أسماء النطاقات الحكومي. وبدلا من ذلك، يمكن أيضا أن يتم إعداد خادم أسماء النطاقات الحكومي كخادم احتياطي لأسماء النطاقات.

NS 19 أن يتم نشر خوادم أسماء النطاقات لضمان عدم وجود نقاط إخفاق أثناء الخدمة وأن تكون مدعمة أمنيا وأن يتم الحفاظ على الأمن بصورة استباقية.

ينص كتيب تأمين المعلومات الوطنية على دراسة عوامل تصميم الأمن الكافي والتوافر الهائل أثناء تصميم خدمات خوادم أسماء النطاقات. وينبغي أن تتم متابعة الخدمات الهامة، مثل خادم أسماء النطاقات، بصورة استباقية وتأمينها بموجب أفضل ممارسات الصناعة الموصى بها.

NS 20 أن يتم توقيع ملفات النطاق رقميا وتوفير توثيق التشفير المتبادل وسلامة بيانات التحويل بين النطاقات والتحديثات الديناميكية.

يوصي كتيب تأمين المعلومات الوطنية بتطبيق الضوابط الأمنية، مثل التوقيع الرقمي وتوثيق التشفير لملفات النطاق، من أجل ضمان سلامة وسرية البيانات الموجودة بأي من خوادم أسماء النطاقات.

NS 21 أن يتم تأمين توثيق وسلامة أصل التشفير لبيانات خادم أسماء النطاقات.

يوصي كتيب تأمين المعلومات الوطنية بتطبيق الضوابط الأمنية، مثل تأمين توثيق وسلامة أصل التشفير، من أجل ضمان سلامة وسرية البيانات الموجودة بأي من خوادم أسماء النطاقات.

NS 22 أن يتم توفير خدمات خادم أسماء النطاقات، بما في ذلك تحويل المناطق، إلى الأشخاص المصرح لهم فقط.

يوصي كتيب تأمين المعلومات الوطنية بتطبيق الضوابط الأمنية، مثل قصر تحويل المناطق على الأشخاص المصرح لهم فقط،، من أجل ضمان سلامة وسرية البيانات الموجودة بأي من خوادم أسماء النطاقات.

NS 23 مهام التشفير ذات الصلة بـNS 20 و NS 21 أعلاه، واستخدام وحدة أمن الأجهزة لكل من الإدارة الرئيسية والمعالجة التشفيرية وفقا لما هو محدد بالفصل C-10، بعنوان "أمن التشفير" [CY].

ينص كتيب تأمين المعلومات الوطنية على التزام مهام التشفير ذات الصلة بـNS 20 و NS 21 بالمتطلبات المحددة بالفصل C-10، بعنوان "أمن التشفير".

6-2 إرشادات حول السياسة والضوابط الرئيسية – أمن شبكة الإنترنت

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

NS 24 أن يتم فحص والتحقق من جميع البرامج والملفات التي يتم تنزيلها من شبكة الإنترنت للتحقق من خلوها من البرامج الضارة، بما في ذلك آليات مسح حركة مرور HTTP.

ينبغي أن تكفل المؤسسة وجود ضوابط أمنية لمسح البيانات التي يتم تنزيلها من شبكة الإنترنت. ويجب أن يتم مسح جميع البرامج والملفات للتأكد من خلوها من البرامج الضارة، وعلى سبيل المثال الفيروسات وبرامج التجسس وطروادة وغيرها. وينبغي أن يكون هناك آليات، مثل بوابات تنقية المضمون، من أجل مسح حركة مرور الويب، مثل HTTP و FTP وغيرها. وينبغي أن يتم النظر في الحد من التنزيلات اليومية أو الحظر المشدد على التنزيلات الخاصة بالأدوار والأنظمة المحددة.

NS 25 أن ترفض بوابة شبكة الإنترنت جميع خدمات الإنترنت ما لم تكن مفعلة بصفة خاصة.

ينبغي أن تكفل المؤسسة دعم وتأمين بوابات شبكة الإنترنت من خلال رفض جميع الخدمات بصفة ضمنية باستثناء تلك الخدمات المفعلة والمسموح بها.

NS 26 أن يتم تهيئة وتحديث برامج تصفح الويب العاملة على محطة عمل المستخدم بصورة سليمة.

وينبغي أن تراجع المؤسسة الإرشادات التالية عند تهيئة برامج تصفح الويب:

أ. **تعطيل أي من خيارات المحتوي النشط، مثل Java وJavaScript وActiveX ضمن تطبيق/ متصفح البريد الإلكتروني، باستثناء حالة التواصل مع مصدر موثوق.**
ب. **استخدام إصدارات حديثة للمتصفح وتطبيق أحدث الإجراءات الأمنية.**
ج. **تعطيل خصائص الاستكمال التلقائي/ تذكر كلمة المرور.**
د. **تفعيل خصائص منع البرامج التي تنشأ فجأة، باستثناء حالة التواصل مع المواقع الموثوقة.**
هـ. **إلغاء الملفات المخفية أو الملفات المؤقتة لبرامج التصفح من أجل حماية خصوصية البيانات.**
و. **تعطيل التنصيب التلقائي لبرامج التوصيل أو الإضافات أو البرامج.**

مع تزايد الاعتماد على برامج الويب بشبكة الإنترنت ووالتطبيقات القائمة على الويب، تعتبر برامج تصفح الويب أحد أكثر التطبيقات المستخدمة شيوعا. ويوفر كتيب تأمين المعلومات الوطنية إرشادات إلى المؤسسة حول كيفية تأمين برامج تصفح الويب من أجل التخفيف من حدة المخاطر ذات الصلة بنقاط الضعف في برامج تصفح الويب.

NS 27 أن يكون لديها القدرة اللازمة لمتابعة حركة مرور البيانات واستنتاج أنماط حركة البيانات والاستخدام وغير ذلك. انظر الفصل B-10 بعنوان "تسجيل الأداء والمتابعة الأمنية" [SM] للتعرف على المزيد من المعلومات.

ينبغي أن تكفل المؤسسة وجود ضوابط مناسبة لمتابعة حركة المرور واستنتاج الأنماط والاستخدام وغير ذلك بما يتفق مع الفصل B-10 بعنوان "تسجيل الأداء والمتابعة الأمنية". ومع ذلك، تخضع تلك الضوابط لسياسات وإجراءات المؤسسة لضمان الاستخدام العادل للتكنولوجيا. ولا يتم استخدام الضوابط الأمنية في التطفل على خصوصية المستخدم، بل في ضمان التزام استخدامات المستخدم بالسياسات والإجراءات المحددة.

7-2 إرشادات حول السياسة والضوابط الرئيسية – أمن البريد الإلكتروني

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

NS 28 أن يتم دعم خوادم البريد الإلكتروني وفقا لأفضل الممارسات وتهيئتها لتكون خوادم حصينة. وينبغي أن يتم تجنب المعلومات التي تكشف عن التفاصيل المحددة للأنظمة الداخلية أو الإعدادات ضمن عناوين البريد الإلكتروني، إذا كان ذلك مجديا من الناحيتين التقنية والتشغيلية، من أجل تجنب الإفصاح عن المعلومات الخاصة بالنظام إلى الأطراف الخارجية.

ينبغي أن تكفل المؤسسة دعم وتهيئة خوادم البريد الإلكتروني الخاصة بها لتكون خوادم حصينة والالتزام بأفضل الممارسات التي توصي بها الصناعة والمورد. ويوفر كتيب تأمين المعلومات الوطنية إرشادات لضمان حماية حوادم البريد الإلكتروني من الهجمات الاستطلاعية من خلال ضمان ألا تكشف عناوين البريد الإلكتروني عن معلومات تقنية (تكنولوجيا، إصدار، غير ذلك) حول الخادم.

NS 29 أن يتم استخدام حماية TLS مع خادم البريد SMTP بما يتماشى مع الفصل C-10 بعنوان "أمن التشفير" [CY].

ينص كتيب تأمين المعلومات الوطنية على التزام مهام التشفير ذات الصلة بحماية TLS بالمتطلبات المحددة بالفصل C-10 بعنوان "أمن التشفير".

NS 30 أن تقوم بتنفيذ إطار سياسة مرسل البريد الإلكتروني (SPF) [RFC4408]. وينبغي على المؤسسة أن ترسل أو تعيد رسائل البريد الإلكتروني المرتدة أو التي لم يتم تسلمها إلى المرسلين الذين يمكن التحقق منهم عن طريق إطار سياسة مرسل البريد الإلكتروني.

ينصح كتيب تأمين المعلومات الوطنية بالالتزام بإطار سياسة المرسل **(SPF) [RFC4408]** لمكافحة تهديد رسائل البريد الإلكتروني غير المرغوب فيها.

NS 31 أن يتم تأمين قوائم توزيع البريد الإلكتروني الداخلية لمنع وصول الأطراف الخارجية إلى المعلومات من أجل الحد من مخاطر رسائل البريد الإلكتروني غير المرغوب فيها.

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بتطبيق ضوابط فعالة لتجنب مخاطر رسائل البريد الإلكتروني غير المرغوب فيها. ويجب أن تكفل سياسة البريد الإلكتروني خضوع وقصر استخدام قائمة توزيع البريد الإلكتروني على الاستخدام الداخلي. وينبغي ألا تستطيع الكيانات الأخرى الخارجية التعامل مع قائمة التوزيع تلك.

وبالإضافة إلى ذلك، ينبغي أن تقتصر أنماط الرد التلقائي على البريد الإلكتروني (مثل "خاصية التواجد خارج المكتب") على أدوار محددة فقط من أجل الحد من انتشار رسائل البريد الإلكتروني الضارة، مثل رسائل البريد الإلكتروني غير المرغوب فيها والاحتيالية وغير ذلك.

NS 32 أن يتم استخدام بوابات البريد الإلكتروني لمسح جميع رسائل البريد الإلكتروني الواردة والصادرة لضمان التزامها بالسياسة الأمنية للمؤسسة وخلوها من أي برمجيات ضارة.

ينبغي أن تكفل المؤسسة وجود ضوابط أمنية لمسح حركة مرور رسائل البريد الإلكتروني الواردة والصادرة. ويجب مسح جميع البيانات للتحقق من خلوها من البرامج الضارة، مثل الفيروسات وبرامج التجسس وفيروس طروادة وغيرها. وينبغي أن يكون هناك آليات، مثل بوابات تنقية المضمون، لضمان التزام حركة مرور SMTP بالسياسة الأمنية للمؤسسة.

8-2 إرشادات حول السياسة والضوابط الرئيسية – الأمن اللاسلكي

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

NS 33 حيثما يتم استخدام الشبكات المحلية اللاسلكية، ينبغي استخدامها من خلال تدابير كافية لتوثيق المعلومات وتشفير نقلها، إضافة إلى الاستعانة بعمليات وممارسات سليمة لإدارة الأمن.

تعد الشبكة المحلية اللاسلكية أحد أنماط الشبكات المحلية التي تستخدم الموجات اللاسلكية عالية التردد بدلا من الأسلاك في الاتصال بين الأجهزة. ومن ثم، يصبح من السهل للغاية أن يتجسس المستخدمون الخبيثون على مثل تلك الشبكات.

تعتمد الشبكات المحلية اللاسلكية على مواصفات IEEE 802.11. وقد تم وضع مواصفات IEEE 802.11 للمهام الأمنية اللاسلكية الخاصة التي تعمل من خلال IEEE 802.1X.

ينبغي أن تكفل ألمؤسسة وجود آليات كافية للرقابة الأمنية عند استخدام الشبكات المحلية اللاسلكية من أجل تأمين الوصول إلى المعلومات. وتتضمن الضوابط الأمنية السياسات والإجراءات الموثقة التي تحكم ذلك الاتصال وتقدم المشورة بشأنه.

وينبغي أن يتم استخدام الضوابط التقنية، مثل تحديد الهوية والتوثيق القوي واستخدام التشفير، ضمن أمور أخرى.

NS 34 أن يتم إستخدام بروتوكولات الأمن اللاسلكية الأكثر قوة، مثل WPA2 و EAP-TLS؛ ومع ذلك، ينبغي ألا يتم الاعتماد على تلك البروتوكولات الأمنية اللاسلكية وحدها لحماية سرية وسلامة البيانات. وتتولى المؤسسة نشر شبكة افتراضية خاصة آمنة على الشبكات اللاسلكية في حالة تبادل البيانات المصنفة C3 أو أكثر عبر الشبكات اللاسلكية. ولا يتم تنفيذ WEP باعتبارها تكنولوجيا أمنية ثبت ضعفها داخل أي شبكة حكومية.

ينبغي أن تكفل المؤسسة مراجعة التكنولوجيا بصفة مستمرة. ويجب أن تتولى تطبيق البروتوكولات التي تم اختبارها وثبتت سلامتها. ويوصى حاليا بتطبيق بروتوكولات WPA2 و EAP-TLS. ومع ذلك، ينبغي ألا تعتمد المؤسسة بصفة أساسية على البروتوكول لحماية سرية وسلامة البيانات. وينبغي أن يتم نشر ضوابط أمنية إضافية، مثل الشبكات الافتراضية الخاصة الآمنة.

NS 35 أن يتم الاحتفاظ بقائمة سليمة لجميع الأجهزة ذات الواجهة اللاسلكية. وبمجرد الإبلاغ عن فقدان جهاز، ينبغي دراسة تعديل مفاتيح التشفير ومحدد هوية مجموعة الخدمة SSID.

ينبغي أن تحتفظ المؤسسة بقائمة تتضمن جميع الأجهزة ذات الواجهة اللاسلكية. ويساعد ذلك مدير الشبكة في الكشف عن الأجهزة اللاسلكية الضارة. ويجب أن يكون هناك إجراءات للحفاظ على هذه القائمة ومتابعتها. ويتم التعامل مع فقدان أو سرقة الأجهزة اللاسلكية باعتباره حادث أمني وفقا لإجراءات إدارة الحوادث التي تحددها المؤسسة. ويتم بدء اتخاذ الضوابط التصحيحية والتي قد تتضمن ضوابط مثل تغيير محدد هوية مجموعة الخدمة SSID و/أو مفاتيح التشفير.

NS 36 أن يتولى مديرو الشبكة إجراء عملية مسح منتظمة لنقاط الوصول اللاسلكية إلى المعلومات "الضارة" أو "غير المصرح بها".

توفر نقاط الوصول اللاسلكية إلى المعلومات الضارة أو غير المصرح بها مدخلا خلفيا للشبكة. ويمكن أن تستحدث نقاط ضعف بالشبكة عن طريق نظام تشغيل مخترق يتم استخدامه من قبل الأجهزة أو نقاط ضعف ضمنية بأجهزة غير معتمدة. ومن ثم، فمن الحكمة أن تكفل المؤسسة وجود إجراءات وإسناد مسؤوليات لمسح الشبكة على فترات منتظمة من أجل الكشف عن الأجهزة اللاسلكية الضارة/ غير المصرح بها.

NS 37 أن يتم تحديد مواقع نقاط الوصول إلى المعلومات من أجل الحد من التصنت على الشبكات من خلال المنطقة المتاحة للجمهور.

تعتزم المؤسسة توفير إرشادات حول موقع نقاط الوصول اللاسلكية إلى المعلومات. وينبغي أن تكفل المؤسسة وجود نقاط الوصول إلى المعلومات في مواقع تعوق أو تحد من محاولات التصنت على الشبكات من خلال المنطقة المتاحة

للجمهور. ويمكن أن تختار المؤسسة إتباع توجه "تحقيق الأمن من خلال الغموض" أو مراقبة جميع نقاط الوصول إلى المعلومات ورصدها.

NS 38 إعدادات العميل لل 802.1x يجب ان تكون امنة.

NS 39 أن يتم تغيير الاسم الافتراضي للشبكة ومفاتيح التشفير وبروتوكول إدارة الشبكة البسيط (SNMP) والسلاسل المجتمعية (وأي إعدادات غير آمنة) عند التنصيب. وينبغي ألا يعكس محدد هوية مجموعة الخدمة اسم أي من إدارات المؤسسة أو اسم النظام أو اسم المنتج.

تكفل المؤسسة تغيير كلمات المرور الافتراضية وأسماء محدد هوية مجموعة الخدمة ومفاتيح التشفير وبروتوكولات إدارة الشبكة البسيطة وأي خصائص مماثلة في وقت التنصيب. وتتولى هذه الخصائص الافتراضية إدخال نقاط الضعف إلى النظام من خلال تيسير عملية اختراق النظام على مستخدم البرامج الضارة. وقد وجد أن شبكة الإنترنت تتضمن موارد وفيرة حول تلك الخصائص، بما في ذلك أسماء المستخدم الافتراضية وكلمات المرور والمفاتيح التي تستخدمها أنواع الشبكات المختلفة والأجهزة والبرمجيات الأمنية. وينبغي ألا يتم تسمية الخصائص الإضافية على أسماء المنظمة أو الإدارة، حيث تستحدث نقاط ضعف إضافية من خلال السماح بتحديد الهوية بسهولة والاستعراض بوصفها أهداف سهلة المنال.

NS 40 فيما يتعلق بنقاط الوصول اللاسلكية غير العامة، ينبغي أن يتم تغيير مفاتيح التشفير بصفة منتظمة وتعطيل بث محدد هوية مجموعة الخدمة SSID. وينبغي أيضا النظر في تنقية عنوان MAC حسب الاقتضاء.

ينص كتيب تأمين المعلومات الوطنية على أنه في حالة وجوب استخدام الأجهزة اللاسلكية وفقا لمتطلبات أنشطة الشركات، ينبغي أن يتم تطبيق ضوابط إضافية، مثل تغيير مفاتيح التشفير بصفة منتظمة وتعطيل بث محدد هوية مجموعة الخدمة. وتعد تنقية عنوان MAC بمثابة أحد الضوابط الأمنية الفعالة، ولكن المضنية، التي قد تعزز الوضع الأمني، رغم كونها غير مقاومة للغش والخداع.

NS 41 أن يكون هناك جدار ناري أو راوتر بين نقطة الوصول إلى المعلومات وشبكة المؤسسة من أجل تنقية الاتصالات. وينبغي تطبيق قواعد الجدار الناري المحظورة كي تسمح للمنافذ اللازمة فقط بالمرور من خلال القسم اللاسلكي.

ينبغي أن يتم تأمين نقاط الوصول إلى المعلومات (الشبكات اللاسلكية) في شبكة المؤسسة باستخدام الجدران النارية/ البوابات. وعلاوة على ذلك، يتم تهيئة الجدران النارية/ البوابات من خلال قواعد مقيدة من أجل التحكم في تدفق البيانات بين الشبكتين.

NS 42 **تفعيل انظمة رصد ومنع إختراقات الشبكة اللاسلكية ذات التصنيف C3 وما فوق لمراقبة التهديدات التي تنشأ من الاجهزة المتواجدة داخل الشبكة اللاسلكية وليست لديها صلاحية الإتصال بالشبكة rouge Aps وهجمات الحرمان من الخدة DOS Attacks وغيرهما.**

NS 43 **إستخدام اكثر من معرف لمجموعة خدمات الشبكة اللاسلكية SSID بمكونات مختلفة لمختلف الشبكات المحلية الظاهرية VLANS واسليب إثبات هوية العميل إلخ: الموظفين والضيوف يمكن ان يرتبطوا بشبكات لاسلكية مختلفة. الشبكات اللاسلكية للضيوف تحتوي على خصائص امنية اقل او تسمح فقط بالاتصال على شبكة الانترنت.**

9-2 إرشادات حول السياسة والضوابط الرئيسية – التزامن

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

NS 44 **يجب تأمين خوادم برتوكول وقت الشبكة NTP وفقا لأفضل الممارسات.**

إتباعاً لافضل الممارسات الموصى بها يجب الا يُصَّلب خادم وقت الشبكة إطلاقاً.

NS 45 **حيثما يكون لدى جهاز الحاسوب أو الاتصالات القدرة على تشغيل ساعة الوقت الفعلي، يتم ضبطها على معيار متفق عليه، على سبيل المثال: التوقيت العالمي المنسق (UTC) أو التوقيت المحلي. ونظرا لأن بعض الساعات تخالف التوقيت بمرور الوقت، فلابد من وجود إجراء يتولى فحص وتصحيح أي تباين في التوقيت.**

في عالم اليوم، ترتبط أجهزة المعالجة الخاصة بنا ببعضها البعض. فلم نعد نعمل في صوامع منعزلة وقد قامت الشركات بتنفيذ حلول المشروعات ودمج العمليات والحلول المتعددة.

ومع ذلك، فعلى الجانب الآخر، حينما تواجه تلك الأنظمة مشكلة ما أو تتعرض لخطر ما، تصبح بمثابة مهمة كبيرة ينبغي دراستها على العديد من الأنظمة.

وتتمثل أهم أداة يتم استخدامها خلال ذلك السيناريو في ملفات تسجيل الأداء. ويتم وضع خاتم التوقيت على ملفات تسجيل الأداء وفقا لزمن النظام.

ومع ذلك، ففي حالة عدم تزامن التوقيت بالأنظمة المختلفة، يكون من الصعب للغاية الربط بين سجلات الأداء الخاصة بالأنظمة المختلفة. وفي حالة وقوع حادث، قد لا يكون للأدلة أي وضع قانوني.

ينص كتيب تأمين المعلومات الوطنية على ضبط التوقيت على جميع أجهزة الحاسبات والاتصالات وفقا للتوقيت المحلي. وينبغي أن تضع المؤسسة إجراءات أو تطبق ضوابط من أجل ضمان قدرة الساعة على تصحيح ذاتها، بصورة يدوية أو من خلال إجراءات آلية، في حالة وجود أي اختلاف في التوقيت.

NS 46 أن يتم استخدام خادم التوقيت الحكومي القطري المصرح به (جزء من الشبكة الحكومية) باعتباره خادم بروتوكول زمن الشبكة الرئيسي NTP.

ينص كتيب تأمين المعلومات الوطنية على امكانية جميع المؤسسات إستخدام خادم التوقيت الحكومي القطري باعتباره خادم بروتوكول زمن الشبكة المصرح به. ويتم اقتراح هذا الخادم كجزء من الشبكة الحكومية. ومع ذلك، لحين توافر هذه الخدمة، يمكن أن تستخدم المؤسسة أحد خوادم بروتوكول زمن الشبكة ذات الموثوقية والمتاحة لجمهور العامة.

NS 47 أن يتم تحقيق التزامن بين جميع الخوادم وأجهزة الشبكة مع خادم بروتوكول زمن الشبكة الرئيسي NTP المتزامن وفقا لما هو محدد في NS43 و NS44.

للحد من تدفق حركة مرور معلومات الشبكة إلى خادم بروتوكول زمن الشبكة الحكومي، من الحكمة أن تتولى المؤسسة تهيئة خادم ضمن شبكتها المحلية باعتباره خادم بروتوكول زمن الشبكة. وسوف يكون هذا الخادم بمثابة خادم ثانوي لخادم بروتوكول زمن الشبكة الحكومي ويتم ضبط توقيته مع توقيت خادم بروتوكول زمن الشبكة الحكومي.

10-2 إرشادات حول السياسة والضوابط الرئيسية – الشبكات الافتراضية الخاصة (VPNs)

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

NS 48 أن تتولى الشبكات الافتراضية الخاصة التي تحمل البيانات المصنفة عند المستوى C3 أو أكثر حيثما يتم استخدام الشبكات المحلية اللاسلكية، ينبغي استخدامها من خلال تدابير كافية لتوثيق المعلومات وتشفير نقلها، إضافة إلى الاستعانة بعمليات وممارسات سليمة لإدارة الأمنعملية التوثيق باستخدام توثيق كلمة المرور لمرة واحدة، مثل جهاز التوثيق أو نظام المفتاح العام/ الخاص الذي يتضمن عبارة مرور قوية.

ينص كتيب تأمين المعلومات الوطنية على استخدام آلية توثيق قوية وآمنة للتحكم في الوصول إلى الشبكات الافتراضية الخاصة. ويوصي باستخدام توثيق كلمة المرور لمرة واحدة، مثل جهاز التوثيق، أو نظام المفتاح العام الخاص الذي يتضمن عبارة مرور قوية.

NS 49 أن تنفصل الشبكات الافتراضية الخاصة تلقائيا عن شبكة المؤسسة بعد فترة توقف محددة مسبقا. ويتم مطالبة المستخدم بالدخول مرة أخرى لإعادة الاتصال بالشبكة.

تستنفد الوصلات غير المستخدمة بالنظام/ الشبكة الكثير من الموارد وتقوض قدرة النظام/ الشبكة. وتمثل تلك الوصلات، إذا ما تم تركها دون مراقبة، مخاطر فادحة على النظام، حيث قد توفر لمستخدم البرامج الضارة إمكانية الوصول غير المصرح به.

ينبغي أن تكفل المؤسسة وجود ضوابط للمحافظة على الموارد المتاحة بالشبكة وتأمين نوافذ الوصول المتاحة للعاملين بها من أجل الاتصال بمواردها بصورة طبيعية. وينبغي أن يتم تطبيق الضوابط التقنية لفصل الخدمة عن أي مستخدم بعد فترة محددة مسبقا من التوقف عن العمل. ويضطر المستخدم إلى الدخول مرة أخرى لإعادة الاتصال بالشبكة. ويضمن ذلك عدم إخفاء بيانات تسجيل الدخول، بما يمثل أحد المخاطر الأمنية.

وعلاوة على ذلك، تستهدف هذه الضوابط بصفة رئيسية المستخدم النهائي؛ ومع ذلك، فقد تمتد إلى الاتصالات بين مواقع الشبكات الافتراضية الخاصة بمقتضى الوفاء بمتطلبات الشبكة.

NS 50 ألا يتم السماح بوجود قناة مشفرة ثنائية ما لم يكن هناك ضوابط مناسبة. وينبغي على المؤسسة أن تسمح بالاتصال بشبكة واحدة فقط في المرة.

تعد القنوات المشفرة الثنائية بمثابة مفهوم للربط الشبكي بين أجهزة الحاسوب يسمح لمستخدم الشبكة الافتراضية الخاصة بالوصول إلى أي شبكة عامة (على سبيل المثال: شبكة الإنترنت) وأي شبكة محلية أو شبكة لاسلكية في نفس الوقت باستخدام نفس الاتصال بالشبكة المادية.

ويتمثل أحد عيوب هذه الطريقة في أنها تجعل الشبكة الافتراضية الخاصة عرضة للهجوم، حيث يمكن الوصول إليها من خلال الشبكة العامة غير الآمنة. وعند تشغيل القنوات المشفرة الثنائية، يتجاوز المستخدمون أمن مستوى البوابة الذي قد يكون قائما داخل البنية الأساسية للشركة. وعلى سبيل المثال، في حالة وجود عملية تنقية الويب أو المضمون، فإنه عادة ما يخضع للرقابة على مستوى البوابة، وليس على مستوى جهاز حاسوب العميل.

يوصي كتيب تأمين المعلومات الوطنية بضرورة عدم تشغيل القنوات المشفرة الثنائية. وفي حالة التفويض بذلك بموجب متطلبات العمل، تكفل المؤسسة وجود ضوابط أمنية مناسبة للتخفيف من حدة نقاط الضعف ذات الصلة.

NS 21 أن يتم تزويد جميع أجهزة الحاسوب المتصلة بشبكات المؤسسة عن طريق شبكة افتراضية خاصة ببرامج أمن شخصي وأحدث البرامج الأمنية وبرامج مقاومة الفيروسات وبرامج الكشف عن البرمجيات الضارة وإصلاحها. ويتم تفعيل برامج الأمن هذه في جميع الأوقات ومن خلال أحدث التوقيعات الفيروسية وتعريفات البرامج الضارة.

تحدد المؤسسة السياسات والإجراءات الخاصة بالاستخدام المقبول للشبكات الافتراضية الخاصة. وينبغي أن تكفل المؤسسة تزويد أجهزة الحاسوب المتصلة بشبكات المؤسسة عن طريق الشبكات الافتراضية الخاصة ببرامج أمن شخصي وأحدث البرامج الأمنية وبرامج الكشف عن البرمجيات الضارة وإصلاحها. ويتم تفعيل جميع هذه البرامج الأمنية في جميع الأوقات وتحديثها بأحدث التوقيعات الفيروسية وتعريفات البرامج الضارة.

تكفل المؤسسة وجود ضوابط تقنية لضمان التزام جميع الحاسبات المتصلة بالسياسة المذكورة أعلاه. ويوصي كتيب تأمين المعلومات الوطنية باستخدام أجهزة التحكم في الوصول إلى الشبكة لضمان الالتزام بالسياسة.

NS 52- أن يتم تنصيب الجدران النارية على مستوى المنافذ من أجل التحكم في حركة المرور بالشبكة من عملاء الشبكة الافتراضية الخاصة إلى أنظمة وخوادم المعلومات المصرح بها.

ينص كتيب تأمين المعلومات الوطنية على تطبيق الضوابط الأساسية، مثل الجدران النارية على مستوى البوابة، من أجل التحكم في تدفق حركة مرور المعلومات من عملاء الشبكات الافتراضية الخاصة إلى أنظمة أو خوادم المعلومات المصرح بها.

11-2 إرشادات حول السياسة والضوابط الرئيسية – الأمن الصوتي لبروتوكول الإنترنت (VoIP)

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

NS 53 يعد الصوت والبيانات شبكتين منفصلتين. وينبغي أن يكون الفصل بينهما ماديا؛ ومع ذلك، يتم السماح بالشبكات المحلية الافتراضية. وتفصل بوابة الصوت، التي تتداخل مع PSTN كل من H.323 أو SIP أو بروتوكولات VoIP الأخرى عن شبكة البيانات.

تتطلب حركة مرور الصوت جودة محددة للخدمة من أجل تأمين حركة مرور الصوت من خلال مجموعات البيانات، التي ينبغي إعدادها للتشغيل في الشبكة المحلية الافتراضية المستقلة من خلال جودة محددة للخدمة. ويؤدي الفصل في المرور أيضا إلى الحفاظ عليه من الهجمات المحتملة على الشبكة المحلية.

ينبغي أن تكفل المؤسسة الفصل بين شبكات الصوت والبيانات؛ ورغم أن الفصل المادي قد يكون مثاليا، إلا أنه يتم السماح بالشبكات المحلية الافتراضية. وعلاوة على ذلك، ينبغي أن تكون البوابة المستخدمة في الفصل بين حركة مرور

الصوت والبيانات متوافقة مع الصوت وأن تكون قادرة على التعامل بفاعلية مع البروتوكولات ذات الصلة بالصوت، مثل H.323 أو SIP أو غيرها.

NS 54 أن يتم استخدام بوابات الأمن الصوتي لبروتوكول الإنترنت وآليات الأمن الملائمة الأخرى.

ينص كتيب تأمين المعلومات الوطنية على أن تكون البوابات المنتشرة لديها قدرة صوتية وأن يتم تزويدها بآليات أمنية ملائمة يتم تصميمها للتعامل مع حركة مرور الصوت.

NS 55 أن تتولى تقييم واستخدام البروتوكولات المفعلة أمنيا مثل بروتوكول الزمن الفعلي الآمن (SRTP).

يوضح بروتوكول النقل الآمن في الزمن الفعلي (أو SRTP) نبذة عن بروتوكول النقل في الزمن الفعلي، الذي يستهدف توفير التشفير وتوثيق وسلامة الرسائل وإعادة حماية بيانات بروتوكول النقل في الزمن الفعلي في كل من التطبيقات الأحادية والمتعددة.

يحظى بروتوكول النقل في الزمن الفعلي أيضا ببروتوكول شقيق يدعى البروتوكول الآمن للرقابة على النقل في الزمن الفعلي؛ ويوفر البروتوكول الآمن للرقابة على النقل في الزمن الفعلي نفس الخصائص الأمنية لبروتوكول النقل الآمن في الزمن الفعلي التي يوفرها بروتوكول النقل الآمن في الزمن الفعلي إلى بروتوكول النقل في الزمن الفعلي.

ويعد استخدام بروتوكول النقل الآمن في الزمن الفعلي أو البروتوكول الآمن للرقابة على النقل في الزمن الفعلي اختياريا لاستخدام بروتوكول النقل في الزمن الفعلي أو بروتوكول الرقابة على النقل في الزمن الفعلي؛ ومع ذلك، ففي حالة استخدام بروتوكول النقل الآمن في الزمن الفعلي أو البروتوكول الآمن للرقابة على النقل في الزمن الفعلي، تكون جميع الخصائص المتوفرة (مثل التشفير والتوثيق) اختيارية ويمكن تشغيلها أو تعطيلها بصورة مستقلة. ويتمثل الاستثناء الوحيد في خاصية توثيق الرسائل الذي لا يمكن الاستغناء عنه عند استخدام البروتوكول الآمن للرقابة على النقل في الزمن الفعلي.

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بتقييم واستخدام البروتوكولات المفعلة أمنيا من أجل ضمان سرية وسلامة بيانات الصوت. وينصح الكتيب باستخدام بروتوكولات مثل بروتوكول النقل الآمن في الزمن الفعلي؛ ومع ذلك، يمكن أن تختار المؤسسة بروتوكولات أخرى قد تكون متاحة وتتلاءم بصورة أفضل مع متطلبات المؤسسة.

NS 56 أن يتم وضع تدابير مكافحة مادية سليمة لحماية البنية الأساسية للأمن الصوتي لبروتوكول الإنترنت.

حتى إذا ما تم استخدام التشفير، قد يسمح الوصول المادي إلى خوادم وبوابات الأمن الصوتي لبروتوكول الإنترنت (VoIP) لأي مهاجم بإجراء تحليل لحركة المرور. ومن ثم، ينبغي أن يكون هناك أمن مادي مناسب للحد من إمكانية الوصول إلى مكونات شبكة الأمن الصوتي لبروتوكول الإنترنت. وينص كتيب تأمين المعلومات الوطنية على وجود ضوابط الأمن المادي الملائمة لتأمين البنية الأساسية للأمن الصوتي لبروتوكول الإنترنت.

NS 57 أن يتم تنفيذ المتابعة الملائمة لسجل المكالمات.

ساعد نقل الصوت عن طريق الإنترنت (VoIP) على الجمع بين حركة مرور الصوت والبيانات. ورغم أنه يوفر العديد من المزايا، إلا أنه يعاني من عيوب متعددة. ونظرا لأن الأمن هو الموضوع الرئيسي، فإنه يتعرض حاليا لمخاوف أمنية تتصل بحركة مرور البيانات. وتتضمن بعض المخاطر الاحتيال في سداد الرسوم والتجسس والاعتراض والتعديل.

ينبغي أن تجري المؤسسة تقييما للمخاطر وأن تتوصل إلى وسيلة رقابة ملائمة لتأمين البنية الأساسية للأمن الصوتي لبروتوكول الإنترنت.

ينص كتيب تأمين المعلومات الوطنية على أن يكون تنفيذ ومتابعة سجلات المكالمات بمثابة وسيلة رقابية أساسية على العمليات لضمان عدم تعرض البنية الأساسية للأمن الصوتي لبروتوكول الإنترنت بالمنظمة للمخاطر. وتتمكن المؤسسة، من خلال متابعة سجلات المكالمات، من التأكد مما إذا كانت البنية الأساسية للأمن الصوتي لبروتوكول الإنترنت قد تعرضت للمخاطر من أجل إجراء مكالمات غير مصرح بها أو تحويل المكالمات أو ما إذا كان قد تم إنشاء خطوط داخلية غير مصرح بها أو غير ذلك.

NS 58 أن تكون برامج المحادثات الهاتفية عن طريق الحاسوب، إذا تم السماح بها، من خلال اتصال آمن، مثل الشبكة الافتراضية الخاصة الآمنة.

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بتأمين وتحديد السياسات والإجراءات فيما يتعلق باستخدام برامج المحادثات الهاتفية عن طريق الحاسوب. ففي حالة التفويض باستخدام برامج المحادثات الهاتفية عن طريق الحاسوب وفقا لمتطلبات العمل، ينبغي أن تكفل المؤسسة تطبيق ضوابط أمنية كافية لتأمين الاتصالات الخاصة بها.

NS 59 أن يتم توفير طاقة احتياطية لأجهزة هاتف الأمن الصوتي لبروتوكول الإنترنت VoIP في حالة انقطاع الطاقة.

ينص كتيب تأمين المعلومات الوطنية على توفير طاقة احتياطية كافية لضمان إتاحة خدمات الأمن الصوتي لبروتوكول الإنترنت في حالة انقطاع الطاقة بصفة عامة.

NS 60 أن يتم تنفيذ ضوابط قوية للتوثيق والوصول إلى المعلومات من أجل حماية نظام بوابة الصوت.

ينص كتيب تأمين المعلومات الوطنية على تطبيق ضوابط قوية للتوثيق والوصول إلى المعلومات من أجل حماية أنظمة بوابة الصوت.

NS 61 أن يتم استخدام IPSEC أو بروتوكول نقل الملفات SSH في جميع عمليات الإدارة أو الوصول إلى المعلومات عن بعد.

ينص كتيب تأمين المعلومات الوطنية على استخدام IPSEC أو بروتوكول نقل الملفات SSH أو أي بروتوكول آمن ومماثل آخر من أجل الإدارة عن بعد أو الوصول إلى البنية الأساسية للأمن الصوتي لبروتوكول الإنترنت.

NS 62 أن يتم وضع خطط طوارئ لإجراء مكالمات صوتية في حالة عدم إتاحة أنظمة الأمن الصوتي لبروتوكول الإنترنت.

ينبغي أن تقوم المؤسسة بتعريف العاملين وإبلاغهم بخطة الطوارئ الخاصة بها من أجل إجراء المكالمات الهاتفية في حالة عدم تواجد بنية أساسية للأمن الصوتي لبروتوكول الإنترنت.

يمكن أن تتخذ المؤسسة القرار بذلك الشأن كجزء من تدريب تخطيط استمرارية تصريف الأعمال الخاص بها. ويمكن أن يوجه تقييم أثر العمل المنظمة في تحديد التكنولوجيا الاحتياطية المناسبة. وتتضمن الأمثلة استخدام الهواتف المحمولة واستخدام شبكة الاتصالات العامة PSTN والهواتف المتصلة بالأقمار الاصطناعية وغير ذلك.

NS 63 أن يتم تفعيل خصائص أمن المنافذ بأجهزة التحويل بالشبكة المحلية التي تربط بين أجهزة الأمن الصوتي لبروتوكول الإنترنت.

ينص كتيب تأمين المعلومات الوطنية على تفعيل الخصائص الأمنية بأجهزة التحويل بالشبكة المحلية من أجل توفير الأمن الإضافي لأجهزة الأمن الصوتي لبروتوكول الإنترنت.

12-2 إرشادات حول السياسة والضوابط الرئيسية – الإصدار رقم 6 لبروتوكول الإنترنت

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

NS 64 أن يتم إجراء عملية تقييم مخاطر من قبل المؤسسة من أجل تقييم مزايا وعيوب الأمن الخاصة بتكنولوجيا IPv4 و IPv6. وينبغي أن تبدأ المؤسسة في دراسة نشر IPv6.

يتم تنفيذ أي تعديل تكنولوجي عقب التقييم الواجب للمخاطر التي يمثلها ذلك التعديل للمنظمة. وتجري المؤسسة عملية تقييم المخاطر من أجل تقييم مدى ملاءمة IPv6 للمنظمة. ويوصي كتيب تأمين المعلومات الوطنية بضرورة أن يكون لدى المؤسسة خارطة طريق محددة للتحول إلى IPv6.

NS 65 أن يتم إجراء عملية تقييم مخاطر إذا ما قررت المؤسسة تطبيق مناخ الحزمة المزدوجة.

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بإجراء تقييم للمخاطر من أجل تقييم المخاطر ونقاط الضعف المحددة الناجمة عن إدارة مناخ الحزمة المزدوجة. وقد ينشأ هذا السيناريو بعد وضع حقائق مثل اول الجزئي وأجهزة التراث وغيرها في الاعتبار.

NS 66 داخل الشبكات الخاصة بها.IPv6أن يتم المطالبة بإعادة المصادقة حيث تتولى المؤسسة نشر

على غرار أي تعديل رئيسي آخر يؤثر على الوضع الأمني للمنظمة، يتعين على المؤسسة إعادة اعتماد ذاتها عقب تحول شبكاتها إلى تكنولوجيا IPv6. ويصبح ذلك هو الحال حتى إذا كان التحول جزئيا، كما هو الحال في بعض القطاعات المختارة من الشبكة.

3 - إرشادات حول تبادل المعلومات [IE]

1-3 أهداف السياسة

2-3 إرشادات حول السياسة والضوابط الرئيسية

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** القيام بما يلي:

IE 1 قبل القيام بتوصيل النطاقات بعضها البعض، تتفهم المؤسسة وتوافق على هيكل وأمن ومخاطر النطاقات الأخرى. ويتم توثيق مراجعة المخاطر من أجل التأكد من مدى الالتزام.

ينص كتيب تأمين المعلومات الوطنية على توخي العناية الواجبة عند تقييم هيكل وأمن ومخاطر النطاق المستهدف توصيل النطاقات به. ويتم توثيق تقييم المخاطر والاحتفاظ بالسجلات وفقا لمتطلبات المراجعة والتدقيق.

تكفل المؤسسة الحفاظ على تصنيف المعلومات عبر النطاق المستهدف.

IE 2 عند اعتزام ربط شبكة أي من المؤسسة بشبكة أخرى آمنة، ينبغي أن يتم:

أ. الحصول على قائمة بالشبكات التي تتصل بها الشبكة الأخرى عن طريق مدير الاعتماد والنظام بالشبكة الأخرى.

ب. فحص المعلومات الصادرة عن كلا المصدرين لتحديد ما إذا كان هناك أي توصيلات غير متعمدة على التوالي.

ج. دراسة المخاطر المتعلقة بالتوصيلات المحددة على التوالي قبل ربط شبكة المؤسسة بالشبكة الأخرى، وخاصة حينما يكون هناك اتصال بإحدى الشبكات غير الموثوقة مثل شبكة الإنترنت.

ينص كتيب تأمين المعلومات الوطنية على إرشادات إضافية فيما يتعلق بتوخي العناية الواجبة أثناء تقييم مدى ملاءمة توصيل شبكة المؤسسة بشبكة أخرى آمنة (أحد المؤسسة الأخرى أو أي شريك استراتيجي غير حكومي). وينبغي تفهم أنه من خلال الربط بأي شبكة خارجية، تتضاعف المخاطر عدة مرات ما لم يتم تطبيق ضوابط محددة ومشددة عند البوابات التي تربط بين كلتا الشبكتين.

IE 3 ضمان إقرار الاتفاقيات اللازمة (وخاصة اتفاقيات السرية) بين الكيانات التي تتبادل المعلومات قبل القيام بتبادل تلك المعلومات. وتنص الاتفاقيات على معلومات حول المسؤوليات وإجراءات إخطار تبادل المعلومات والمعايير التقنية لنقل المعلومات وتحديد شركات النقل والمسؤوليات والملكية والضوابط. وفي حالة الموردين والأطراف الأخرى، يتم استخدام اتفاقيات رسمية لعدم الإفصاح عن المعلومات. وينص الملحق "د" على نموذج لاتفاقية الإفصاح عن المعلومات.

ينص كتيب تأمين المعلومات الوطنية على قيام الكيانين اللذين يتبادلان المعلومات بصياغة الاتفاقيات الملائمة والاتفاق عليها وتوقيعها من قبل الموقعين المعتمدين لدى كل كيان.

تتضمن الاتفاقيات تفاصيل حول الموافقة على تبادل المعلومات وتفاصيل تقنية حول كيفية إجراء التبادل والمسؤوليات المحددة والوظائف المختارة من كل جهاز لمراقبة ومتابعة وإدارة عملية تبادل هذه المعلومات.

يتفق كلا طرفي المؤسسة على الضوابط (التقنية والإدارية) التي يتم تطبيقها لتيسير هذه الرقابة.

IE 4 ضمان حماية الوسائط المستخدمة في تبادل المعلومات من الوصول غير المصرح أو التلاعب أو سوء الاستخدام داخل وخارج المؤسسة.

تكفل المؤسسة وجود ضوابط مناسبة (استنادا إلى تصنيف المعلومات) من أجل حماية الوسائط من الوصول غير المصرح أو التلاعب أو سوء الاستخدام داخل وخارج المؤسسة.

ينبغي أن تدرس المؤسسة ضوابط مثل ضوابط الجرد الأكثر تشددا واستخدام الوسائط التي توفرها وتعتمدها المؤسسة وتشفير الوسائط والخزائن المؤمنة ماديا.

IE 5 الحفاظ على التصنيف وحماية المعلومات التي يتم الحصول عليها من المؤسسة الأخرى.

تكفل المؤسسة الحفاظ على التصنيف وحماية المعلومات التي يتم الحصول عليها من المؤسسة الأخرى. ويتم إدراج مثل هذا النص بالاتفاقيات الموقعة بين المؤسسة قبل بدء تبادل البيانات فيما بينها. وتحظى المؤسسة بالحق في رفض نقل المعلومات إذا لم يكن الجهاز المنقول إليه يحظى بوسيلة الوفاء بهذه المتطلبات.

IE 6 الاحتفاظ بمستويات مناسبة من الحماية المادية للوسائط التي يتم نقلها وتخزينها في عبوات تحميها ضد أي مخاطر تجعل المضمون غير مقروء.

تكفل المؤسسة وجود مستوى ملائم (بناءً على تصنيف المعلومات) من ضوابط الأمن المادي من أجل الحفاظ على الوسائط أثناء تخزينها أو نقلها.

ينبغي أن تدرس المؤسسة الضوابط المناسبة لتخزين وترتيب وتعبئة الوسائط. وتتضمن أمثلة تلك الضوابط ما يلي:

1- ضمان الحفاظ على الظروف المناخية المحددة للوسائط، وعلى سبيل المثال: درجة الحرارة والرطوبة وغيرها.
2- استخدام أغلفة/ مظاريف غير شفافة وغير قابلة لإعادة الاستعمال ومغلقة وتحمل العنوان الصحيح.
3- ضمان أن ينطوي العنوان على اسم وعنوان المرسل إليه، بالإضافة إلى عنوان المرتجع في حالة عدم الاستدلال على العنوان.
4- إذا كنت تعتبر المعلومات حساسة أو سرية للغاية ولا تريد أن يتم فتح الرسالة من قبل أي طرف آخر (مساعد أو سكرتير أو غير ذلك)، ينبغي ألا يحمل المظروف علامة السرية فحسب، بل يحمل أيضا رسالة "لا يفتحه سوى الشخص المرسل إليه فقط".

IE 7 ضمان الاستعانة بشركات وخدمات النقل الموثوقة ذات المصداقية فقط اعتمادا على قائمة من شركات النقل المعروفة والمصرح لها.

تدرس المؤسسة الضوابط المناسبة لنقل الوسائط. وينبغي أن يتضمن ذلك ضوابط مثل الاستعانة بشركات النقل الخاضعة للفحص الأمني والخزانات الآمنة الخاضعة للفحص الأمني والتابعة لأي طرف آخر.

سوف تخضع الاستعانة بمقدمي الخدمات التابعين لأي طرف آخر للضوابط المحددة بالفصل B3، بعنوان "إدارة خدمات الأطراف الأخرى".

IE 8 حماية المعلومات التي يتم تبادلها عن طريق الرسائل الإلكترونية من الوصول غير المصرح له أو التغيير أو انقطاع الخدمة.

تتولى المؤسسة تطبيق ضوابط لضمان سرية وسلامة المعلومات التي يتم تبادلها عبر الرسائل الإلكترونية. ورغم أن ذلك يشير بصفة رئيسية إلى رسائل البريد الإلكتروني، فإنه يتضمن الرسائل المرسلة عبر الهواتف المحمولة، مثل رسائل بلاكبيري وخدمة الرسائل القصيرة وغيرها.

تعتمد الضوابط المختارة على تصنيف المعلومات، بينما يعتمد اختيار الضوابط الخاصة بالبرنامج أو البنية الأساسية (على سبيل المثال: خادم البريد الإلكتروني) على أعلى تصنيف للمعلومات التي يتولى البرنامج/ البنية الأساسية معالجتها أو نقلها.

ويتم فيما يلي استعراض الخطوط الإرشادية لاختيار الضوابط الخاصة بالإرسال الإلكتروني.

أ. التأكد من دقة العنوان أو قائمة الأشخاص المرسل إليهم قبل إرسال المعلومات عن طريق البريد الإلكتروني.

ب. التأكد من صحة عناوين البريد الإلكتروني عند إرسال معلومات محظورة أو ذات وصول محدود عن طريق البريد الإلكتروني. والتأكد من أن جميع الأشخاص المدرجين بالقوائم يحظون بتصريح لاستلام المعلومات عند استخدام قوائم عناوين محددة مسبقا. وطلب تقديم دليل على الإرسال والتسلم.

ج. التحقق مما إذا كان هناك حاجة إلى حماية إضافية فيما يتعلق بالمرفقات التي تحظى بحماية كلمة المرور أو التشفير أو التوقيع الرقمي قبل إرسال البريد الإلكتروني.

د. أن تحظى جميع المعلومات المصنفة عند المستوى C2 بكلمات مرور توفر الحد الأدنى من الحماية. ويتم إرسال المعلومات ضمن مرفقات تحظى بحماية كلمات مرور من خلال البريد الإلكتروني. ويتم إرسال كلمات المرور إلى المستقبل من خلال وسيلة اتصال مستقلة، مثل الصوت أو خدمة الرسائل القصيرة أو الفاكس أو غير ذلك.

IE 9 ضمان استخدام الرسائل الآمنة (يتم توقيع و/أو تشفير المعلومات رقميا) في نقل جميع المعلومات المصنفة عند المستوى C3 أو أكثر. وينبغي على المؤسسة استخدام بروتوكول مكافئ او افضل من البروتوكول الآمن متعدد الأغراض للتوسع في البريد الإلكتروني وفقا لما هو محدد بالفقرة CY7، الفصل C-10 بعنوان "أمن التشفير [CY].

ينص كتيب تأمين المعلومات الوطنية على التشفير و/أو التوقيع الرقمي لجميع المعلومات المصنفة عند المستوى C3 باستخدام الأدوات التي تعتمدها المؤسسة عند إرسالها من خلال الرسائل الإلكترونية. ويوصي كتيب تأمين المعلومات الوطنية باستخدام البروتوكول الآمن متعدد الأغراض للتوسع في البريد الإلكتروني S/MIME من أجل تأمين الرسائل وفقا لما هو محدد بالفقرة CY6، الفصل C-10 بعنوان "أمن التشفير [CY].

IE 10 إرفاق إخلاء المسؤولية عن البريد الإلكتروني أو ما شابه بجميع رسائل البريد الإلكتروني الصادرة:

"قد تتضمن المعلومات التي يشتمل عليها هذا البريد الإلكتروني، بما في ذلك المرفقات، معلومات سرية تحظى بحماية حقوق الملكية الفكرية أو تكون ذات امتيازات قانونية. ويتم إرسال هذا البريد الإلكتروني إلى الأشخاص المستهدفين. ويعد الوصول إلى هذا البريد الإلكتروني من قبل أي شخص آخر غير مصرح به. ويحظر أي استخدام أو الإفصاح عن أو نسخ أو توزيع هذا البريد الإلكتروني من قبل أشخاص آخرين بخلاف الشخص المرسل إليه. فإذا لم تكن الشخص المرسل إليه، ينبغي أن تحذف هذه الرسالة على الفور من نظامك. وإذا كنت تعتقد أنك قد تسلمت هذا البريد الإلكتروني عن طريق الخطأ، يرجى الاتصال بالمرسل أو اسم <المؤسسة وبيانات الاتصال>. وتعد الآراء التي يتم التعبير عنها بهذا البريد الإلكتروني أو مرفقاته خاصة بالمرسل فقط ما لم ينص المرسل صراحة على كونها آراء خاصة بالمؤسسة.

ليس مؤكدا ما إذا كان إخلاء المسؤولية عن البريد الإلكتروني سوف يوفر الحماية من المسؤولية في المحاكم. ومع ذلك، فمن المؤكد أن يساعد إخلاء المسؤولية المصاغ بصياغة جيدة في الدعوى المقامة ضد المؤسسة وقد يؤدي إلى إعفائها من

المسؤولية في بعض الحالات. والأهم من ذلك، قد يحول الإخلاء من المسؤولية دون إقامة الدعوى الفعلية ضد المؤسسة، نظرا لأن مجرد وجود تلك العبارة قد يمنع معظم الأشخاص من المطالبة بتعويض قانوني من المؤسسة.

ومن ثم، يوصي كتيب تأمين المعلومات الوطنية باستخدام إخلاء المسؤولية. ويعد إخلاء المسؤولية المشار إليها أعلاه هو الأسلوب الموصى به والذي يمكن استخدامه من قبل المؤسسة.

IE 11 ممارسة العناية الواجبة لضمان خلو أي معلومات يتم إرسالها او استقبالها من الفيروسات وفيروس طروادة والبرمجيات الضارة الأخرى.

تمارس المؤسسة العناية الواجبة أثناء إرسال المعلومات (رسائل البريد الإلكتروني أو تبادل البيانات) من أجل التأكد من أن المعلومات التي يتم إرسالها خالية من الفيروسات وفيروس طروادة والبرمجيات الضارة الأخرى. ومع ذلك، يتحمل المستقبل المسؤولية بالمناصفة ويتم نصحه باتخاذ أقصى الاحتياطيات لحماية البنية الأساسية للمعلومات الخاصة به.

يوصي كتيب تأمين المعلومات الوطنية باستخدام الضوابط المناسبة عند البوابات من أجل متابعة وفحص وضمان التزام البيانات التي يتم نقلها من خلالها.

IE 12 ضمان حماية المعلومات التي يتم تبادلها بين الأنظمة ضد سوء الاستخدام أو الوصول غير المصرح به إلى المعلومات أو فساد البيانات. ولنقل المعلومات المصنفة عند المستوى C1 أو C2 أو أكثر، يتم استخدام القنوات الموثقة والمشفرة وفقا لما هو محدد في CY4، الفصل C-10 بعنوان "إرشادات حول أمن التشفير" [CY].

ينبغي أن تكفل المؤسسة وجود الضوابط الأمنية المناسبة من أجل حماية سلامة وسرية المعلومات التي يتم تبادلها بين الأنظمة المختلفة.

تهدف الضوابط في الأساس إلى حماية نقل البيانات بين الأجهزة. ومع ذلك، يمكن التوسع بها لتشمل الأنظمة الداخلية للجهاز وسوف تدعم بالتأكيد الوضع الأمني للمؤسسة.

ينص كتيب تأمين المعلومات الوطنية على نقل المعلومات المصنفة عند المستوى C1 أو C2 أو أكثر باستخدام قنوات البيانات الموثقة والمشفرة. ويلتزم التشفير بالفصل C-10 بعنوان "فصل التشفير".

يوصي كتيب تأمين المعلومات الوطنية باستخدام الضوابط التالية:

أ- ينبغي استخدام البروتوكولات الآمنة مثل S-FTP أو SSH عند إرسال أو استقبال المعلومات. ويجب ألا يتم استخدام البروتوكولات غير الآمنة، مثل Telnet والأصدار الأول والثاني من بروتوكول SNMP.

ب- يتم الربط بين المؤسسة من خلال وصلات مادية مستقلة أو وصلة آمنة، مثل الشبكة الافتراضية الخاصة عن طريق سحابة ISP. وينبغي أن تكون الشبكة الحكومية بمثابة أسلوب الربط المفضل.

IE 13 قصر المعلومات المتاحة إلى جمهور العامة (عن طريق وسائل الإعلام) على المعلومات الموثقة والمعتمدة من خلال متحدث إعلامي محدد ومدرب.

ينص كتيب تأمين المعلومات الوطنية على ضرورة أن يكون لدى المؤسسة متحدث إعلامي/ فريق إعلامي محدد ومدرب.

يكون المتحدث الإعلامي/ الفريق الإعلامي المحدد بمثابة نقطة الاتصال الوحيدة المسؤولة عن نشر المعلومات بين جمهور العامة/ الأطراف الرئيسية خارج نطاق المؤسسة. ويتعين ألا يتم الكشف عن أي معلومات ينبغي الإفصاح عنها إلى وسائل الإعلام، حتى إذا كانت تحظى بتصنيف "عام"، إلا من خلال المتحدث الإعلامي/ الفريق الإعلامي المحدد بعد التشاور مع إدارة العلاقات العامة بالمؤسسة.

يتولى المتحدث الإعلامي/ الفريق الإعلامي المحدد المسؤولية عن ضمان أن تكون المعلومات الصادرة تحظى بتصنيف "عام" أو "داخلي" (على أساس كل حالة على حدة عند إصدارها إلى مجموعة محدودة من الأشخاص المصرح لهم/ وسائل الإعم المصرح لها) عند إصدار المعلومات.

4 - إرشادات حول أمن البوابة [GS]

1-4 أهداف السياسة

الهدف الرئيسي من هذه السياسة هو توفير الحد الأدنى لمتطلبات الأمن من أجل حماية البوابات المستخدمة في الاتصالات بين المؤسسة بالإضافة إلى الاتصالات بالروابط الخارجية.
يمكن استخدام عملية نشر البوابة الخاضعة للسيطرة لضمان انتقال المعلومات المسموح بها فقط بين البوابة والشبكات المتصلة بها. ويمكن استخدام ذلك للحفاظ على متطلبات الحاجة إلى المعرفة ومنع الأنشطة الضارة من الانتشار من شبكة إلى أخرى. وتتضمن البوابات أجهزة الراوتر والجدران النارية وحلول تنقية المضمون والخوادم البديلة.

2-4 إرشادات حول السياسة والضوابط الرئيسية – عام

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

GS 1 أن يتم حماية الشبكات من الشبكات الأخرى من خلال بوابات والتحكم في تدفق البيانات بصورة سليمة.

ينبغي أن تكفل المؤسسة حماية الشبكات المادية من بعضها البعض باستخدام البوابات، كحد أدنى. ويوصي كتيب تأمين المعلومات الوطنية باستخدام البوابات لحماية الشبكات المنطقية داخل المؤسسة.

وعلاوة على ذلك، ينبغي أن تكفل المؤسسة تهيئة وإعداد البوابات بصورة صحيحة كي تضطلع بدور رقابي فعال. وقد وجد في كثير من الأحيان أنه يتم تهيئة وإعداد البوابات من خلال قواعد متراخية. ولا يؤدي ذلك إلى إيجاد نقاط ضعف داخل الشبكة فحسب، بل إلى غرس مستوى زائف من الثقة.

GS 2 أن يتم تنفيذ البوابات التي تربط شبكات المؤسسة بشبكات المؤسسة الأخرى أو بالشبكات العامة غير الخاضعة للرقابة:

أ. من خلال جهاز الشبكة الملائم للتحكم في تدفق البيانات.
ب. من خلال التحكم في تدفق البيانات بالصورة الملائمة.
ج. من خلال وضع المكونات المادية للبوابة الإلكترونية داخل غرفة الخادم المؤمنة بالصورة الملائمة.

بالإضافة إلى الضوابط المذكورة في البند GS1، ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بممارسة العناية الواجبة أثناء اختيار جهاز البوابة لضمان أن يفي بالمتطلبات التقنية والوظيفية للمؤسسة.

ضمان التحكم في تدفقات (قواعد) البيانات؛ وينبغي أن يتم فحص أي تغيير في تدفق البيانات من خلال عملية إدارة التغيير. ويجب أن يتم توثيق ومراجعة كل تلك التغييرات بصفة منتظمة.

ينبغي أن يتم تأمين جهاز البوابة بصورة مادية.

GS 3 أن يتولى فريق العمل المصرح له والمدرب إدارة البوابات والحفاظ عليها.

تعد البوابات بمثابة حلول أمنية متخصصة؛ وبالتالي، ينبغي أن يتم إدارتها والمحافظة عليها من قبل فريق العمل المدرب. وينص كتيب تأمين المعلومات الوطنية على وجود ضوابط مناسبة للوصول إلى المعلومات تقصر إمكانية الوصول على فريق العمل المصرح له ويكون ذلك الفريق مدربا بالصورة الملائمة. وسوف يضمن ذلك تهيئة وإعداد البوابة والمحافظة عليها بالصورة المناسبة.

GS 4 أن يتم توفير إمكانية الوصول الإداري إلى البوابات التي تتولى معالجة أو نقل المعلومات المصنفة عند المستوى C3 أو أكثر اعتمادا على الرقابة المزدوجة ومبادئ الرقابة من قبل شخصين.

بالإضافة إلى الضوابط المذكورة بالبند GS3، ينبغي أن تكفل المؤسسة مستوى إضافي من الضوابط للبوابات التي تتولى معالجة أو نقل المعلومات المصنفة عند المستوى C3 أو أكثر.

يتم توفير إمكانية الوصول الإداري بناءً على الرقابة المزدوجة ومبدأ الرقابة من قبل شخصين. سوف يضمن ذلك عدم قدرة أي شخص على حدة أن يقوم بتعريض النظام للمخاطر. وسوف يستحدث إجراء عملية فحص وتوازن للإعدادات الخاصة بالنظام.

GS 5 أن يتم وسم المعلومات التي يتم تبادلها عبر البوابات وفقا لسياسة تصنيف البيانات [IAP-NAT-DCLS] وحمايتها وفقا لما تنص عليه هذه الوثيقة. وينبغي أن يتم تصنيف البوابات بما يتماشى مع المعلومات التي تنقلها.

تعد البوابات أو أي صناديق أخرى خاصة بالشبكة في حد ذاتها مجرد أصول معلوماتية ليس لها قيمة أو متطلبات فعلية فيما يتعلق بالسرية أو السلامة. وعلى سبيل المثال، يمكن أن تتم تهيئة جهاز البوابة للربط بين منزلين يتبادلان الملفات الشخصية أو أن تتم تهيئة نفس جهاز البوابة للربط بين اثنين من المؤسسة يتبادلان المعلومات السرية. وفي كلا السيناريوهين، تتغير بيانات البوابة بناءً على المعلومات التي تتولى معالجتها. ومن ثم، يتم تصنيف البوابات بما يتماشى مع المعلومات التي تعالجها أو تنقلها ويتم اختيار الضوابط الأمنية وفقا لذلك.

ينبغي أن تكفل المؤسسة وسم المعلومات التي يتم تبادلها عبر البوابات وفقا لسياسة تصنيف البيانات [IAP-NAT-DCLS] وحمايتها وفقا لما تنص عليه هذه الوثيقة.

ينص كتيب تأمين المعلومات الوطنية على ضرورة أن تكفل المؤسسة، متى أمكن، قدرة البوابات على تنقية وإدارة مضمون المعلومات بحيث يلتزم ذلك المضمون بالسياسات.

GS 6 أن يتم استخدام المناطق منزوعة السلاح DMZ لفصل الأنظمة التي يمكن الوصول إليها من الخارج عن الشبكات العامة غير الخاضعة للرقابة والشبكات الداخلية عن طريق استخدام جدران نارية وأجهزة أمن الشبكات الأخرى.

ينص كتيب تأمين المعلومات الوطنية على تصميم الشبكات لفصل الأنظمة التي يمكن الوصول إليها من الخارج عن الشبكات العامة غير الخاضعة للرقابة والشبكات الداخلية بصورة فعالة. ويوصي الكتيب باستخدام جدران نارية أو أي أجهزة أخرى لأمن الشبكات مثل أجهزة الراوتر وغيرها.

ينبغي أن يتم تهيئة الأجهزة من خلال القواعد المناسبة لتدفق/ مراقبة البيانات.

GS 7 البوابات:

هي سبل الاتصال الوحيدة من وإلى الشبكات الداخلية.

ترفض بصورة افتراضية جميع التوصيلات من وإلى الشبكة.

تسمح بالتوصيلات المصرح بها فقط.

تخضع للإدارة عن طريق مسار آمن يتم عزله عن جميع الشبكات المتصلة.

توفر قدرة تدقيق كافية للكشف عن أي اختراق أمني للبوابات وأي محاولة لاقتحام الشبكات.

توفر إنذار في الزمن الفعلي.

ينص كتيب تأمين المعلومات الوطنية على قواعد لإعداد وإدارة أجهزة البوابات. وتعتمد القواعد على أفضل الممارسات الأمنية التي توصي بها الصناعة.

GS 8 أن يتم دعم البوابات قبل التطبيق على أي موقع إنتاج وحمايتها من:

أ. البرمجيات الضارة ونقاط الضعف.
ب. الإعدادات الخاطئة أو السيئة.
ج. تسوية الحسابات وزيادة الامتيازات.
د. متابعة الشبكات الضارة.
هـ. رفض الاعتداءات على الخدمة.
و. تسرب المعلومات/ البيانات.

يتم إعداد وتهيئة أي جهاز/ خادم/ حل/ نظام بصورة افتراضية من أجل تعظيم المهام الوظيفية وسهولة الاستعمال. ومع ذلك، يؤدي ذلك إلى ظهور نقاط ضعف كثيرة بالنظام، مما قد يعرض النظام للمخاطر. ورغم ذلك، يمكن التخفيف من حدة العديد من نقاط الضعف بالنظام أو التخلص منها من خلال ضمان إعداد النظام بالصورة السليمة القائمة على الاحتياجات. ويتم الإشارة إلى هذه العملية باعتبارها عملية دعم.

ينص كتيب تأمين المعلومات الوطنية على ضرورة دعم البوابات قبل أي عملية تنفيذ أو انتشار في أي موقع من مواقع الإنتاج. ويوفر الكتيب الإرشادات أيضا حول المخاطر الرئيسية التي ينبغي وضعها في الاعتبار أثناء تأمين/ دعم جهاز البوابة.

GS 9 أن تكون هناك متابعة وإشراف على البوابات وتتضمن تلك المتابعة والإشراف آليات درء المخاطر وتسجيل الأداء والإنذار ومراقبة المعدات. الفصل B-10 بعنوان "إرشادات حول تسجيل الأداء ومتابعة الأمن" [SM].

ينبغي أن تكفل المؤسسة وجود إجراءات محددة لضمان متابعة أجهزة البوابة وتسجيل الإنذار والأداء بمقتضى الفصل B-10 بعنوان "تسجيل الأداء ومتابعة الأمن".

ينبغي أن تكفل المؤسسة تخصيص الموارد الملائمة لمتابعة أنظمة البوابة. وينبغي أن تتم متابعة أنظمة البوابة التي تتولى معالجة أو نقل المعلومات المصنفة عند المستوى C3 أو أكثر على مدار 24 ساعة يوميا خلال سبعة أيام أسبوعيا.

ينبغي أن يتم تحليل سجلات الأداء وربطها، إن أمكن، بسجلات أداء الأنظمة الأخرى من أجل الكشف عن أنماط المخاطر والهجمات والشذوذ في النظام.

GS 10 أن تمنع البوابات أو تستبعد أي بيانات يعتبرها مرشح المضمون مريبة، بما في ذلك على الأقل ما يلي:

أ. اللغة أو المرفقات البذيئة أو العدائية.
ب. المضمون المفعم بالبرامج الخبيثة.
ج. الاعتداءات على الخدمة.
د. تصنيف المواقع الإلكترونية/المضمون التي يعتبرها قانون الجرائم الإلكترونية المقترح غير ملائمة، بما في ذلك المواقع الإلكترونية التي تستضيف المواد الإباحية ومواقع المقامرة...الخ.

ينص كتيب تأمين المعلومات الوطنية على ضرورة أن تكون البوابات قادرة على تحليل حركة المرور عند طبقة التطبيق.

وينص الكتيب على الحد الأدنى لمتطلبات تنقية المضمون التي يتم الوفاء بها من قبل البوابات.

من الممكن ألا يكون الجهاز الواحد قادرا على الوفاء بهذا الشرط؛ ومن ثم، يمكن أن تستخدم المؤسسة مجموعة من الأجهزة التي قد تحقق النتيجة المرجوة.

ومع ذلك، ينبغي أن تكفل المؤسسة التزام جميع الأجهزة ضمن هذه المجموعة بالضوابط المذكورة أعلاه.

3-4 السياسة والضوابط الرئيسية – تصدير البيانات

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

GS 11 مستخدمو النظام:

أ. يكونون عرضة للمساءلة عن البيانات التي يقومون بتصديرها.
ب. تصدر إليهم التعليمات بإجراء فحص الوسم الوقائي والفحص العيني وفحص البيانات الوصفية ذات الصلة حول إمكانية تصدير البيانات.

يهدف كتيب تأمين المعلومات الوطنية إلى تقييد المساءلة عن تصدير البيانات التي تضطلع بها المؤسسة. وينبغي أن يكفل مستخدمو النظام المسؤولون عن تصدير البيانات إلى المؤسسة الخارجية التزامهم بالأحكام ذات الصلة بسياسة وكتيب تأمين المعلومات الوطنية. وينبغي أن يكفل هؤلاء، بصفة رئيسية، تصنيف تلك المعلومات التي يتم تصديرها ووضع العلامات عليها وفقا للتصنيف والضوابط الضرورية الموجودة من أجل الالتزام بمتطلبات تصنيف المعلومات C-I-A.

GS 12 صادرات البيانات إما أن:

أ. يتم تنفيذها وفقا للعمليات و/أو الإجراءات التي تصدق عليها المؤسسة.

ب. يتم اعتمادها بصفة فردية من قبل مدير أمن المعلومات.

يكفل مستخدمو النظام المسؤولون عن تصدير البيانات التزامهم بالعملية/ المعايير المقررة التي تعتمدها المؤسسة. ويتولى مدير أمن المعلومات اعتماد وإقرار أي استثناء من العملية/ الإجراءات المقررة بصورة واضحة وفقا لكل حالة على حدة.

GS 13 أن يتم حظر تصدير البيانات إلى نظام يحظى بتصنيف أقل من خلال ترشيح البيانات باستخدام فحوص علامات التصنيف على الأقل.

ينبغي أن تكفل المؤسسة تصنيف أنظمة المعلومات التي تتولى معالجة التصنيفات المتعددة للمعلومات وفقا لأعلى مستويات المعلومات التي تقوم بمعالجتها أو تخزينها. وقد تتصل الأنظمة التي تعالج التصنيف المتعدد للمعلومات بالأنظمة الأخرى في الأجهزة الخارجية التي يمكن تصنيفها عند مستوى أدنى.

ومع ذلك، تكفل المؤسسة وجود ضوابط أمنية لضمان عدم تصدير المعلومات المصنفة عند مستوى مرتفع إلى نظام يحظى بمستوى تصنيف أدنى. وتطبق الأنظمة حلول التنقية التي سوف تتمكن، كحد أدنى، من اتخاذ إجراء بشأن علامة تصنيف المعلومات.

وعلى سبيل المثال، يتم تصنيف النظام، الذي يتولى معالجة المعلومات المصنفة عند مستوى يصل إلى C2، باعتباره المستوى C2. ويتصل هذا النظام بنظام خارجي مصنف عند المستوى C1؛ ومع ذلك، تتوافر الضوابط لمنع تصدير المعلومات المصنفة عند المستوى C2.

GS 14 أن يتم فحص صادرات البيانات بما يكفل:

أ. البحث عن الكلمات الرئيسية في جميع البيانات النصية.

ب. حظر أي بيانات غير معرفة لحين مراجعتها والموافقة على إصدارها من قبل أي مصدر موثوق بخلاف جهة إصدار البيانات.

ينبغي أن تكفل المؤسسة استخدام آليات تنقية المضمون عند البوابات التي تحظى بالقدرة على البحث عن الكلمات الرئيسية في جميع البيانات النصية التي يتم تصديرها إلى المؤسسة الخارجية. وينبغي أن يكون نظام تنقية المضمون قادرا على إجراء مسح للكلمات الرئيسية المحددة، بما في ذلك علامات التصنيف.

يتم حظر أي انتهاك وخضوعه للمراجعة والاعتماد من قبل أي مصدر موثوق بخلاف جهة إصدار البيانات.

يجدر الإشارة إلى أن محرك البحث الآلي قد لا يكون قادرا على مسح الملفات المشفرة أو التي تخضع لحماية كلمات المرور. وقد يوفر التعديل اليدوي أو تبادل مفتاح التشفير من خلال محرك البحث الآلي بعض المساعدة هنا. ومع ذلك، يتم تقييم مخاطر فك تشفير البيانات وإعادة تشفيرها عند البوابات بالصورة الملائمة.

4-4 السياسة والضوابط الرئيسية – استيراد البيانات

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

GS 15 مستخدمو النظام:

أ- يكونون عرضة للمساءلة عن البيانات التي يقومون باستيرادها.
ب- تصدر إليهم التعليمات بإجراء فحص الوسم الوقائي والفحص العيني وفحص البيانات الوصفية ذات الصلة.

يهدف كتيب تأمين المعلومات الوطنية إلى تقييد المساءلة عن استيراد البيانات التي تضطلع بها المؤسسة. وينبغي أن يكفل مستخدمو النظام المسؤولون عن استيراد البيانات إلى المؤسسة الخارجية التزامهم بالأحكام ذات الصلة بسياسة وكتيب تأمين المعلومات الوطنية. وينبغي أن يكفل هؤلاء، بصفة رئيسية، تصنيف تلك المعلومات التي يتم استيرادها ووضع العلامات عليها وفقا للتصنيف والضوابط الضرورية الموجودة من أجل الالتزام بمتطلبات تصنيف المعلومات C-I-A.

GS 16 واردات البيانات إما أن:

أ- يتم تنفيذها وفقا للعمليات و/أو الإجراءات التي تصدق عليها المؤسسة.
ب- يتم اعتمادها بصفة فردية من قبل مدير أمن المعلومات.

يكفل مستخدمو النظام المسؤولون عن استيراد البيانات التزامهم بالعملية/ المعايير المقررة التي تعتمدها المؤسسة. ويتولى مدير أمن المعلومات اعتماد وإقرار أي استثناء من العملية/ الإجراءات المقررة بصورة واضحة وفقا لكل حالة على حدة.

GS 17 أن يتم مسح البيانات الواردة إلى نظام المؤسسة من أجل الكشف عن المضمون الضار والنشط.

ينبغي أن تكفل المؤسسة وجود ضوابط من أجل مسح البيانات التي يتم استيرادها إلى أنظمتهم للتحقق من خلوها من مضمون البرامج الخبيثة.

5 - إرشادات حول أمن المنتجات [PR]

5-1 أهداف السياسة

تقر هذه السياسة الحد الأدنى من الأمن اللازم لانتقاء وحيازة منتجات المعلومات من خلال عملية سليمة للانتقاء والاستحواذ. وينبغي أن تكفل **المؤسسة** اختيار المنتجات المنتقاة بعد إجراء عملية تقييم مستقلة تفي بالمتطلبات الأمنية المدرجة بهذه السياسة.

5-2 إرشادات حول السياسة والضوابط الرئيسية

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

PR 1 أن يتم إجراء عملية انتقاء المنتجات بعناية واجبة وأن تكفل استقلالية المنتجات والموردين.

ينبغي أن تكفل المؤسسة أن تحظى عملية شراء خدمات وحلول تكنولوجيا المعلومات بالعدالة والاستقلالية عن تأثيرات المنتجات و/أو الموردين. وتدعو المؤسسة إلى تقديم عدد كاف من المقترحات وأن يتم تقييم كل منها بالصورة الملائمة. وينبغي أن يستند مستوى العناية الواجبة على تقييم المخاطر من البائع والمخاطر المرتبطة بأصول المعلومات المتضررة من المنتجات المعروضة من قبل البائع. على سبيل المثال، قد يتطلب إجراء تحقيقات دورية على بائع ذو مخاطر عالية ، بينما بائع منخفض المخاطر قد لا يتطلب سوى مراجعة القوائم المالية المدققة للبائع.

PR 2 أن يتم تصنيف ووسم المنتجات وفقا لسياسة تصنيف البيانات الوطنية [IAP-NAT-DCLS].

يتم وسم جميع المنتجات التي يتم شراؤها أو تصنيعها وفقا لسياسة تصنيف البيانات الوطنية [IAP-NAT-DCLS]. ويتم تصنيف أجهزة نظام المعلومات بناءً على المعلومات التي تتولى معالجتها أو تخزينها.

قد يكون من الحكمة أن تجري المؤسسة تحليلا لعملية التصنيف أثناء مرحلة التحليل والتصميم من أجل تقييم التصنيف المحتمل للمنتجات التي يتم شراؤها و/أو تصنيعها.

من خلال التفكير في التصنيف المحتمل خلال مرحلة التحليل/ التصميم، قد تؤثر مرحلة الشراء على اختيار الموردين والمنتج ذاته.

وعلى سبيل المثال، قد تحتاج إلى شراء منتج يمكن تصنيفه عند المستوى "C3" من مورد ما ليس لديه سجل إيجابي حافل.

PR 3 **أن تتضمن عملية الانتقاء تحديد الموردين بالصورة الملائمة وفحص الموردين وتحديد معايير التقييم التي ينبغي أن تتضمن كحد أدنى ما يلي:**

وضع وهوية المورد، بما في ذلك الموقع والملكية.

الموقف المالي.

المراجع حول المشاركات السابقة الناجحة.

قدرة البائع على بناء و/ أو الحفاظ على الضوابط المناسبة على النحو الذي يحدده تقييم المخاطر

تحدد المؤسسة إجراءً لشراء السلع والخدمات ذات الصلة بتكنولوجيا المعلومات. وتشتمل عملية الشراء، كحد أدنى، على تحديد وفحص الموردين. ويتم تحديد معيار التقييم الذي يتضمن كحد أدنى ما يلي:

أ- وضع وهوية المورد، بما في ذلك الموقع والملكية: تكفل العملية ممارسة العناية الواجبة في تحديد المورد. وقد يكون من الحكمة، أثناء دراسة الحلول الخاصة بالأمن القومي أو الحلول التي تستهدف حماية السلامة الوطنية، أن يتم التأكد من أن المورد أو المنتج لا ينتمي إلى دولة عدو أو دولة ذات علاقات متوترة أو غير ذلك. وقد يكون من الضروري في بعض القطاعات أو في بعض الظروف الحرجة أن يكون المورد أو الحل محليا أو يحظى بشراكة محلية (يتمتع الشريك المحلي بالأغلبية) من أجل ضمان توفير الدعم المناسب والتغطية القانونية والحد من خطر سوء استخدام السلطة الأجنبية. وعلاوة على ذلك، ينبغي التأكد أيضا من عدم المبالغة في الاعتماد على مورد/ منتج واحد...الخ.

ب- الموقف المالي: تكفل المؤسسة ممارسة العناية الواجبة في تقييم الإمكانات المالية للمورد المحتمل. وتشكل الشركات المؤقتة خطرا على التنظيم بما يعرض الاستثمارات والثقة في سلامة الأنظمة للمخاطر. وعلاوة على ذلك، ينبغي توخي الحذر أثناء شراء الحلول/ الخدمات من الشركات الصغيرة التي قد لا تستمر في العمل لفترة طويلة أو تتعرض لمخاطر استيلاء القوى التنافسية عليها.

ج- المراجع حول المشاركات السابقة الناجحة: ينبغي أن تكفل المؤسسة أن يوفر الموردون مراجع حول المشاركات السابقة الناجحة. وتتولى المؤسسة فحص المراجع التي يقدمها الموردون. وبناءً على هذه المراجع، ينبغي أن تتولى المؤسسة تقييم قدرات المورد فيما يتعلق بمدى قدرته على تسليم المشروع/ توفير الحل وقوة المنتج والقدرات وغير ذلك.

PR 4 أن يتم إجراء الاختبار السليم والمضاهاة الفعالة بين طلب الموردين وأسلوب العمل من أجل تجنب فقدان سرية وسلامة و/أو إتاحة المعلومات.

ينبغي أن تكفل المؤسسة تحديد الإجراءات للتأكد من أن اختبارات القبول تمثل جزءا من عملية إغلاق المشروع. وينبغي أن تكون اختبارات القبول شاملة وأن تكفل اشتمالها على ما يلي:

أ- يفي الحل بالمتطلبات التقنية والوظيفية التي تحددها المؤسسة. ويمكن أن يتم تحديد المتطلبات بوثيقة طلب تقديم العروض وطلب عروض الأسعار ووثائق التصميمات المتفق عليها بعد انتهاء العقد وغير ذلك.

ب- يتوافق الحل مع المطالبات التي يقدمها المورد أثناء مرحلة تقديم العطاءات (الشراء) أو عقب تلك المرحلة.

ت- يتوافق الحل مع ما تنص عليه النشرات والبيانات المتوفرة مع النظام..

PR 5 أن يتم إجراء تقييم أمني للمنتج على أساس الإعدادات الأمنية المخصصة، بما في ذلك اختبارات أسلوب العمل واختبارات الأمن من أجل الحماية من المخاطر المحتملة ونقاط الضعف.

ينبغي أن تكفل المؤسسة تقييم المنتجات الجديدة على منصة اختبار خاصة. ويضمن ذلك ألا يشكل اختبار وتقييم المنتج أي مخاطر على بيئة الإنتاج.

وعلاوة على ذلك، تتضمن تلك الإجراءات اختبارات وظيفية واختبارات أمنية ودعم المنتج من خلال تطبيق التعديلات المناسبة وضبط الإعدادات. وسوف يكفل ذلك أن يكون أداء المنتج وفقا لما هو متوقع ضمن الإعدادات المرجوة، بما يؤدي إلى الحد من المخاطر الناجمة عن أداء الاختبارات وفقا إعدادات افتراضية.

PR 6 أن يتفق تقديم المنتجات مع الممارسات الأمنية للمؤسسة من أجل تقديمها بصورة آمنة.

ينبغي أن تكفل المؤسسة أن تستوعب عملياتها وإجراءاتها المحددة مبادئ/ ممارسات أمن المعلومات. ويجب أن تضمن التزام جميع المنتجات، التي يتم تقدمها، بهذه المنهجية الآمنة للتقديم.

ينبغي أن يكفل الموردون التزام المنتجات، التي يتم تقديمها، بمعايير أمن المعلومات التي توصي بها المؤسسة (وعلى سبيل المثال: سياسات تأمين المعلومات الوطنية). وتلتزم جميع العمليات التي تندرج ضمن تقديم الخدمة بأفضل ممارسات أمن المعلومات الموصى بها. ويتضمن ذلك على سبيل المثال اتفاقيات مستوى الخدمات والمستندات المناسبة وتنفيذ الضوابط الأمنية المتفق عليها وغير ذلك.

PR 7 أن تتضمن إجراءات تقديم المنتجات بصورة آمنة تدابير للكشف عن أعمال العبث أو التخفي.

وعلاوة على البند PR 6، تكفل المؤسسة أن تتضمن إجراءات نقل وتسليم المنتج تدابير للكشف عن أعمال العبث بالمنتجات أو إخفاءها، مثل التحقق من وجود أختام المنتجات وغير ذلك.

يساعد ذلك المؤسسة في الكشف عن المنتجات المادية الزائفة أو المجددة أو التي يتم العبث المادي بها من أجل السماح لمستخدمي البرامج الضارة بالتجسس عليها. وتساعد الضوابط الإضافية، مثل مراجعات الأكواد، المؤسسة في الكشف عن البرمجيات الضارة.

PR 8 أن يتم شراء المنتجات من الجهات المطورة التي تلتزم بإجراء عمليات صيانة مستمرة لمنتجاتها.

بالإضافة إلى البندين PR1 و PR3، ينبغي أن تتأكد المؤسسة من قيامها باختيار الموردين/ المطورين الذين يبدون التزامهم على المدى الطويل واستمرارهم في الحفاظ على منتجاتهم وتطويرها.

ويوصى بصفة عامة بالالتزام بالمنتجات/ الأنشطة الأساسية لأي مطور. وعلى سبيل المثال، تعد شركة إنتل Intel رائدة إنتاج أجهزة المعالجة الدقيقة على مستوى العالم. ومع ذلك، فإذا شرعت شركة Intel غدا في بيع أجهزة الحاسوب الشخصي أو الخوادم، قد لا يكون شراء أجهزة الحاسوب الشخصي أو الخوادم منها بمثابة فكرة جيدة بالضرورة، نظرا لأنها لا تمثل مجال نشاطها الرئيسي.

PR 9 أن تكون هناك عمليات لتطوير وتحديث المنتجات. وينبغي أن تلتزم التحديثات بسياسات إدارة التغيير المحددة بالفصل B-5 بعنوان "إرشادات حول إدارة التغيير" [CM].

ينبغي أن تكفل المؤسسة تحديث وتطوير جميع المنتجات التي يتم شراؤها بانتظام وفقا لما تحدده السياسة الأمنية للمؤسسة. ويتم إجراء عمليات التحديث والتطوير بعد تقييم المخاطر بالصورة الواجبة وبما يتماشى مع سياسات إدارة التغيير المحددة بالفصل B-5 بعنوان "إدارة التغيير".

6 - إرشادات حول أمن البرمجيات [SS]

1-6 أهداف السياسة

2-6 إرشادات حول السياسة والضوابط الرئيسية – تطوير وحيازة البرمجيات

SS 1 أن يتم دراسة تضمين الأمن في جميع مراحل دورة حياة تطوير البرمجيات/ النظام وأن يكون جزءا لا يتجزأ من مشروع تطوير وتنفيذ البرمجيات.

تعد تطبيقات البرمجيات (نظام التشغيل، التطبيقات، قاعدة البيانات ...الخ) أساس أي نظام معلومات. ولا تحظى أقوى البرمجيات بفائدة مجدية دون نظام تشغيل مناسب وتطبيق متصل به يطلق العنان لقدراته.

ومع ذلك، يجدر الإشارة إلى أن ملاءمة البرمجيات (نظام التشغيل، التطبيقات ...الخ) لا تمكن في قدرتها على توفير مجموعة متنوعة من الحلول العملية فحسب، بل في استكمالها من خلال بيئة آمنة أيضا.

ينبغي أن تكفل المؤسسة وضع الأمن في الاعتبار خلال جميع مراحل دورة حياة تطوير البرمجيات. وتتألف دورة حياة تطوير البرمجيات من المراحل التالية:

أ- الاستهلال

ب- الحيازة/ التطوير

ت- التنفيذ

ث- التشغيل/ الصيانة

ج- التخلص

SS 2 أن يتم تصنيف جميع التطبيقات (بما في ذلك الجديدة والمطورة) باستخدام سياسة تصنيف المعلومات الوطنية [IA-NAT-CLAS] وأن تحظى بالحماية الأمنية الملائمة لتصنيفات سرية وسلامة وإتاحة المعلومات.

بناءً على سياسة تصنيف المعلومات الوطنية، تجري المؤسسة تقييم الحساسية (المعلومات، الخسائر المحتملة، القوانين واللوائح، المخاطر، المخاوف البيئية، الخصائص الأمنية ...الخ) للتأكد من سرية وسلامة وإتاحة التصنيفات.

وعلاوة على ذلك، تجري المؤسسة عملية تقييم المخاطر الأولية للتأكد من بيئة المخاطر التي سوف يعمل بها النظام.

يتم دمج نتائج تدريب تقييم المخاطر ضمن عملية صنع القرار فيما يتعلق بتطوير/ حيازة النظام.

SS 3 أن يتم تطوير وتنفيذ المتطلبات الأمنية (المتطلبات الوظيفية والتقنية ومتطلبات التأمين) كجزء من متطلبات النظام.

بناءً على نتائج تدريب تقييم المخاطر، تقوم المؤسسة بتحليل المتطلبات الأمنية (المتطلبات الوظيفية والتقنية ومتطلبات التأمين) للتطبيقات وتضع ضوابط للتخفيف من حدة المخاطر. وتعد تلك الضوابط بمثابة جزء أساسي من تصميم وتنفيذ النظام.

ينبغي أن تكفل المؤسسة تطبيق المتطلبات التالية على مرحلة التصميم ثم تطبيقها على النظام:

1- استراتيجيات عمل نسخ احتياطية البيانات: تتضمن المتطلبات مدى تكرار عمل نسخ احتياطية من البيانات وتفاصيل وسائط الاحتياطي وامتيازات الوصول إلى النسخ الإحتياطية وما إذا كانت النسخ الاحتياطية مشفرة. وتوفر هذه المتطلبات مدخلات، بينما تحد من متطلبات التخزين الخاصة بالنظام. وعلاوة على ذلك، تكفل الوفاء متطلبات المعلومات C-I-A.

2- استراتيجيات نقل البيانات: يتم اختيار أسلوب مناسب لنقل/ تبادل المعلومات، بناءً على تصنيف المعلومات/ النظام. وينبغي أن تدرس المؤسسة متطلبات مثل تشفير البيانات أثناء النقل والتشفير النهائي وأي ضوابط أمنية أخرى وغير ذلك.

3- المتطلبات الأمنية لتخزين البيانات: تخضع المتطلبات الأمنية للبيانات المختزنة لتصنيف البيانات. ويتم التركيز بصورة أكبر على البيانات اللازمة للتوثيق، مثل تطبيق التشفير من جانب واحد.

4- إستراتيجية التوثيق: ينبغي أن تكفل المؤسسة تنفيذ إستراتيجية التوثيق المناسبة التي تعتمد على تصنيف النظام، حيث تكون هذه الإستراتيجية بمثابة نقطة الدخول إلى النظام.
تتمثل بعض الأمور التي يمكن دراستها في سياسة كلمة المرور القوية وتوثيق العاملين للتطبيقات الهامة واستراتيجيات التحقق من المدخلات وفترة توقف عمل الحساب وإغلاق الحساب وآلية استرجاع كلمة المرور وإستراتيجية تخزين اسم المستخدم/ كلمة المرور.

5- وضع حدود الثقة ومستويات الثقة والاستحقاقات ومتطلبات التشفير: تتولى المؤسسة تحليل وتحديد مستويات الثقة وحدود الثقة في السياق الكلي لكيفية تدفق المعلومات داخل النظام وكيفية تدفق المعلومات داخل البنية الأساسية، بما في ذلك الاتصال بالأنظمة الخارجية (فيما بين الأجهزة وداخل الجهاز الواحد). وسوف تفي المتطلبات بشرط أمني واسع النطاق في إطار السياق الكلي.
تدرس المؤسسة الضوابط الأمنية الإضافية حيث ينخفض مستوى الثقة. ويساعد تصنيف البيانات على تحديد متطلبات التشفير. وينبغي أيضا أن يتم تحديد وتوثيق تفاصيل التشفير، مثل لوغاريتم التشفير ولوغاريتم الاختزال والطول الأساسي، في وثيقة التصميم. وبالمثل، ينبغي أن يتم تحديد متطلبات الوصول إلى

المعلومات. ويجب أن تحدد وثيقة التصميم الكيانات والموارد. وينبغي أن تحدد أيضا مستوى وصول أي كيان إلى الموارد داخل النظام.

6- تصميم سجلات المراجعة والتدقيق: ينبغي أن تحدد المؤسسة متطلبات تسجيل الأداء من أجل تحقيق متابعة وإدارة واستكشاف النظام بصورة فعالة. ويجب أن يتم الاتفاق على إستراتيجية إدارة السجلات والاحتفاظ بها. وينبغي أن يكفل مصممو النظام ألا تساعد سجلات المراجعة والتدقيق في التعرف على أخطاء النظام فحسب، بل في الربط بالسجلات الأخرى المتعددة من أجل تحديد أنماط الكشف عن أخطاء النظام و/أو الهجمات التي يتعرض لها.

7- إعداد وتنفيذ وثيقة أفضل الممارسات الأمنية للبنية الأساسية (دعم النظام) لمعالجة نظام التشغيل وخادم الويب وخادم التطبيقات وقاعدة البيانات و FTP والبريد الإلكتروني: سوف تساعد هذه الوثيقة على دعم تأمين البنية الأساسية وينبغي أن يتم إعدادها خلال مرحلة التصميم.

SS 4 أن يتم إتاحة البنية الأساسية المخصصة للاختبار والتطوير (الأنظمة والبيانات) وأن تكون منفصلة عن أنظمة الإنتاج. وعلاوة على ذلك، يكون تدفق المعلومات بين الكيانات محدودا للغاية وفقا لسياسة محددة وموثقة، بحيث يحظى مستخدمو النظام الذين تتطلب مسئوليات عملهم ذلك بإمكانية الوصول إلى المعلومات ويتم تعطيل إمكانية الوصول إلى الكتابة على المصدر المسؤول عن البرمجيات.

ينبغي أن تكفل المؤسسة توافر البنية الأساسية المخصصة للاختبار والتطوير وأن تكون منفصلة عن أنظمة الإنتاج. ويهدف ذلك إلى ضمان ألا يعاني الإنتاج من أي خرق أو توقف نتيجة لأعمال التطوير التي يتم تنفيذها. ويتعين على المؤسسة أيضا أن تكفل حماية بيانات المعلومات وعدم استخدام بيانات الإنتاج المباشر في أعمال التطوير. ويجب على شركات التطوير أن تتولى تطوير بيانات الاختبار الخاصة بها لمنع تسرب أي معلومات.

وتحدد المؤسسة السياسات والإجراءات التي تنظم وتحمي عملية التطوير. ويتم تحديد الضوابط اللازمة لتدفق المعلومات بين أنظمة المعلومات والاختبار والإنتاج. وسوف تخضع إمكانية الوصول إلى الأنظمة إلى الحاجة إلى المعرفة أو الحاجة إلى الحيازة.

ويتم تفعيل الضوابط الإضافية للوصول إلى المعلومات، بما في ذلك تسجيل الأداء والتدقيق من أجل ضمان حماية المصدر الموثوق للبرمجيات. ويتم تحديد الإجراءات كي تتحكم في إدارة مراجعة البرمجيات، بما في ذلك النشر.

SS 5 أن يتم إتاحة جميع التطبيقات (المكتسبة و/أو المطورة) لاستغلالها في الإنتاج فقط بعد إجراء الاختبارات والفحوص الملائمة لتوكيد الجودة والأمن لضمان التزام النظام بالمتطلبات الأمنية المستهدفة.

تكفل المؤسسة توافق جميع التطبيقات (المكتسبة و/أو المطورة) مع معيار القبول المحدد. ويتضمن معيار القبول التوافق مع اختبارات توكيد الجودة والأمن الملائمة.

ينبغي أن تضع المؤسسة إجراءات لضمان عدم نشر أي تطبيقات في نظام الإنتاج، ما لم تجتاز الاختبارات المناسبة لتوكيد الجودة والأمن.

SS 6 أن تستخدم شركات تطوير البرمجيات ممارسات البرمجة الآمنة عند كتابة البرمجيات، بما في ذلك:

أ. الالتزام بأفضل الممارسات، وعلى سبيل المثال أخطر 25 خطأ برمجي [Mitre].

ب. تصميم البرمجيات كي تستخدم أدنى مستويات التميز من أجل تحقيق مهمتها.

ج. رفض الوصول إلى المعلومات افتراضيا.

د. فحص مستوى الاستجابة لاستدعاءات البرنامج.

هـ. التحقق من سلامة جميع المدخلات.

ينبغي أن تكفل المؤسسة تدريب شركات التطوير على استخدام ممارسات البرمجة الآمنة عند كتابة البرمجيات. ويوفر كتيب تأمين المعلومات الوطنية إرشادات حول بعض العوامل التي يتم دراستها لضمان أن يعكس أسلوب البرمجة أسلوب ترميز آمن.

ينبغي الالتزام بإرشادات الترميز الآمنة، مثل الخطوط الإرشادية لمشروع أمن تطبيقات الويب المفتوحة (OWASP).

SS 7 أن تتم مراجعة و/أو اختبار البرمجيات للكشف عن نقاط الضعف قبل استخدامها في بيئة الإنتاج. ولابد أن تتم مراجعة و/أو اختبار البرمجيات من قبل طرف مستقل وليس من قبل شركة التطوير.

ينص كتيب تأمين المعلومات الوطنية على اختبار البرمجيات (المكتسبة و/أو المطورة) للكشف عن نقاط الضعف قبل استخدامها في بيئة الإنتاج.

ويمكن استخدام الآليات التالية لتحليل مدى قوة أمن البرمجيات. ومع ذلك، يوصى بتنفيذ مثل هذه الاختبارات/ المراجعات من قبل طرف آخر أو إدارة مستقلة لتوكيد الجودة داخل المنظمة.

1- مراجعة البرمجيات الخاصة بالخطوط الإرشادية للترميز الآمن: تساعد مراجعة البرمجيات في تحديد جرثومات الحاسوب أو ممارسات البرمجيات السيئة. ويمكن أن يساعد ذلك في التخفيف من حدة نقاط الضعف في البرمجيات التي يمكن أن يستغلها المهاجمون.

هناك بعض الأدوات الآلية المتاحة بالسوق لإجراء مراجعة البرمجيات الأمنية.

2- تقييم نقاط الضعف/ اختبار الاختراق/ القرصنة الأخلاقية: تساعد مثل هذه الاختبارات على تحديد نقاط الضعف الأمنية في أي تطبيق بالسياق العام للبنية الأساسية.

يمكن أن تستفيد الشركات من هذا الاختبار في دعم تطبيقاتها والبنية الأساسية ذات الصلة.

3- اختبار التشفير: لا فائدة من استخدام التشفير إذا لم يكن آمنا بالصورة الكافية. فمن خلال أدوات مثل جداول قوس قزح، يكون من الأسهل نسبيا فك التشفير.

ومن ثم، ينبغي أن تختبر الشركات قوة التشفير المستخدم. وتعد الإدارة الآمنة لمفتاح التشفير على نفس القدر من الأهمية .

وينبغي أيضا اختبار التطبيقات بواسطة تقنيات التطبيقات المتخصصة لإختبار الأمن مثل SAST (التطبيق الثابت لاختبار الأمن)، DAST (التطبيق الديناميكي لاختبار الأمن)، وIAST (التطبيق التفاعلي لاختبار الأمن). (ينصح بإستخدام تكنولوجيا SAST لاختبار المصدر /الوحدات الثنائية/الارقام الثنائية من كافة التطبيقات / حزم البيانات الجاهزة المكتسبة أو حزم البيانات المقدمة من طرف ثالث) . وينبغي اختبار تطبيقات الويب المقدمة من طرف ثالث في بيئة التشغيل (ينصح بتكنولوجيا DAST للاختبار)

SS 8 أن يلتزم النظام (المكتسب و/أو المطور) بجميع المتطلبات القانونية، بما في ذلك التراخيص وحقوق الطبع والنشر وحقوق الملكية الفكرية...الخ.

ينبغي أن تكفل المؤسسة التزام جميع الأنظمة بكل المتطلبات القانونية، مثل الترخيص وحقوق النشر وحقوق الملكية الفكرية وغير ذلك.

يتم ترخيص جميع البرمجيات والأجهزة على مدار دورة حياتها. وتكفل المؤسسة التزامها بمتطلبات ترخيص البرمجيات/ الأجهزة في جميع الأوقات. وينبغي أن تكفل المؤسسة عدم انتهاك حقوق الملكية الفكرية.

تكفل المؤسسة التزامها بجميع المتطلبات القانونية (القوانين واللوائح) السارية في ذلك الوقت والالتزام أيضا باللوائح القانونية التي يمكن صياغتها في المستقبل.

SS 9 أن يتم توثيق جميع الأنظمة (المكتسبة و/أو المطورة) بالصورة الملائمة.

يعد التوثيق عملية رئيسية في أي نظام. ويجب أن تكفل المؤسسة توثيق جميع البرمجيات/ الأنظمة (المكتسبة/ المطورة) بالأسلوب المناسب. ويتضمن التوثيق ما يلي:

1- وثيقة المتطلبات: يعد توثيق المتطلبات وصفا لما تقوم به البرمجيات المحددة أو تحققه. ويتم استخدامه على مدار عملية التطوير للتعرف على ما تقوم به البرمجيات. ويتم استخدامه أيضا كاتفاق أو أساس للاتفاق على ما تحققه البرمجيات.

سوف تنطوي هذه الوثيقة على المتطلبات الأولية لتصميم النظام/ التطبيق المكتسب و/أو المطور. وعلى سبيل المثال: طلب تقديم العروض/ طلب عروض الأسعار أو أي وثيقة أخرى مماثلة.

2- وثيقة الهندسة/ التصميم: يعد التوثيق الهندسي بمثابة وثيقة تصميم رفيعة المستوى. وتمثل الوثائق الهندسية المشتق الثالث من البرمجيات (حيث تكون وثيقة التصميم هي المشتق الثاني، ووثائق البرمجيات هي المشتق الأول). ولا تتضمن الوثائق الهندسية أي شيء محدد للبرمجيات ذاتها. ولا تصف هذه الوثائق كيفية برمجة نظام محدد أو حتى سبب وجود ذلك النظام المحدد في شكله الحالي، بل تحدد المتطلبات العامة التي تشجع على وجود ذلك النظام فقط. وقد تقترح توجهات لتصميم المستوى الأدنى.

تعد وثيقة التصميم وثيقة تفصيلية منخفضة المستوى تتضمن عناصر تصميم نظرية ومنطقية ومادية. وتحدد تفاصيل العلاقات وتدفق البيانات بين الكيانات المتعددة. وتتولى توثيق الاستراتيجيات ذات الصلة بكيفية تنفيذ المتطلبات المحددة والتوافق معها.

3- التوثيق التقني: عند إنشاء برمجيات، لا يكون الكود وحده كافيا. فلابد أن يكون هناك نص ما يصف الجوانب المتعددة للأسلوب المستهدف لإدارتها. ويمكن أن يتم استخدام هذا التوثيق، الذي يتضمن نظرة عامة حول توثيق تطبيقات البرمجيات أو منتجات البرمجيات المزمع توثيقها، من قبل شركات التطوير ومسؤولي الاختبار والمستهلكين أو العملاء النهائيين أيضا باستخدام تطبيق البرمجيات هذا. وقد أصبح التوثيق التقني هاما، حيث يتزايد عدد العمليات الهامة التي تعمل بصورة آلية وقد يتغير المستوى الأساسي والمتقدم للمعلومات ذات الصلة على مدار فترة زمنية مع حدوث التغيرات الهندسية.

4- التوثيق الوظيفي/ توثيق المستخدم: يصف توثيق المستخدم كل ملمح من ملامح البرنامج ويساعد المستخدم في تحقيق هذه الملامح. ويمكن أن توفر وثيقة المستخدم الجيد مساعدات شاملة في عملية استكشاف الأخطاء وتعديلها. ومن المهم للغاية ألا تكون وثائق المستخدم محيرة وأن تكون مستحدثة. وليس هناك حاجة لأن تكون وثائق المستخدم منظمة بصورة محددة؛ ولكن من المهم للغاية أن يتم فهرستها بصورة شاملة. ويعد التوافق والبساطة ذات قيمة كبيرة للغاية أيضا.

5- تقارير اختبار القبول: تتمثل الخطوة الأخيرة في الانتهاء من حيازة/ تطوير البرمجيات في اختبار البرمجيات لضمان حسن تشغيلها والتزامها بالتصميمات والمعايير المتفق عليه...الخ. ويمكن أن تجري المؤسسة أنماطا مختلفة من الاختبارات لضمان الموافقة النهائية. ويمكن أن تتضمن هذه الاختبارات اختبارات قبول المستخدمين لضمان حسن التشغيل ومراجعات البرمجيات واختبارات الاختراق من أجل اختبار الالتزام الأمني وإجراء مراجعة وتدقيق لضمان الالتزام بسياسات تأمين المعلومات الوطنية وغير ذلك. ويتم توثيق جميع هذه التقارير وتنفيذ بنود العمل التي تبرزها التقارير.

6- وثيقة المخاطر ونقاط الضعف: تحدد هذه الوثيقة وتوثق المخاطر أو نقاط الضعف القائمة بالنظام في وقت نشره في بيئة الإنتاج. ويتم توقيع الوثيقة من قبل القائم على إدارة الأعمال.

SS 10 أن تتم إتاحة مصدر برمجيات التطبيقات الحساسة المطورة خصيصا، وفي حالة التطبيقات التجارية (التي تخدم التطبيقات/ العمليات الحساسة)، يتعين على المؤسسة النظر في خيارات توفير ضمان لمصدر البرمجية.

ينبغي أن تكفل المؤسسة إتاحة مصدر برمجيات التطبيقات الحساسة المطورة خصيصا داخل المؤسسة أو من خلال أي طرف آخر من أجل إجراء مراجعات البرمجيات وتأمين ذلك المصدر بالصورة الملائمة لحماية سريته وسلامته وإتاحته.

وفي حالة التطبيقات التجارية الجاهزة للاستخدام (التي يتم تعديلها وفقا للمتطلبات) مع التطبيقات والعمليات الحساسية، يتعين على المؤسسة النظر في خيارات توفير ضمان لمصدر البرمجية. وتعد اتفاقية الضمان بمثابة اتفاقية يتم إبرامها بين المؤسسة ومطور البرمجيات، حيث يوافق المطور على إيداع مصدر البرمجية المستحدث لدى طرف آخر يقوم بدور الوصي.

في أسوأ السيناريوهات، حيث لا يكون مطور البرمجيات في وضع يسمح له بالاحتفاظ بالبرمجيات لأسباب مثل الإفلاس أو عمليات الاندماج/ الشراء من قبل شركات أخرى أو تغيير خارطة الطريق أو غير ذلك، يحق للمؤسسة شراء مصدر البرمجية من الوصي حتى تتمكن من مواصلة الحفاظ على تطبيقاتها الحساسة.

SS 11 أن يتم المصادقة على التطبيقات قبل تنفيذها وفقا لما محدد بالفصل B-13 بعنوان "التدقيق و إصدار الشهادات" [AC].

ينبغي أن تكفل المؤسسة اعتماد جميع تطبيقات البرمجيات الجديدة قبل تنفيذها باعتبارها برمجيات إنتاج. ومع ذلك، يمكن أن تؤجل المؤسسة عملية الاعتماد لضمان أن تتماشى مع خارطة طريقها بموجب موافقة رئيس المؤسسة/ مدير إدارة المراجعة والتدقيق الداخلي. وتتولى أيضا إخطار جهاز المراجعة والتدقيق بقطر بذلك.

3-6 السياسة والضوابط الرئيسية – تطبيقات البرمجيات

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

SS 12 أن يتم توثيق جميع أهداف وآليات أمن الخوادم ومحطات العمل ضمن خطة أمن النظام المعنية.

ينبغي أن تكفل المؤسسة تصنيف نظام المعلومات (الخوادم، محطة العمل، البرمجيات ذات الصلة) وتحديد وتوثيق الضوابط الأمنية ذات الصلة. ويتم دعم جميع الأجهزة وفقا لتصنيفها وبمقتضى الضوابط الأمنية المتفق عليها والمذكورة ضن خطة أمن النظام المعنية.

SS 13 أن تخضع حاسبات نقاط العمل لبيئة عمل مؤمنة وموحدة تغطي ما يلي:

أ. إلغاء البرمجيات غير اللازمة.

ب. تعطيل أسلوب العمل غير المستغل أو غير المستحب في البرمجيات وأنظمة التشغيل التي تم تركيبها.

ج. تطبيق ضوابط الوصول إلى المعلومات على البنود ذات الصلة لقصر إمكانية وصول مستخدمي النظام والبرامج على الحد الأدنى اللازم لأداء المهام والواجبات.

د. تنصيب الجدران النارية القائمة على البرمجيات والتي تحد من الاتصالات الصادرة والواردة من وإلى الشبكة.

هـ. تهيئة تسجيل الأداء عن بعد أو نقل سجلات الأداء المحلية إلى خادم مركزي.

ينص كتيب تأمين المعلومات الوطنية على الضوابط الأساسية التي يتم وضعها في الاعتبار أثناء دعم بيئة العمل القياسية.

SS 14 أن يتم الحد من نقاط الضعف المحتملة في بيئة العمل القياسية المدعمة وفي الأنظمة عن طريق:

أ. إلغاء عملية تبادل الملفات غير اللازمة.

ب. ضمان تحديث عملية تعديل البرمجيات.

ج. تعطيل إمكانية الوصول إلى أسلوب عمل المدخلات/ المخرجات غير الضرورية.

د. إلغاء الحسابات غير المستخدمة.

هـ. إعادة تسمية الحسابات الافتراضية.

و. استبدال كلمات المرور الافتراضية.

ينص كتيب تأمين المعلومات الوطنية على الضوابط الأساسية التي يتم وضعها في الاعتبار لضمان التخفيف من حدة نقاط الضعف في النظام. ويتم دمج هذه الضوابط ضمن بيئة العمل القياسية المنتشرة بالمؤسسة لتحقيق الحد الأدنى من الحماية الأمنية.

SS 15 الخوادم ذات المخاطر المرتفعة، مثل الويب والبريد الإلكتروني والملفات وخوادم الاتصالات الهاتفية الخاضعة لبروتوكول الإنترنت وغيرها، التي تتصل بالشبكات العامة غير الخاضعة للرقابة:

أ. الفصل الوظيفي الفعال بين الخوادم بما يسمح لتلك الخوادم بأن تعمل بصورة مستقلة.

ب. الحد من الاتصالات بين الخوادم بكل من الشبكة ومستوى نظام الملفات، حسب الاقتضاء.

ج. قصر وصول مستخدمي النظام والبرامج على الحد الأدنى اللازم لأداء المهام والواجبات.

ينص كتيب تأمين المعلومات الوطنية على أن تحظى الخوادم التي تدير الخدمات الهامة و/أو تخضع لنطاقات المخاطر المرتفعة في الأساس (وعلى سبيل المثال: خوادم الويب والبريد الإلكتروني في المناطق منزوعة السلاح) للضوابط الأمنية الإضافية القائمة من أجل التخفيف من مخاطر الإضرار بالخوادم الأخرى عند تعرضها لتلك المخاطر.

SS 16 فحص سلامة جميع الخوادم التي تحظى وظائفها بأهمية لدى المؤسسة وتلك الخوادم التي تتعرض لمخاطر كبيرة. وينبغي متى أمكن أن يتم إجراء هذه الفحوص من قبل بيئة موثوقة بدلا من النظام ذاته.

ينص كتيب تأمين المعلومات الوطنية على تنفيذ الضوابط من أجل متابعة سلامة الخوادم التي تحظى وظائفها بأهمية لدى المؤسسة و/أو تلك الخوادم التي تتعرض لمخاطر كبيرة.

ويوصى بإجراء هذه الفحوص من قبل بيئة موثوق بها، ويفضل أن يكون نطاق آمن يحظى بمستوى أمني مماثل للخوادم التي يتم متابعة سلامتها أو مستوى أمني أعلى. ويوصى أن تخضع عملية المتابعة لإدارة مركزية لضمان فاعلية التدقيق والمتابعة بدلا من خضوعها لوكلاء مستقلين مسؤولين عن كل خادم.

SS 17 تخزين معلومات السلامة بصورة آمنة بعيدا عن الخادم بأسلوب يحافظ على السلامة.

بالإضافة إلى البند SS16، ينص كتيب تأمين المعلومات الوطنية على تخزين معلومات السلامة (على سبيل المثال: قواعد الاختزال وغيرها) بصورة آمنة بعيدا عن الخادم. ويوصى بتخزين معلومات السلامة في خادم الإدارة الكائن في بيئة آمنة وموثوقة. ويتم تصنيف معلومات السلامة عند المستوى I3 ويتم تأمينها وفقا لذلك.

SS 18 تحديث معلومات السلامة عقب كل تغيير قانوني في النظام.

بالإضافة إلى البندين SS16 و SS17، ينبغي أن يكفل مديرو أمن النظام تحديث المعلومات في جميع الأوقات من أجل فحص ومتابعة السلامة بفاعلية.

ينبغي أن يكفل مدير أمن المعلومات أن يتضمن توثيق النظام المستحدث تحديث معلومات السلامة كجزء من البند CM5 بالفصل "ب" بعنوان "إدارة التغيير". وسوف يؤدي ذلك إلى منع ظهور إيجابيات زائفة حينما يخضع النظام لتغيير قانوني.

SS 19 مقارنة معلومات السلامة المختزنة بمعلومات السلامة الحالية لتحديد ما إذا كان قد حدث تسوية أو تعديل قانوني ولكنه غير مكتمل بالصورة الصحيحة، كجزء من جدول التدقيق المستمر بالمؤسسة.

بالإضافة إلى البند SS17، ينص كتيب تأمين المعلومات الوطنية على أن يتضمن جدول التدقيق بالمؤسسة فحص سلامة الخوادم ضمن نطاقه.

يقارن المدقق معلومات السلامة الحالية بمعلومات السلامة المختزنة لتحديد ما إذا كان قد حدث تسوية أو تعديل قانوني ولكنه غير مكتمل بالنظام بصورة صحيحة.

يتم إجراء الفحص على فترات منتظمة حتى تصبح فحوص السلامة بمثابة ضوابط وأدوات أمنية فعالة.

SS 20 تسوية أي تعديلات يتم الكشف عنها وفقا لإجراءات إدارة الحوادث الأمنية لتكنولوجيا الاتصالات والمعلومات بالمؤسسة.

يشير الكشف عن أي تعديل إلى ارتفاع إمكانية تعرض النظام للمخاطر. وينبغي أن تكفل المؤسسة التعامل مع الكشف عن أي تعديل وفقا لإجراءات إدارة الحوادث الخاصة بها.

SS 21 أن تتم مراجعة جميع التطبيقات لتحديد ما إذا كانت تحاول الاتصال بأية أجهزة أخرى. وفي حالة إمكانية تفعيل خاصية الإتصال الآلي لبعض البرمجيات، يتعين على المؤسسة اتخاذ قرار عملي لتحديد ما إذا كان ينبغي السماح بتفعيل هذه الخاصية، بما في ذلك تقييم المخاطر التي ينطوي عليها ذلك القرار.

يتولى مديرو أمن المعلومات، كجزء من اختبارات مراجعة البرمجيات ونقاط الضعف، تحليل سلوك التطبيق. وينبغي أن يراجع مديرو أمن المعلومات تصميم تدفق المعلومات بالتطبيق والمكونات المتعددة لأي بنية أساسية يتصل بها ونمط تلك الوصلات.

ينبغي أن يكفل مديرو أمن المعلومات التزام المنتجات النهائية بوثيقة التصميم. ويكفل هؤلاء أن تتماشى الوصلات الخاصة بالتطبيقات بالضوابط المحددة لتصنيفها. وعلى سبيل المثال: استخدام القنوات الآمنة للمعلومات المصنفة عند المستوى C3.

وعلاوة على ذلك، يكفل مديرو أمن المعلومات أن تتماشى منافذ الاتصالات التي يستخدمها التطبيق مع سياسة شبكة المؤسسة.

يجري مدير أمن المعلومات عملية تقييم المخاطر من أجل تقييم التهديدات والمخاطر الناجمة عن السماح بتلك الوصلات؛ ويمثل ذلك أساسا لقيام المسؤولين عن إدارة العمل بتأييد هذه الوصلة أو إلغائها.

4-6 السياسة والضوابط الرئيسية – تطبيقات الويب

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

SS 22 أن تتم مراجعة كل المحتوى الفعال بخوادم الويب الخاصة بها لأسباب أمنية. وينبغي أن تلتزم المؤسسة بالوثائق المنصوص عليها بدليل مشروع أمن تطبيقات الويب المفتوحة من أجل بناء تطبيقات وخدمات ويب آمنة.

تفضل شركات التطوير التطبيقات القائمة على الويب إلى حد كبير، حيث تسمح باستخدام برامج الحاسوب المعيلة (thin client) وتيسر من نشر التطبيقات بين عدد كبير من المستخدمين دون الحاجة إلى تنصيب برامج مستقلة على كل جهاز حاسوب وتحظى بمرونة تسمح بوجود أجهزة حاسوب متسقة وحرية وجود أنظمة معالجة داخلية متنوعة.

ومع ذلك، تثير هذه السهولة الكثير من المخاوف الأمنية. وقد أثبتت سنوات طويلة من البحوث وجود العديد من نقاط الضعف بخوادم وبروتوكولات الويب، وبالتالي، تطبيقات الويب.

ينص كتيب تأمين المعلومات الوطنية على أن تكفل المؤسسة ممارسة العناية الواجبة في فحص ومراجعة المحتوى الفعال بخوادم الويب. وينص كتيب تأمين المعلومات الوطنية على التزام المؤسسة بممارسات البرمجة الآمنة. ويوصي الكتيب باستخدام دليل مشروع أمن تطبيقات الويب المفتوحة من أجل بناء تطبيقات وخدمات ويب آمنة.

SS 23 أن يتم خفض الاتصال والوصول بين كل من مكونات تطبيقات الويب إلى الحد الأدنى.

ينص كتيب تأمين المعلومات الوطنية على خفض الاتصال والوصول بين كل من مكونات تطبيقات الويب والأطراف الرئيسية المتعددة إلى الحد الأدنى على أساس "الحاجة إلى المعرفة". ويؤدي ذلك إلى الحد من المخاطر ذات الصلة بالوصلات المفتوحة.

SS 24 أن تتم حماية المعلومات الشخصية والبيانات الحساسة أثناء التخزين والنقل باستخدام ضوابط التشفير الملائمة.

ينص كتيب تأمين المعلومات الوطنية على أن تضع المؤسسة ضوابط كافية لتأمين المعلومات الشخصية والبيانات الحساسة التي يتم جمعها من خلال بوابات الويب. وينبغي أن تتم حماية البيانات أثناء النقل والتخزين.

SS 25 أن تستخدم المواقع الإلكترونية التي ينبغي توثيقها شهادات SSL التي يوفرها مقدم خدمة الشهادات الذي يحظى بترخيص داخل دولة قطر.

ينص كتيب تأمين المعلومات الوطنية على أن تستخدم البوابات الإلكترونية التي ينبغي توثيقها شهادات SSL التي يوفرها مقدم خدمة الشهادات الذي يحظى بترخيص داخل دولة قطر. ولحين وجود G-PKI، تصدر وزارة الداخلية مثل هذه الشهادات.

SS 26 الجدار الناري لحماية تطبيقات الويب (WAF) يجب أن تستخدم للتطبيقات ذات تصنيف الحساسية المتوسط او المرتفع.

تطبيقات الويب ذات التصنيفات المتوسطة أو العالية يجب أن تكون محمية باستخدام جدار حماية تطبيق ويب (WAF). WAF يمنع العديد من نقاط الضعف بالتطبيق من الوصول إلى التطبيق. تجدر الإشارة إلى أن شبكة الجدران النارية لا تحتوي على هذه الخاصية. (WAF تعمل في طبقة التطبيقات من طراز OSI بينما تعمل الجدران النارية الشبكة في طبقة النقل وطبقة الشبكة).

5-6 السياسة والضوابط الرئيسية – قواعد البيانات

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

SS 27 أن ترتبط جميع المعلومات التي يتم تخزينها داخل أي قاعدة بيانات بتصنيف ملائم إذا كانت تلك المعلومات:

أ. يمكن تصديرها إلى نظام مختلف أو

ب. تتضمن تصنيفات مختلفة و/أو متطلبات معالجة مختلفة.

ينبغي أن تكفل المؤسسة تصنيف جميع المعلومات داخل قاعدة البيانات ووسمها بالصورة الملائمة، وخاصة إذا أمكن تصدير البيانات إلى نظام آخر أو كانت تلك البيانات تتضمن تصنيفات متعددة.

SS 28 ينبغي أن تكفل المؤسسة تطبيق التصنيفات بمستوى من التفاصيل والوضوح يكفي لتحديد متطلبات معالجة وتداول أي معلومات يتم استرجاعها أو تصديرها من أي قاعدة بيانات.

بالإضافة إلى البند SS26، ينص كتيب تأمين المعلومات الوطنية على أنه عند تطبيق تصنيف قاعدة البيانات بمستوى من التفاصيل، يكفي أن يتم تحديد متطلبات معالجة أي معلومات يتم استرجاعها أو تصديرها من أي قاعدة بيانات.

يسري ذلك بصفة خاصة على قواعد البيانات الكبرى (RDBMS و ERP وغيرها)، حيث يتم تخزين كميات كبيرة من المعلومات والربط بينها. ولا تحظى جميع المعلومات بنفس التصنيف C-I-A. ومن الضروري أن يتم تصنيف المعلومات بصورة عملية بمستوى من التفاصيل يكفل ضوابط أمنية مناسبة.

SS 29 أن يتم حماية ملفات قواعد البيانات من الوصول إليها بما يتجاوز ضوابط الوصول الطبيعية لقاعدة البيانات.

ينبغي أن تكفل المؤسسة تأمينا ملائما لقواعد البيانات. وتحظى أي قاعدة بيانات بصفة عامة بضوابط الوصول الخاصة بها. ويجب أن تكفل المؤسسة عدم إمكانية تجاوز هذه الضوابط.

ويتم تحقيق ذلك من خلال منع الوصول إلى ملفات قاعدة البيانات باستخدام وظائف (جوهر) نظام التشغيل. ويتم تدقيق الوصول إلى قواعد البيانات ومراجعة السجلات على فترات منتظمة.

SS 30 أن توفر قواعد البيانات أسلوب العمل بما يسمح بتدقيق إجراءات مستخدمي النظام.

ينص كتيب تأمين المعلومات الوطنية على أن تدعم قواعد البيانات أعمال التدقيق التفصيلية. ويمكن أن يتم تدقيق تحركات مستخدمي النظام. ويتضمن ذلك الوظائف الإدارة، مثل تأسيس قاعدة البيانات وحذفها وتعديل الجداول وتعديل حقوق المستخدمين وغير ذلك.

SS 31 لا يستطيع مستخدمو النظام، ممن ليس لديهم امتياز كافي للاطلاع على مضمون قاعدة البيانات، رؤية البيانات الوصفية ذات الصلة ضمن قائمة نتائج البحث الصادرة عن محرك البحث. وفي حالة عدم القدرة على تنقية نتائج البحث في قاعدة البيانات بالصورة الملائمة، يتعين على المؤسسة ضمان سلامة جميع نتائج البحث من أجل الوفاء بالحد الأدنى لمتطلبات الأمن لدى مستخدمي النظام.

ينبغي أن تكفل المؤسسة عدم إمكانية التلاعب بتصنيف المعلومات وضوابط الوصول داخل نظام قاعدة البيانات.

ويخضع الوصول إلى المعلومات، في الأساس، لقاعدة "الحاجة إلى المعرفة" أو "الحاجة إلى الحيازة". وإذا ما تضمنت قاعدة البيانات معلومات مصنفة عند مستويات مختلفة، يتم تصنيف البيانات على مستويات تفصيلية ويتم مراقبة الوصول إلى المعلومات على مستوى تفصيلي.

يكفل ذلك عدم وصول المستخدمين إلى المعلومات التي لا يتم السماح لهم بالاطلاع عليها.

ومع ذلك، يمكن تجاوز هذه الضوابط من خلال استخدام أنظمة البحث والمحركات المؤقتة وغيرها، حيث يمكن تنفيذ هذه العملية من خلال مستوى امتياز مختلف. ويجب أن تكفل المؤسسة وجود ضوابط لمنع سوء الاستخدام، وخاصة من قبل مستخدمي النظام.

ينبغي أن تكفل المؤسسة أيضا أن يحظى مديرو قواعد البيانات بحقوق كافية لتنفيذ هذه المسؤوليات، وأن يتم فرض قيود على مستوى البيانات الوصفية في ذات الوقت.

سوف تحظى قواعد البيانات الحساسة، أي التي تتضمن بيانات مصنفة عند المستوى C3 أو أكثر، بعناية خاصة. ويجب أن تخضع امتيازات الإدارة لتقسيم كلمات المرور ومبدأ الرقابة من قبل شخصين.

SS 32 يجب إخفاء البيانات الحساسة في قاعدة بيانات باستخدام تقنية اخفاء البيانات عند المستوى C3 أو أكثر.

لقاعدة البيانات التي تحمل المعلومات المصنفة عند المستوى C3 أو أكثر يجب أن تحجب بيانات باستخدام تقنية اخفاء البيانات وذلك لمنع المسؤولين من دخول / استرجاع تلك البيانات.

7 - إرشادات حول أمن استخدام النظام [SU]

7-1 أهداف السياسة

7-2 إرشادات حول السياسة والضوابط الرئيسية

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

SU 1 أن يتولى مستخدمو الأنظمة المسؤولية عن الأصول المعلوماتية (الأنظمة/ البنية الأساسية) التي يتم تزويدهم بها لتنفيذ مسؤولياتهم الرسمية. ويقوم مستخدمو النظام بمعالجة الأصول المعلوماتية من خلال العناية الواجبة وإدارتها بما يتماشى مع سياسة الاستخدام المقبول لدى المورد/ المؤسسة.

ينص كتيب تأمين المعلومات الوطنية على أن يتولى مستخدمو الأنظمة المسؤولية عن الأصول المعلوماتية (الأنظمة/ البنية الأساسية) بالإضافة إلى إمكانية الوصول اللازم التي يتم تزويدهم بها لتنفيذ مسؤولياتهم الرسمية. وينبغي على مستخدمي الأنظمة ممارسة العناية الواجبة لضمان ألا يكونوا سببا مباشرا أو غير مباشر في إخفاق النظام أو تعرضه للمخاطر. ويجب أن يبذلوا العناية الواجبة من أجل معالجة الأصول وإدارتها وفقا للخطوط الإرشادية المحددة/ سياسات الاستخدام المقبول.

SU 2 أن يمارس مستخدمو النظام العناية الواجبة عند الدخول إلى الويب وتصفحه ويلتزم هؤلاء بمبادئ وإرشادات المؤسسة بشأن الوصول إلى شبكة الإنترنت. وينبغي أن تنظر المؤسسة في ما إذا كان استخدام المنتديات والشبكات الاجتماعية وغيرها مسموحا أو غير مسموح به.

يتم توعية مستخدمي النظام باقتصار الموارد التي توفرها المؤسسة، بما في ذلك الوصول إلى شبكة الإنترنت، على أغراض العمل. ويمكن السماح بالاستخدام الشخصي، ولكنه يخضع لسياسات المؤسسة.

تحدد المؤسسة، من جانبها، السياسات والإرشادات الخاصة بالاستخدام المقبول للويب وموارده بما يتماشى مع متطلبات عملها. وبناءً على تدريب تقييم المخاطر، تحدد المؤسسة مدى ملاءمة استخدام أساليب العمل المتعددة القائمة على الويب، مثل البريد الإلكتروني القائم على الويب والدردشة والشبكات الاجتماعية وغيرها.

SU 3 أن تتم حماية أصول تكنولوجيا الاتصالات والمعلومات من المخاطر القائمة على الويب عن طريق تنفيذ التدابير التي سوف تحول دون تنزيل البرمجيات والمضمون الفعال والمواقع الإلكترونية غير ذات الصلة بالنشاط.

ينبغي أن تكفل المؤسسة وجود ضوابط أمنية لحماية أصول تكنولوجيا الاتصالات والمعلومات من المخاطر القائمة على الويب.

ويوصي كتيب تأمين المعلومات الوطنية بإمكانية التخفيف من حدة المخاطر من خلال ضمان الضوابط التي تحول دون تنزيل البرامج من الويب والمضمون الفعال والمواقع الإلكترونية غير ذات الصلة بالنشاط. وقد وجد أن المواقع ذات الصلة بالشبكات الاجتماعية والتنزيلات المجانية والموسيقى والوصلات الإلكترونية هي المصدر الأكبر لانتشار المحتوى الضار.

سوف تتولى المؤسسة تنفيذ التوصيات السابقة بما يتماشى مع الضوابط المحددة بالبند SU1 أعلاه.

SU 4 أن يتم توفير إمكانية الوصول إلى الويب من خلال الخوادم البديلة وبوابات التنقية الآمنة وفقا لما هو محدد بالفصل C-4 بعنوان "أمن البوابة" [GS].

ينص كتيب تأمين المعلومات الوطنية على إمكانية الوصول إلى الويب من خلال الخوادم البديلة وبوابات التنقية الآمنة وفقا لما هو محدد بالفصل C-4 بعنوان "أمن البوابة" [GS]. ويكفل ذلك أن تتم إدارة سياسة الوصول إلى الويب الخاص بالمؤسسة بصورة مركزية وأن تتم متابعتها ومراقبتها بصورة فعالة.

SU 5 أن يكون العاملون على دراية بأنماط المضمون المصرح به والمحظور داخل المؤسسة وفقا لما هو محدد بالفصل B-4 بعنوان "إرشادات حول أمن البوابة" [GS]. وينبغي أن تنظر المؤسسة في إيجاد حل فعال لمتابعة مضمون القنوات المشفرة.

تكفل المؤسسة توعية العاملين بالاستخدام المقبول لموارد الويب التي يتم توفيرها لهم. وينبغي أن تتأكد المؤسسة من أن دورات التوعية الأمنية التي تنظمها تركز على الاستخدام الفعال للويب وموارده.

وعلاوة على ذلك، يتم متابعة الوصول إلى موارد الويب لضمان التزام العاملين بسياسة الويب. وينبغي أن تنظر المؤسسة في إيجاد حل فعال لمتابعة مواقع الويب المشفرة/ الآمنة. ويتم إجراء تقييم شامل للمخاطر من أجل المقارنة بين مزايا وعيوب وفاعلية مثل هذا الحل.

SU 6 أن يقوم العاملون باستخدام البريد الإلكتروني بالحيطة والحذر المطلوبين وإدراج علامات التصنيف اللازمة اعتمادا على المضمون/ المرفقات وفقا لسياسة تصنيف المعلومات الوطنية [IAP-NAT-DCLS].

ينبغي أن تتولى المؤسسة توعية العاملين بها حول الاستخدام المقبول لخدمات البريد الإلكتروني. وينبغي أن يقوم العاملون، من جانبهم، بممارسة العناية الواجبة أثناء استخدام خدمات البريد الإلكتروني المتاحة لأغراض العمل. ويمكن السماح بالاستخدام الشخصي بما يتماشى مع سياسة الاستخدام المقبول بالمؤسسة.

ينبغي أن تنظر المؤسسة في فرض قيود على استخدام هوية البريد الإلكتروني الحكومي الرسمي في المنتديات العامة ومواقع الويب غير ذات الصلة بالعمل.

ينبغي أن يقوم العاملون بتصنيف ووسم البريد الإلكتروني بالصورة الملائمة بناءً على مضمون/ مرفقات البريد الإلكتروني.

SU 7 أن يتم اتخاذ التدابير الملائمة لحماية البريد الإلكتروني من المخاطر المحتملة كالفيروسات وفيروس طروادة والرسائل التطفلية والتزوير والهندسة الاجتماعية (Social Engineering).

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بتطبيق الضوابط الأمنية المناسبة لحماية البريد الإلكتروني من المخاطر المحتملة كالفيروسات وفيروس طروادة والرسائل التطفلية والتزوير والهندسة الاجتماعية (Social Engineering) وغير ذلك.

ينبغي أن تكفل المؤسسة أن توفر دورات التوعية الأمنية التي تنظمها التوعية للعاملين بها حول المخاطر المحتملة لخدمات البريد الإلكتروني.

يوصي كتيب تأمين المعلومات الوطنية باستخدام بوابات البريد الإلكتروني في تنقية وإدارة البريد الإلكتروني ومضمونه.

SU 8 أن يكون العاملون على دراية بعدم السماح باستخدام خدمات البريد الإلكتروني العامة القائمة على الويب في إرسال واستقبال البريد الإلكتروني من أنظمة المؤسسة.

ينبغي أن تكفل المؤسسة حظر استخدام البريد الإلكتروني القائم على الويب و/أو أي خدمات بريد إلكتروني أخرى لا ترتبط بالمؤسسة. إن خدمات البريد الإلكتروني قد توفر بوابة خلفية إلى النظام لا يمكن متابعتها بفاعلية ويمكن استخدامها لاختراق النظام كقناة لاختلاس المعلومات.

تكفل المؤسسة تحقيق ذلك من خلال سياسة الاستخدام المقبول الخاصة بها. وينبغي أن تتم توعية العاملين بذلك من خلال دورات التوعية الأمنية الفعالة.

وبالإضافة إلى ذلك، ينبغي أن تدرس المؤسسة الضوابط التقنية الفعالة التي تساعد في تطبيق هذه السياسة.

SU 9 أن يكون العاملون على وعي بضرورة إرسال رسائل البريد الإلكتروني المستخدمة في تبادل المعلومات السرية إلى المستلمين المذكورين وليس إلى مجموعة أو قائمة توزيع.

يوفر كتيب تأمين المعلومات الوطنية إرشادات لمنع إرسال رسائل البريد الإلكتروني السرية إلى عناوين خاطئة. وقد يكون من الممكن أن تتضمن قائمة توزيع محددة (شخصية أو خاصة بالمؤسسة) مستقبلين آخرين بخلاف المستقبلين المستهدف إرسال البريد الإلكتروني إليهم؛ ومن ثم، يكون من الأفضل إرسال رسائل البريد الإلكتروني السرية إلى أشخاص بعينهم فقط.

تقوم المؤسسة بتوعية المستخدمين بذلك من خلال برامج التوعية الأمنية الخاصة بها.

SU 10 أن يكون العاملون على وعي بأن استخدام إعادة التوجيه التلقائية لرسائل البريد الإلكتروني تعتمد على حساسية رسائل البريد الإلكتروني العادية الخاصة بهم. وينبغي ألا يتم إعادة توجيه رسائل البريد الإلكتروني التي تحمل معلومات مصنفة عند المستوى C2 أو أكثر بصورة تلقائية إلى خارج أنظمة المؤسسة.

يوفر كتيب تأمين المعلومات الوطنية إرشادات لمنع تسرب رسائل البريد الإلكتروني السرية باستخدام إعادة التوجيه التلقائي.

يمكن السماح بإعادة التوجيه التلقائي داخل المؤسسة كما هو الحال عند قيام سكرتير بفرز البريد الإلكتروني الخاص برئيسه في العمل. ومع ذلك، ينصح بتوخي قدر من الحذر عند إعادة التوجيه التلقائي للبريد الإلكتروني إلى بدلاء مؤقتين أو زملاء يقومون بالعمل بالإنابة خلال فترة التغيب عن العمل.

لا يتم إعادة توجيه رسائل البريد الإلكتروني المصنفة عند المستوى C2 أو أكثر بصورة تلقائية إلى عنوان بريد إلكتروني خارج نطاق المؤسسة. ويكفل المستخدم وجود ضوابط أمنية كافية وموافقات (تصريح باستخدام الحسابات الشخصية من قبل المسؤول المعني عن إدارة العمل/ مدير أمن المعلومات) قبل إعادة توجيه أي بريد إلكتروني مصنف عند المستوى C2 أو أكثر خارج نظام البريد الإلكتروني الخاص بالمؤسسة.

تقوم المؤسسة بتوعية المستخدمين بذلك من خلال برامج التوعية الأمنية الخاصة بها.

SU 11 أن تكفل المؤسسة عند التعامل مع الأطراف الخارجية أن يتفهم المستقبلون أو المصدرون الخارجيون ويوافقون على استخدام البيانات المصنفة وفقا لما هو محدد بالفصل C-3 بعنوان "تبادل المعلومات" [IE].

يوفر كتيب تأمين المعلومات الوطنية إرشادات تكفل وجود الضوابط الأمنية وإجراءات معالجة المعلومات ذات الصلة لدى الطرف الخارجي. ويوصي كتيب تأمين المعلومات الوطنية بوجود اتفاقيات السرية وعدم الإفصاح ذات الصلة لدى الأطراف الخارجية وبإجراء تقييم المخاطر اللازمة قبل تبادل البيانات مع الأطراف الخارجية.

8 - إرشادات حول أمن الوسائط [MS]

8-1 أهداف السياسة

8-2 إرشادات حول السياسة والضوابط الرئيسية – تصنيف ووسم الوسائط

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

MS 1 أن يتم تصنيف الأجهزة التي تحتوي على الوسائط عند مستوى تصنيف المعلومات التي تشتمل عليها الوسائط أو أعلى من هذا المستوى.

لا تحظى الأجهزة أو الوسائط بأي قيمة بصفة عامة. وتستمد قيمتها من خلال المعلومات المختزنة عليها. وتعد الوسائط التي تحتوي على خطط وتوقعات مالية رئيسية لأي شركة وسائط أكثر قيمة وأهمية من الوسائط المماثلة التي تحتوي على نسخ من الألعاب.

ينبغي أن تكفل المؤسسة تصنيف الوسائط عند مستوى تصنيف المعلومات التي تشتمل أو قد تشتمل عليها الوسائط أو أعلى من هذا المستوى. ويهدف ذلك إلى ضمان تخصيص الضوابط المناسبة من أجل الحفاظ على الوسائط.

MS 2 أن يتم تصنيف الوسائط غير المعرضة للتأثر وفقا لأعلى مستوى تصنيف تحظى به المعلومات المختزنة بها.

بالإضافة إلى البند، MS1، إذا كانت الوسائط تتضمن معلومات مصنفة عند مستويات متعددة، ينبغي أن يتم تصنيف الوسائط عند أعلى مستوى.

وعلى سبيل المثال، قد يتضمن مشغل USB ثلاثة وثائق. يمكن تصنيف الوثيقة الأولى عند المستوى C1 والثانية عند المستوى C2 والثالثة عند المستوى Co. وفي هذا السيناريو، سوف يكون التصنيف الفعال للوسائط (مشغل USB) عند المستوى C2، الذي يعد أعلى تصنيف للمعلومات المختزنة به.

MS 3 أن يتم تصنيف الوسائط سريعة التأثر التي تعتمد على مصدر طاقة مستمرة ضمن أعلى مستوى لتصنيف المعلومات المختزنة بها أثناء عملية توصيل الطاقة. ويمكن التعامل مع الوسائط سريعة التأثر باعتبارها معلومات مصنفة عند المستوى C1 بمجرد فصل الطاقة عن الوسائط.

بالإضافة إلى البندين MS1 و MS2، يهدف كتيب تأمين المعلومات الوطنية إلى توضيح أنه في حالة الوسائط سريعة التأثر، قد تفقد الوسائط تصنيفها عقب فقدان الطاقة، حيث أنها لم تعد تحتفظ بأي معلومات.

ينبغي أن يتم التعامل مع الوسائط سريعة التأثر في حالة عدم الاتصال بالطاقة باعتبارها مصنفة عند المستوى C1.

وعلى سبيل المثال، افترض أن هناك جهاز حاسوب محمول يتم استخدامه في تخزين ومعالجة المعلومات المصنفة عند المستوى C2. يتضمن هذا الحاسوب المحمول نمطين من أنماط الوسائط، هما ذاكرة الوصول العشوائية سريعة التأثر والأقراص الصلبة غير المعرضة للتأثر.

طالما أن الحاسوب المحمول متصل بالطاقة، سوف يتم تصنيف القرص الصلب وذاكرة الوصول العشوائية عند المستوى C2. وبمجرد فصل الحاسوب المحمول عن الطاقة، سوف يحتفظ محرك الأقراص الصلبة بمستوى التصنيف C2، بينما يتم تصنيف ذلكرة الوصول العشوائية عند المستوى C1.

MS 4 أن يتم إعادة تصنيف وسائط التخزين إذا:

أ. كانت المعلومات المنقولة إلى تلك الوسائط تحظى بمستوى تصنيف مرتفع.
ب. كانت المعلومات التي تتضمنها تلك الوسائط تخضع لإمكانية تطوير مستوى التصنيف.

ينبغي أن تضع المؤسسة إجراءات لضمان الحفاظ على تحديث التصنيف. ويتم توعية المستخدمين بأهمية وإجراءات تصنيف المعلومات والوسائط ذات الصلة.

ينص كتيب تأمين المعلومات الوطنية على الإرشادات التي يتم استخدامها لتحديد ما إذا كانت الوسائط بحاجة إلى إعادة التصنيف.

MS 5 يمكن إلغاء تصنيف الوسائط التي تحمل معلومات مصنفة عقب:

أ. إلغاء تصنيف المعلومات المختزنة على الوسائط من قبل المنشئ
ب. تطهير الوسائط وفقا للفصل رقم C-8-3 بعنوان "السياسة والضوابط الرئيسية – تطهير الوسائط".

ينبغي أن تضع المؤسسة إجراءات لضمان الحفاظ على تحديث تصنيف الوسائط. وتكفل المؤسسة الالتزام بالإجراءات بمجرد ارتفاع أو انخفاض التصنيف أيضا.

رغم أن الحفاظ على مستوى تصنيف أعلى للوسائط قد لا يستتبع وجود نقاط ضعف أمنية من وجهة النظر الأمنية، إلا أنه قد يستتبع ارتفاع تكاليف الصيانة.

يتم توعية المستخدمين بأهمية وإجراءات إلغاء تصنيف المعلومات والوسائط ذات الصلة.

ينص كتيب تأمين المعلومات الوطنية على الإرشادات التي يتم استخدامها لتحديد ما إذا كانت الوسائط بحاجة إلى إلغاء التصنيف.

MS 6 في حالة عدم إمكانية تطهير وسائط التخزين، لا يمكن إلغاء تصنيفها ويتعين تدميرها.

ينبغي أن تكفل المؤسسة تطهير وسائط التخزين التي تتضمن معلومات مصنفة بما يتماشى مع الفصل C8-3 بعنوان "السياسة والضوابط الرئيسية – تطهير الوسائط" قبل إلغاء تصنيفها. وفي حالة عدم إمكانية تطهير المعلومات، ينبغي أن يتم تدمير الوسائط خشية أن تؤدي إلى تسرب المعلومات.

MS 7 يمكن التعرف على تصنيف جميع الوسائط بوضوح. وينبغي أن تحقق المؤسسة ذلك عن طريق وسم الوسائط بعلامة وقائية تنص على الحد الأقصى لمستوى التصنيف وفقا لما هو محدد بالفصل رقم B-4، بعنوان "وسم البيانات" [DL].

ينص كتيب تأمين المعلومات الوطنية على إمكانية التعرف على تصنيف الوسائط بوضوح. وينبغي أن تضع المؤسسة الإجراءات وتحدد الضوابط التي تكفل وسم الوسائط بالصورة المناسبة وفقا لمستوى التصنيف

ينبغي أن تحدد العلامات الحد الأقصى للتصنيف وأن يتم حمايتا ضد العبث.

MS 8 يمكن التعرف على تصنيف جميع الوسائط بوضوح. وعند استخدام الضمانات غير النصية لعلامات التصنيف نتيجة لأمن التشغيل، يتعين على المؤسسة توثيق خطة التوسيم وتدريب أعضاء فريق العمل بالصورة الملائمة.

يقر كتيب تأمين المعلومات الوطنية استخدام الضمانات غير النصية لعلامات التصنيف (على سبيل المثال: الشفرة العمودية) من أجل تعزيز الأمن؛ ومع ذلك، تكفل المؤسسة توثيق خطة التوسيم وتطبيقها بصورة متسقة بجميع أنحاء المنظمة وتدريب العاملين على استخدامها بفاعلية.

3-8 السياسة والضوابط الرئيسية – تطهير الوسائط

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

MS 9 أن تتولى توثيق الإجراءات الخاصة بتطهير الوسائط، التي يتم اختبارها بانتظام

ينبغي أن تحدد المؤسسة الإجراءات الخاصة بتطهير الوسائط. وتحدد الأجهزة وتقر الأدوات الملائمة للوفاء بمتطلبات تطهير الوسائط بالمؤسسة والتي تخضع للاختبارات بنجاح.

يتم إجراء تلك الاختبارات على فترات منتظمة لضمان فاعلية الأدوات.

MS 10 أن يتم تدمير جميع أنماط الوسائط التي تتضمن معلومات مصنفة عن المستوى C1 أو أكثر قبل التخلص منها, مثال:

أ. الميكروفيش والميكروفيلم.

ب. الأقراص الضوئية.

ج. شرائط الطابعات وسطح التأثير المواجه للاسطوانة.

د. الذاكرة القراءة فقط القابلة للبرمجة.

هـ. ذاكرة القراءة فقط.

و. الوسائط الخاطئة التي لا يمكن تطهيرها بنجاح.

ينص كتيب تأمين المعلومات الوطنية على تدمير الذاكرة غير المعرضة للتأثر، والتي لا يمكن تطهيرها، قبل التخلص منا. ويوفر أمثلة حول أنماط هذه الوسائط. ويتم تدمير جميع هذه الوسائط والوسائط المماثلة، التي قد تتضمن معلومات مصنفة عند المستوى C1 أو أكثر، قبل التخلص منها.

MS 11 أن يتم تطهير الوسائط سريعة التأثر عن طريق:

أ. فصل الطاقة عن الوسائط لمدة 10 دقائق على الأقل أو

ب. إحلال جميع مواقع الوسائط من خلال نمط عشوائي يليه إعادة قراءة الوسائط للتحقق من عملية الإحلال.

يهدف كتيب تأمين المعلومات الوطنية إلى تقديم إرشادات حول تطهير الوسائط سريعة التأثر.

MS 12 أن يتم تطهير الوسائط المغناطيسية غير المعرضة للتأثر عن طريق:

أ. إحلال الوسائط بالكامل، إذا ما كانت صادرة قبل عام 2001 أو كانت أقل من 15 جيجابايت بأسلوب عشوائي يليه إعادة قراءة الوسائط للتحقق من عملية الإحلال لثلاثة مرات.

ب. إحلال الوسائط بالكامل، إذا ما كانت صادرة بعد عام 2001 أو كانت أكبر من 15 جيجابايت بأسلوب عشوائي يليه إعادة قراءة الوسائط للتحقق من عملية الإحلال لمرة واحدة.

ج. استخدام جهاز نزع المغناطيسية بمجال قوة يكفي لمسح الوسائط (ملاحظة: إزالة مغناطيسية قد تجعل بعض وسائل الإعلام الحديثة غير صالحة للاستعمال).

يهدف كتيب تأمين المعلومات الوطنية إلى تقديم إرشادات حول تطهير الوسائط غير المعرضة للتأثر.

MS 13 أن يتم تطهير وسائط EPROM ذات ذاكرة القراءة القابلة للبرمجة والتطهير عن طريق المسح وفقا لمواصفات الشركة المصنعة، بما يزيد من الزمن المحدد للمسح بالأشعة فوق البنفسجية إلى ثلاثة أضعاف، ثم إحلال الوسائط بالكامل من خلال نمط شبه عشوائي. يجب توثيق تطهير الوسائط ذات التصنيف C3 او اكثر.

يهدف كتيب تأمين المعلومات الوطنية إلى تقديم إرشادات محددة حول تطهير وسائط EPROM ذات ذاكرة القراءة القابلة للبرمجة وغير المعرضة للتأثر.

MS 14 أن يتم تطهير وسائط الذاكرة السريعة عن طريق إحلال الوسائط مرتين بالكامل باستخدام نمط شبه عشوائي يليه إعادة قراءة الوسائط للتحقق من عملية الإحلال.

يهدف كتيب تأمين المعلومات الوطنية إلى تقديم إرشادات حول تطهير وسائط الذاكرة السريعة.

4-8 السياسة والضوابط الرئيسية – إصلاح وصيانة الوسائط

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

MS 15 أن يقوم العاملون المطلعون الخاضعون للفحص الملائم بتنفيذ عمليات إصلاح وصيانة الأجهزة التي تتضمن معلومات مصنفة.

ينبغي أن تكفل المؤسسة أن يقوم الأشخاص المفوضون فقط بإجراء أعمال الإصلاح والصيانة للأجهزة المصنفة. ويلتزم العاملون المفوضون (العاملون و/أو المتعاقدون) بالضوابط اللازمة المحددة بالفصل B6. ويتم إطلاع هؤلاء العاملين المفوضين على الإجراءات والسياسات والإرشادات الأمنية ذات الصلة بالمؤسسة.

MS 16 أن يتم إجراء عمليات إصلاح الأنظمة التي تشتمل على معلومات مصنفة عند المستوى C3 أو أكثر في ظل الإشراف.

ينبغي أن تكفل المؤسسة خضوع عمليات الإصلاح بأي نظام يتضمن معلومات مصنفة عند المستوى C3 أو أكثر للإشراف. ورغم أن الكتيب لا يحدد نمطا معينا للإشراف، إلا أنه يمكن استخدام الوسائل الآلية (وعلى سبيل المثال: تحت رقابة الكاميرات ومراقبة الوصول)؛ ومع ذلك، عند تنفيذ تلك العمليات خارج موقع العمل، فلابد أن تخضع إشراف بشري مشدد.

ويهدف ذلك إلى التخفيف من مخاطر العبث بنية سرقة المعلومات أو تدمير سلامتها واختلاسها.

5-8 السياسة والضوابط الرئيسية – تدمير الوسائط والتخلص منها

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

MS 17 أن تتولى توثيق الإجراءات الخاصة بتدمير الوسائط والتخلص منها

تتولى المؤسسة توثيق إجراءات تدمير الوسائط والتخلص منها. وتتماشى الإجراءات مع الضوابط المحددة في كتيب تأمين المعلومات الوطنية.

MS 18 أن يتم تدمير الوسائط عن طريق:

أ. نزع مغناطيسية وسائط EPROM ذات ذاكرة القراءة القابلة للبرمجة والمسح.

ب. تفكيك الوسائط.

ج. تسخين الوسائط لحين حرقها وتحولها إلى رماد أو انصهارها.

يوفر كتيب تأمين المعلومات الوطنية إرشادات حول كيفية تدمير الوسائط. وعند تفكيك الوسائط، فلابد من القيام بذلك بطريقة يستحيل معها إعادة تركيبها أو إصلاحها.

MS 19 أن يتولى أعضاء فريق العمل الإشراف على تدمير الوسائط:

أ. معالجة الوسائط إلى حد التدمير.

ب. ضمان نجاح تدمير الوسائط بالكامل.

ج. يجب توثيق تطهير الوسائط ذات التصنيف C3 او اكثر.

يوفر كتيب تأمين المعلومات الوطنية إرشادات تكفل تنفيذ إجراءات تدمير الوسائط بنجاح. وينبغي أن تكفل المؤسسة ممارسة العناية الواجبة عند تدمير البيانات.

MS 20 أن يتم تطهير الوسائط لأقصى درجة ممكنة، بما في ذلك الوسائط الخاطئة، التي تشتمل على معلومات مصنفة قبل التخلص منها.

ينص كتيب تأمين المعلومات الوطنية على تطهير جميع الوسائط، بما في ذلك الوسائط الخاطئة، قبل التخلص منها، كإجراء أمني إضافي.

MS 21 ألا تجتذب عملية التخلص من الوسائط ومخلفات الوسائط اهتماما غير مستحق.

يهدف كتيب تأمين المعلومات الوطنية إلى الالتزام بمبدأ "تحقيق الأمن من خلال الغموض" لضمان ألا تجتذب مرافق وعمليات التخلص من الوسائط ومخلفات الوسائط اهتماما غير مستحق. وقد يؤدي ذلك إلى محاولات من قبل مستخدمي البرامج الضارة إلى البحث في المخلفات من أجل الوصول إلى المعلومات واختلاسها أو فرض السيطرة عليها.

9 - إرشادات حول أمن السيطرة على صلاحيات الاستخدام [AM]

9-1 أهداف السياسة

9-2 إرشادات حول السياسة والضوابط الرئيسية – عام

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

AM 1 أن يحظى المستخدمون بإمكانية الوصول إلى المعلومات استنادا إلى مفهوم "الامتياز الأقل" على أساس "الحاجة إلى المعرفة" و"الحاجة إلى الحيازة".

يعد مفهوم الامتياز الأقل مبدأً أساسيا من مبادئ أمن المعلومات يؤيد أن تحظى الكيانات (الأشخاص والعمليات والأجهزة) بأقل امتيازات بما يتفق مع الواجبات والوظائف المنوطة بها.

وعلى سبيل المثال، يحدد التوجه المقيد "للحاجة إلى المعرفة" عدم إمكانية الوصول بصورة افتراضية ثم يتيح تطبيق الوضع الأمني وفقا للحاجة. وتعد جميع المعلومات بأي شبكة مؤسسية محظورة على الجميع باستثناء أشخاص محددين أو مجموعات محددة تحتاج إلى الوصول إلى هذه البيانات لأغراض نشاطها الرسمي.

ينبغي أن تكفل المؤسسة توفير إمكانية الوصول إلى المعلومات إلى المستخدمين استنادا إلى مفهوم "الامتياز الأقل" على أساس "الحاجة إلى المعرفة" و"الحاجة إلى الحيازة". وسوف يضمن ذلك أن يكون الكيان قادرا على تنفيذ العمل المنوط به دون أن يتسبب في وقوع أي حوادث، ما لم يعتزم مخالفة السياسات المحددة.

AM 2 أن تخضع إمكانية الوصول إلى المعلومات للإدارة والرقابة من خلال ضوابط الوصول إلى النظام والهوية والتوثيق وعمليات المراجعة والتدقيق التي تستند إلى حساسية المعلومات. وينبغي أن تتم الموافقة على طلب الوصول إلى المعلومات من قبل المشرف أو المدير الذي يرأس أحد أعضاء فريق العمل.

ينص كتيب تأمين المعلومات الوطنية على خضوع اختيار ضوابط الوصول لحساسية المعلومات التي تتولى الرقابة عليها. وتضع المؤسسة الضوابط المناسبة التي تقوم بتحديد وتوثيق المستخدم وتدقيق عملية المراجعة.

تعتمد هوية وتوثيق المستخدم على ما يلي:

عامل المعرفة: ما الذي يعرفه أي مستخدم؟ كلمة المرور/ رقم التعريف الشخصي

عامل الملكية: ما الذي يمتلكه أي مستخدم؟ التوثيق الأمني/ بطاقات الوصول

عامل الوراثة: ما هي هوية أي مستخدم وما الذي يمتلكه؟ علم الإحصاء الحيوي

بناءً على حساسية النظام، قد يتولى القائمون على إدارة النظام تنفيذ خطة توثيق العوامل المتعددة. وعلى سبيل المثال: بطاقة ماكينة الصرف الآلي (عامل الملكية) ورقم التعريف الشخصي (عامل المعرفة).

ينبغي أن تكفل المؤسسة إقرار عملية فعالة للمراجعة والتدقيق من أجل تحديد سوء استخدام أو مخاطر أنظمة الرقابة على الوصول والتعرف على المرتكبين في حالة وقوع أي حوادث.

وعلاوة على ذلك، يحظى مدير أو مشرف العمل بالحق في الموافقة على جميع طلبات الوصول الخاصة بالمستخدمين (الإنشاء/ الحذف/ التعديل). ويكفل ذلك وجود ضوابط لحماية النظام من خطر إنشاء مستخدمين وهميين أو زيادة الامتيازات التي يحظى بها المستخدمون.

AM 3 أن تستند حقوق أي مستخدم أو كيان في الوصول إلى المعلومات من أجل إنشاء أو قراءة أو تحديث أو حذف أو نقل الأصول المعلوماتية للمؤسسة على نموذج هرمي للحقوق التي تحددها قواعد العمل المقررة من قبل أصحاب تلك المعلومات.

يهدف كتيب تأمين المعلومات الوطنية إلى توضيح عملية إسناد حقوق الوصول إلى النظام، اعتمادا على المبادئ الأساسية المذكورة بالبند AM1.

يضع كتيب تأمين المعلومات الوطنية عبء تحديد قواعد حقوق الوصول إلى النظام بفاعلية على عاتق أصحاب المعلومات. وعلاوة على ذلك، يحدد أصحاب المعلومات ذلك العبء بناءً على متطلبات العمل.

AM 4 أن يتم إقرار عملية تكفل تحديث الوصول إلى نظام المعلومات كي يعكس الدور الجديد المنوط بالموظف، فور إجراء أي تغيير في دور أو وضع الموظف.

ينص كتيب تأمين المعلومات الوطنية على تحقيق تكامل دقيق بين عمليات المؤسسة. وينبغي أن تكفل المؤسسة وجود عملية لتنسيق تدفق المعلومات بين إدارتي الموارد البشرية وتكنولوجيا المعلومات وبين إدارة العمليات.

نظرا لمشاركة إدارة الموارد البشرية في عملية توظيف وترقية/ خفض رتبة أو إنهاء تعاقد أي موظف، ينبغي أن تكفل الإدارة نقل تلك المعلومات إلى إدارة تكنولوجيا المعلومات/ العمليات التي قد تضمن تحديث نظام الرقابة على الوصول إلى المعلومات داخل المؤسسة بفاعلية كي يعكس تلك التعديلات. وينبغي أن تكفل المؤسسة تمديد تلك الرقابة إلى الأمن المادي أيضا، حيث تكون الرقابة على الوصول إلى المعلومات في العديد من المنظمات منفصلة عن إدارة تكنولوجيا المعلومات/ العمليات.

AM 5 أن يسعى مستخدمو النظام الذين يحتاجون إلى قدرة إضافية للوصول إلى المعلومات لتجاوز الآليات الأمنية لأي سبب وراء الحصول على تفويض رسمي من قبل مدير أمن المعلومات.

ينص كتيب تأمين المعلومات الوطنية على وجود ضوابط فعالة للتخفيف من حدة تجاوز/ مخاطر نظام الرقابة على الوصول إلى النظام من أجل الوصول إلى المعلومات. ويكون مديرو النظام في وضع قد يسمح لهم بالوصول إلى نظام المعلومات دون قيود. ويتم تنفيذ الضوابط الملائمة، بما في ذلك عمليات المراجعة والتدقيق وتناوب المهام الوظيفية والتدقيق المنتظم من قبل كيان مستقل، من أجل إجراء عمليات الفحص بهدف تجنب سوء الاستخدام.

ومع ذلك، فهناك حالات قد يحتاج مديرو النظام من خلالها الوصول إلى المعلومات من أجل تحري الحوادث واستكشاف القضايا وغير ذلك. ويستطيع مديرو النظام الاستفادة من تلك الامتيازات، رغم ضرورة الحصول على موافقة رسمية من قبل مدير الأمن. ويكفل مدير الأمن، بدوره، استخدام التحايل على رقابة الوصول إلى النظام بفاعلية في الأنشطة المستهدفة والتوقيت المستهدف فقط. ويتم تسجيل أداء مثل هذه الأنشطة بالصورة الملائمة.

AM 6 أن يتم اعتبار أي محاولة غير مفوضة للتحايل على رقابة الوصول إلى معلومات المؤسسة بمثابة حادث أمني ويتم التعامل معه وفقا للإجراءات المقررة للتعامل مع الحوادث و/أو سياسات وإجراءات الموارد البشرية الملائمة.

ينص كتيب تأمين المعلومات الوطنية على اعتبار أي محاولات للتحايل على رقابة الوصول إلى معلومات المؤسسة بمثابة حادث أمني. ويتم التعامل مع أي من تلك المحاولات الناجحة/ المخفقة وفقا للإجراءات المقررة للإبلاغ عن الحوادث و/أو سياسات وإجراءات الموارد البشرية الملائمة.

ويتم التعامل مع الحوادث وفقا للإجراءات التأديبية المقررة الخاصة بإدارة الحوادث/ الموارد البشرية بالمؤسسة.

AM 7 أن يتم تفعيل والحفاظ على سجلات التدقيق بأسلوب يسمح بمتابعة الالتزام بالسياسة ويساعد في إدارة الحوادث.

تكفل المؤسسة تفعيل عملية التدقيق بنظام الرقابة على الوصول إلى المعلومات وتهيئة العملية بالأسلوب المناسب. وتساعد سجلات التدقيق في متابعة الالتزام بالسياسات والإجراءات الأمنية الخاصة بالمؤسسة. وتساعد سجلات التدقيق أيضا في فحص والتحقيق في الحوادث الأمنية.

تلتزم سجلات التدقيق بالضوابط المنصوص عليها بالفصل B10، بعنوان "متطلبات تسجيل الأداء والمتابعة الأمنية".

AM 8 أن يخضع الوصول المنطقي لشبكات المؤسسة للرقابة التقنية. وقد يكون ذلك باستخدام خدمات/ أجهزة الرقابة على الوصول إلى الشبكات.

ينص كتيب تأمين المعلومات الوطنية على قيام المؤسسة بنشر ضوابط إضافية لضمان تأمين أصولها المعلوماتية. وبالإضافة إلى تحديد وتوثيق المستخدم، لابد من وجود ضوابط تكفل عدم قيام المستخدم الموثق بإدخال نقاط ضعف إلى النظام من خلال النظام الذي يستخدمه.

وعلى سبيل المثال، قد يقوم المستخدم الذي يعمل عن بعد بتوصيل جهاز حاسوبه الشخصي المنكوب بالفيروسات بشبكة المؤسسة، مما يتسبب في انتشار الفيروس وإصابة شبكات المؤسسة.

يتعين وجود ضوابط أخرى لضمان تفويض المستخدم الموثق من قبل النظام أيضا بتنفيذ العمل المستهدف. وهناك خط دقيق يفصل بين التوثيق والتفويض.

وعلى سبيل المثال، قد يحظى المستخدم بوثائق تفويض للوصول إلى النظام، ولكنه قد لا يكون مفوضا بالوصول إلى جميع المعلومات الكائنة بذلك النظام.

AM 9 أن يتم الحفاظ على سجلات آمنة لما يلي:

أ. جميع مستخدمي النظام المفوضين.

ب. هوية المستخدم الخاصة بهم.

ج. الأشخاص الذين منحوهم الموافقة على الوصول إلى النظام.

د. موعد منح الموافقة والتفويض.

هـ. الحفاظ على السجل على مدارفترة تواجد النظام الذي تم منح إمكانية الوصول إليه.

ينبغي أن تكفل المؤسسة الحفاظ على سجلات سليمة فيما يتعلق بنظام الرقابة على الوصول إلى المعلومات. ويوفر كتيب تأمين المعلومات الوطنية إرشادات حول بعض السجلات الإلزامية التي ينبغي الاحتفاظ بها للمساعدة في إجراء تدريب التدقيق الفعال والتحريات بشأن الحوادث وغير ذلك.

ينص كتيب تأمين المعلومات الوطنية أيضا على فترة الاحتفاظ بالسجلات، والتي ترتبط في الأساس بفترة تواجد النظام.

AM 10 أن يتم عرض شعارتسجيل الدخول قبل منح إمكانية الوصول إلى النظام. وينبغي أن تشمل هذه الشعارات ما يلي:

أ. السماح لمستخدمي النظام المفوضين فقط بالوصول إلى النظام.

ب. موافقة مستخدم النظام على الالتزام بسياسات الأمن ذات الصلة.

ج. دراية مستخدم النظام بإمكانية متابعة استخدام النظام.

د. تعريف الاستخدام المقبول للنظام.

هـ. التبعات القانونية لانتهاك السياسات ذات الصلة.

و. طلب استجابة مستخدم النظام، متى أمكن، على سبيل الإقرار.

ينبغي أن تكفل المؤسسة، متى أمكن، الاستخدام الفعال للموارد والأدوات لتوعية المستخدم بمسؤولياته الأمنية وردع الدخلاء على النظام.

ينبغي أن تتولى المؤسسة تنفيذ الشعارات التي تنادي بالسماح للمستخدمين المفوضين فقط بالوصول إلى النظام وضرورة التزام المستخدم بالسياسات الأمنية ذات الصلة ومتابعة النظام وتحديد الاستخدام المقبول للنظام والتبعات القانونية لانتهاك وسوء استعمال النظام (الشعارات يمكن أن تكون في أشكال بصرية أو سمعية).

ينبغي أن تكفل المؤسسة أيضا (إن أمكن) الحصول على إقرار المستخدم للشعار وموافقته على الالتزام بشروطه وأحكامه قبل الحصول على إمكانية الوصول إلى النظام.

AM 11 أن تتم حماية هيئات التوثيق المركزية (Active Directory)، مثل LDAP وقواعد بيانات التوثيق وغيرها من الاعتداءات على الخدمة واستخدام قنوات آمنة وموثقة لاسترجاع بيانات التوثيق. وتتولى مثل تلك الهيئات تسجيل الأحداث التالية:

أ. تحديث المعلومات/ الوصول إلى المعلومات دون تفويض.

ب. تاريخ البدء والانتهاء وزمن النشاط بالإضافة إلى محدد النظام.

ج. هوية المستخدم (لتسجيل الدخول غير القانوني).

د. نشاط تسجيل الدخول والخروج (لتسجيل الدخول غير القانوني).

هـ. الجلسة/ المحطة الطرفية أو الاتصال عن بعد.

تعد هيئات التوثيق المركزية، مثل LPAD، بمثابة أهداف رئيسية غير محصنة لمستخدمي البرمجيات الضارة. وقد يساعد تعرض تلك الأنظمة للمخاطر مستخدم البرمجيات الضارة على اختراق النظام دون سابق إنذار. وعلاوة على ذلك، قد يؤدي الاعتداء على الخدمة إلى عدم إمكانية وصول جميع المستخدمين إلى الخدمات المتكاملة.

ينبغي أن تكفل المؤسسة حماية تلك الأنظمة بفاعلية من مخاطر الاعتداءات على الخدمة. وتكون الاتصالات بين الكيانات المشاركة من خلال قنوات آمنة وموثقة، مثل القنوات المشفرة.

تكفل المؤسسة تسجيل أداء الأنشطة الرئيسية (تلك الأنشطة المذكورة أعلاه على الأقل). وتساعد تلك السجلات في فحص والتحري عن الحوادث الأمنية.

3-9 إرشادات حول السياسة والضوابط الرئيسية – تحديد الهوية والتوثيق

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسة أن تكفل ما يلي:

AM 12 أن تضع وتحتفظ بمجموعة من السياسات والخطط والإجراءات المشتقة من سياسة التصنيف الوطنية [IA-NAT-DCLS] تشمل مستخدمي النظام فيما يتعلق بما يلي:

أ. تحديد الهوية.

ب. التوثيق.

ج. التفويض.

تحدد المؤسسة السياسات والإجراءات ذات الصلة بما يتماشى مع سياسة التصنيف الحكومي [IA-NAT-DCLS] وكتيب تأمين المعلومات الوطنية. وتشمل السياسات والإجراءات مجالات تحديد الهوية والتوثيق والتفويض.

تستند السياسات إلى مفهوم الامتياز الأقل وتخضع لمبادئ "الحاجة إلى المعرفة" و"الحاجة إلى الحيازة" وفقا لما تم مناقشته بالبند AM1.

AM 13 أن تتولى توعية مستخدمي النظام لديها بسياسات وإجراءات المؤسسة.

ينبغي أن تكفل المؤسسة توعية مستخدمي النظام بسياسات وإجراءات المؤسسة.

يتضمن التدريب التوجيهي المقدم للعاملين الجدد التوعية بسياسات وإجراءات إدارة الوصول إلى المعلومات. ويتم تنظيم دورات توعية أمنية منتظمة تتضمن التوعية فيما يتعلق بإدارة الوصول إلى النظام.

AM 14 جميع مستخدمي النظام:

أ. يمكن تحديد هويتهم بصورة فريدة.

ب. يتم توثيقهم في كل مناسبة يتم خلالها منح إمكانية الوصول إلى النظام.

تعد المساءلة الفردية ضرورية لأمن أنظمة تكنولوجيا المعلومات. وينبغي ألا تفوض المؤسسة بإنشاء الحسابات التي يمكن استخدامها من قبل مجهولين أو من قبل أكثر من شخص واحد. ويساعد حساب الضيف على تفعيل إمكانية الوصول إلى نظام تكنولوجيا المعلومات من قبل مجهولين، بينما يخفي الحساب المشترك (أو كلمة المرور المشتركة) المساءلة الفردية بين مجموعة من الأفراد. ويتم حظر كلا نمطي الحساب والمشاركة في كلمات المرور أو أساليب الوصول المنطقية الأخرى.

ينبغي أن تكفل المؤسسة أن يستخدم جميع العاملين والمتعاقدين والاستشاريين والعمالة المؤقتة هوية المستخدم الفريدة وكلمات المرور من أجل الحصول إلى تصريح بالوصول إلى أي من الأصول المعلوماتية الخاصة بالمؤسسة.

يتم مساءلة المستخدمين المفوضين ويتحمل هؤلاء المسؤولية عن استخدام أي نشاط خاص بهوية المستخدم الفريدة التي يتم إسنادها إليهم.

يتم تطبيق ضوابط إضافية لضمان عدم إخفاء وثائق تفويض المستخدم بالذاكرة المؤقتة. ويتم توثيق المستخدمين كلما تم منح إمكانية الوصول إلى المعلومات. ومع ذلك، يمكن أن يتم السماح للمؤسسة بنشر تطبيقات الدخول الفردية طالما تستطيع ضمان الحفاظ على كلمة المرور بأسلوب آمن.

AM 15 ألا يتم منح الأفراد من غير العاملين أو المتعاقدين أو الاستشاريين حساب مستخدم أو امتيازات لاستخدام الموارد المعلوماتية أو أنظمة الاتصالات الخاصة بالمؤسسة دون موافقة صريحة من مدير أمن المعلومات الذي يتحقق من إبرام الاتفاقيات المناسبة واستيفاء نماذج التراخيص والوصول إلى النظام.

ينص كتيب تأمين المعلومات الوطنية على ضوابط تكفل عدم تعرض نظام الرقابة على الوصول إلى معلومات المنظمة للمخاطر أو خرق ذلك النظام. ومن الناحية الافتراضية، لا يتم منح الأفراد من غير العاملين أو المتعاقدين أو الاستشاريين (المتعاقدون والاستشاريون الذين تتم إقامة شراكة عمل محددة معهم ويحصلون على تصريح أمني) إمكانية الوصول إلى أنظمة المعلومات الخاصة بالمؤسسة..

يتم اعتماد أي استثناء (على سبيل المثال: الموردون الجدد الذين قد يرغبون في عرض منتج/ خدمة) من القاعدة السابقة بصورة واضحة من قبل مدير الأمن الذي يكفل وجود التصريح الأمني اللازم قبل توفير إمكانية الوصول إلى المعلومات.

AM 16 أن تكون هناك وسائل بديلة لتحديد هوية مستخدم النظام عند استخدام حسابات مشتركة/ غير محددة.

ينبغي أن تكفل المؤسسة تحقيق المساءلة الفردية من خلال إسناد هوية مستخدم فريدة لكل مستخدم. ومع ذلك، فحينما يكون هناك قيود (تقنية أو غير ذلك) على تنفيذ تلك الحلول، ينبغي أن تحدد المؤسسة أساليب بديلة لتحديد مستخدم النظام أثناء استخدام الحسابات المشتركة/ غير المحددة.

يمكن أن تتضمن الضوابط المشاركة في الحسابات بناءً على الوقت (على سبيل المثال: تغيير المستخدمين) والموقع (على سبيل المثال: محطات العمل والمناطق المكتبية وغير ذلك).

AM 17 أن تكون معلومات التوثيق غير المحمية التي تسمح بالوصول إلى النظام أو تتولى فك تشفير أي جهاز مشفر قائمة داخل النظام الذي تمنح معلومات التشفير إمكانية الوصول إليه.

ينبغي أن تكفل المؤسسة حماية معلومات التوثيق التي تسمح بالوصول إلى النظام أو تتولى فك تشفير أي جهاز مشفر بالصورة المناسبة. وفي أسوأ الأحوال، حيثما لا يكون ذلك ممكنا لأسباب مثل أنظمة التراث وأنظمة الملكية، ينبغي ألا تترك هذه المعلومات النظام الذي تمنح إمكانية الوصول إليه. وسوف يكفل ذلك أن تتم حماية المعلومات، كحد أدنى، باستخدام الضوابط المادية الملائمة التي يمكن أن تسري على هذا النظام.

AM 18 ألا تكون بيانات توثيق النظام المستخدمة عرضة للاعتداءات ويشتمل ذلك، على سبيل المثال لا الحصر، على تخزين المعلومات وإعادة استخدامها واعتراض نقل المعلومات بين طرفين والتحكم في الجلسات.

ينبغي أن تكفل المؤسسة وجود ضوابط ملائمة لحماية بيانات التوثيق ضد مخاطر مثل إعادة استخدام المعلومات واعتراض نقل المعلومات بين طرفين والتحكم في الجلسات ضمن أمور أخرى. وينبغي أن تختار المؤسسة التكنولوجيات التي تشفر بيانات التوثيق أثناء الانتقال والمعالجة والتخزين.

AM 19 سياسة كلمة المرور التي تفرض حد أدنى لكلمة المرور يصل إلى 12 رمز دون أي شروط معقدة أو حد أدنى يصل إلى سبعة رموز تتألف من ثلاثة على الأقل من مجموعات الرموز التالية:

أ. حروف صغيرة (a-z).

ب. حروف كبيرة (A-Z).

ج. أرقام (0-9).

د. علامات الترقيم والرموز الخاصة.

ينبغي أن تحدد المؤسسة سياسة كلمة المرور وإجراءاتها ذات الصلة. وينص كتيب تأمين المعلومات الوطنية على المتطلبات الخاصة بكيفية صياغة كلمات المرور. ويشجع الكتيب على استخدام عبارات المرور التي يسهل تذكرها نسبيا ويصعب حل رموزها.

AM 20 أن يتم تغيير كلمات المرور مرة واحدة على الأقل كل 90 يوما.

ينص كتيب تأمين المعلومات الوطنية على تغيير كلمات المرور كل 90 يوما.

AM 21 ألا يستطيع مستخدمو النظام تغيير كلمة المرور لأكثر من مرة يوميا ويجبر النظام المستخدم على تغيير كلمة المرور المنتهية الصلاحية عند تسجيل الدخول المبدئي أو عند إعادة التشغيل.

وعلاوة على ذلك، ينص كتيب تأمين المعلومات الوطنية على ضوابط للحد من النفقات العامة للنظام/ الإداري من خلال ضمان ألا يتمكن المستخدمون من تغيير كلمات المرور أكثر من مرة واحدة يوميا. وينص أيضا على ضرورة أن يجبر النظام المستخدمين على تغيير كلمات المرور عند تسجيل الدخول بعد انتهاء صلاحياتها أو إعادة تشغيلها.

AM 22 أن يتم فحص كلمات المرور المختارة لمنع ما يلي:

أ. كلمات المرور التي يمكن التنبؤ بها عند إعادة التشغيل.

ب. إعادة استخدام كلمات المرور عند إعادة تشغيل الحسابات المتعددة.

ج. كلمات المرور التي يتم إعادة استخدامها بعد إجراء ثمانية تغييرات لها.

د. استخدام المستخدمين لكلمات المرور التسلسلية أو المتعاقبة.

ينبغي أن تكفل المؤسسة ضرورة تطبيق الضوابط، متى كان ذلك مجديا من الناحية التقنية، لضمان التزام النظام بسياسة كلمات المرور. وعلاوة على ذلك، ينبغي أن تحول الضوابط دون إعادة استخدام كلمات المرور ومدى قوة كلمات المرور وغير ذلك.

يتم توعية المستخدمين والمديرين لضمان الالتزام بسياسات كلمات المرور.

AM 23 ضبط إعدادات قفل الشاشة/ الجلسة على:

أ. التشغيل بعد 15 دقيقة كحد أقصى من توقف مستخدم النظام عن العمل.

ب. التشغيل يدويا من قبل مستخدم النظام عند الرغبة في ذلك.

ج. الإقفال لإخفاء جميع المعلومات الظاهرة على الشاشة تماما.

د. ضمان عدم ظهور الشاشة كما لو كانت مغلقة في حالة الإقفال.

هـ. قيام مستخدم النظام بإعادة التوثيق من أجل فتح النظام.

و. عدم السماح لمستخدم النظام بتعطيل آلية الإقفال.

ينص كتيب تأمين المعلومات الوطنية على وجود ضوابط لتأمين الجلسات العاملة. ويتم تهيئة وإعداد الأنظمة من أجل تشغيل إعدادات قفل الشاشة/ الجلسة بعد بعد 15 دقيقة كحد أقصى من توقف مستخدم النظام عن العمل.

يتمكن المستخدم أيضا من تشغيل قفل الشاشة/ النظام يدويا.

يتم تهيئة وإعداد الأنظمة لضمان أن تخفي الشاشة جميع المعلومات تماما بمجرد إقفالها. ومع ذلك، ينبغي ألا تبدو مغلقة (لمنع أي شخص من فصل الطاقة الكهربائية).

تظل الأنظمة مقفلة حتى يقوم المستخدم بإعادة إقرار الوصول باستخدام الإجراءات الملائمة لتحديد الهوية والتوثيق (أي هوية المستخدم وكلمة المرور).

AM 24 أن يتم تعليق الوصول إلى النظام بعد عدد محدد من محاولات تسجيل الدخول المخفقة أو بمجرد عدم حاجة أي من أعضاء فريق العمل إلى الدخول على النظام نتيجة لتغيير الأدوار أو ترك العمل بالمؤسسة.

ينص كتيب تأمين المعلومات الوطنية على وجود ضوابط الجلسات لمنع سوء استخدام الحسابات/ كلمات المرور.

يتم تهيئة النظام لضمان إغلاق حساب المستخدم بعد ثلاث محاولات متتالية فاشلة لتسجيل الدخول وتعطيل تسجيل الدخول لفترة لا تقل عن 30 دقيقة أو اشتراط وجود مدير للنظام لإعادة تشغيل الحساب قبل السماح بتسجيل الدخول.

تكفل المؤسسة أن يطلب مدير المستخدم، الذي ينتقل (إلى خارج المؤسسة) أو يتقاعد أو يحصل على إجراء تأديبي أو غير ذلك، حذف هوية تسجيل الدخول على الحاسوب وإلغاء حقوق الوصول إلى جميع الأصول المعلوماتية المخصصة.

تكفل المؤسسة أن يطلب مدير المستخدم، الذي يتم إعادة إسناد مهامه داخل المؤسسة بمقتضى ترقية أو انتقال داخلي، إعادة إسناد حقوق الوصول إلى الموارد المتعددة لتكنولوجيا المعلومات بما يتماشى مع المسؤوليات الجديدة.

AM 25 كلمات المرور المفقودة أو المسروقة أو المعرضة لخطر الكشف عنها:

أ. يتم إبلاغ مدير أمن المعلومات عنها كي يكفل تعليق العمل بالحساب الخاص بها.

ب. يتم تغييرها بمجرد التحقق من هوية المستخدم.

ينبغي أن توثق المؤسسة الإجراءات الخاصة بالتعامل مع كلمات المرور المفقودة أو المسروقة أو المعرضة لخطر الكشف عنها. وكحد أدنى، تتطلب هذه الإجراءات من المستخدمين ما يلي:

أ- أن يتم إبلاغ مدير أمن المعلومات على الفور عن فقدان أو سرقة أو تعرض كلمات المرور للمخاطر.
ب- أن يتم تغيير كلمة المرور الخاصة بهم، إذا ما تعرضت للمخاطر.
ت- ينبغي أن تضع الأجهزة العمليات المتسقة والآمنة وتلتزم بها من أجل التحقق من هوية المستخدم قبل تقديم كلمة مرور بديلة.

AM 26 أن يتم تعليق العمل بالحسابات التي تكون غير عاملة لمدة تتجاوز ثلاثة (3) شهور.

ينبغي أن تحدد المؤسسة إجراءات متابعة نشاط وصول المستخدم إلى النظام. ويتم تعليق العمل بالحسابات التي تكون غير عاملة لمدة تتجاوز ثلاثة (3) شهور (وعلى سبيل المثال: الإجازة الطويلة/ الإجازة الطبية) بموجب المزيد من الفحص والدراسة. وفي حالة عدم الحاجة إلى الحساب، يتم اتخاذ الإجراءات المناسبة لحذف الحساب.

AM 27 أن يتم تدقيق الحسابات الخاصة بمعلومات معالجة الأنظمة المصنفة عند المستوى C2 أو I2 أو A2 أو أي مستوى أعلى من أجل التحقق من حداثتها كل ستة (6) شهور.

تحدد المؤسسة الإجراءات التي تكفل تدقيق الحسابات الخاصة بمعلومات معالجة الأنظمة المصنفة عند المستوى C2 أو I2 أو A2 أو أي مستوى أعلى كل ستة (6) شهور من أجل التحقق من حداثتها.

يؤكد التدقيق على ذلك في حالة العاملين الذين تغيرت مراكزهم أو أدوارهم أو مسؤولياتهم بسبب الترقية أو خفض الرتبة أو الانتقال أو فسخ التعاقد أو غير ذلك.

4-9 السياسة والضوابط الرئيسية – صلاحيات استخدام النظام

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسة أن تكفل ما يلي:

AM 28 أن تتولى سياسات الأمن توثيق شروط الوصول إلى النظام والتراخيص الأمنية والتعليمات اللازمة من أجل الوصول إلى النظام.

ينبغي أن تكفل المؤسسة أن تنص سياساتها الأمنية على شرط توثيق نموذج متطلبات الوصول إلى النظام والتراخيص الأمنية والتعليمات والتوعية الأمنية التي قد تكون ضرورية قبل منح إمكانية الوصول إلى النظام.

AM 29 أن يتم فحص مستخدمي النظام وفقا لما هو محدد بالفصل B-6 بعنوان "الأمن الشخصي" [PS] قبل منح أي منهم تصريح بالدخول على النظام.

بالإضافة إلى البند AM28، ينبغي أن تكفل المؤسسة فحص مستخدمي النظام وفقا للمتطلبات المحددة بالفصل B-6 بعنوان "الأمن الشخصي". ويتضمن مستخدمو النظام العاملين والاستشاريين والمتعاقدين. ويتم تحديد المتطلبات، مثل فحص العاملين، كجزء من الإجراءات الخاصة بمنح تصريح الدخول على النظام.

AM 30 أن يتلقى مستخدمو النظام أي تعليمات لازمة قبل منح أي منهم تصريح بالدخول على النظام.

بالإضافة إلى البند AM29، ينص كتيب تأمين المعلومات الوطنية على وجود ضوابط لتوعية المستخدم بمسؤولياته والتوعية الأمنية والاستخدام المقبول قبل منحه تصريح بالدخول على النظام.

5-9 السياسة والضوابط الرئيسية – الوصول إلى النظام بامتيازات خاصة

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسة أن تكفل ما يلي:

AM 31 أن يتم توثيق ومراقبة ومساءلة والحد من استخدام الحسابات المتميزة. وينبغي أن يتم استخدام الحسابات المتميزة في العمل الإداري فقط.

ينبغي أن تكفل المؤسسة وجود إجراءات للحد من استخدام الحسابات المتميزة. ويتم توثيق ومتابعة ومساءلة أي من تلك الحسابات. ويتم أيضا تدقيق جميع الأنشطة التي تم تنفيذها من خلال حساب متميز.

يتم الحد من استخدام مثل هذه الحسابات واستخدامها في العمل الإداري فقط.

AM 32 أن يتم إسناد حساب فردي إلى مديري النظام من أجل الاضطلاع بمهامهم الإدارية.

بالإضافة إلى البند AM33، يحظى مستخدمو النظام ذوو إمكانية الوصول المتميز إلى النظام بحساب مختلف لممارسة أنشطتهم اليومية العادية.

AM 33 أن يحظى المواطنون القطريون وحدهم دون غيرهم بإمكانية الوصول المتميز إلى معلومات معالجة الأنظمة المصنفة عند المستوى C4 أو أي مستوى أعلى ما لم يتم منح موافقة صريحة لاستثناء هذه السياسة.

في ضوء الأمن القومي، يحظى المواطنون القطريون وحدهم دون غيرهم (ممن لديهم التصريح الأمني المطلوب بما يتماشى مع متطلبات الفصل B-6 بعنوان "أمن العاملين") بإمكانية الوصول المتميز إلى معلومات معالجة الأنظمة المصنفة عند المستوى C4 أو أي مستوى أعلى.

يتم الموافقة على أي استثناء من هذه القاعدة من قبل مدير أمن المعلومات ورئيس المؤسسة.

AM 34 أن يتم تحديث سجل إدارة النظام من أجل تدوين المعلومات التالية:

أ. أنشطة التطهير.

ب. بدء تشغيل النظام وإغلاقه.

ج. إخفاق المكونات أو الأنظمة.

د. أنشطة الصيانة.

هـ. أنشطة الدعم والأرشفة.

و. أنشطة استعادة قدرة النظام على العمل.

ز. الأنشطة الخاصة أو الأنشطة خارج ساعات العمل.

ينبغي أن تحدد المؤسسة الإجراءات الخاصة بتسجيل أداء الأنشطة الرئيسية لإدارة النظام. ويتم الاحتفاظ بسجلات تلك الأنشطة بما يتماشى مع المتطلبات المحددة بالفصل B10، بعنوان "تسجيل الأداء والمتابعة".

تتضمن الأنشطة الرئيسية إتاحة النظام (البدء والإغلاق واستعادة المعلومات) وصيانته ودعمه واستعادته وغير ذلك.

6-9 السياسة والضوابط الرئيسية – الدخول على النظام عن بعد

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسة أن تكفل ما يلي:

AM 35 ألا يتم السماح بالدخول على النظام عن بعد ما لم تكن هناك موافقة صريحة من قبل مدير الإدارة وما لم تكن مبررة بمقتضى متطلبات العمل وبعد ممارسة العناية الواجبة لتحليل المخاطر المتعلقة وتنفيذ الضوابط المناسبة للتخفيف من حدة المخاطر المحددة.

لا توفر المؤسسة لمستخدميها إمكانية الدخول على النظام عن بعد ما لم يكن مبررا بمقتضى متطلبات العمل وما لم تكن هناك موافقة من قبل مدير الإدارة و/أو مدير أمن المعلومات.

تستند موافقات مدير الإدارة و/أو مدير أمن المعلومات على تدريب العناية الواجبة الذي يتم تنفيذه من أجل تحليل المخاطر ذات الصلة بتوفير مرافق الوصول إلى النظام عن بعد إلى المستخدمين. ويكفل هؤلاء أيضا وجود الضوابط الكافية للتخفيف من حدة أي مخاطر محددة قبل تقديم الخدمة.

AM 36 أن يتم استخدام توثيق العامل المزدوج من خلال استخدام رمز أو إشارة أوالضوابط الخاصة بالسمات البيولوجية وما شابه عند الدخول إلى بيانات معالجة الأنظمة المصنفة عند المستوى C3 أو أي مستوى أعلى.

ينبغي أن تكفل المؤسسة استخدام الضوابط الإضافية، بما في ذلك توثيق العامل المزدوج، من أجل توثيق المستخدمين والوصول عن بعد إلى الأنظمة المصنفة عند المستوى C3 أو أي مستوى أعلى.

AM 37 أن يتم تأمين جلسات الدخول عن بعد باستخدام التشفير الملائم من البداية إلى النهاية وفقا لما هو محدد بالفصل C-10 بعنوان "أمن التشفير" [CY].

ينص كتيب تأمين المعلومات الوطنية على تنفيذ الضوابط الأمنية، مثل التشفير من البداية إلى النهاية وفقا لما هو محدد بالفصل C-10 بعنوان "أمن التشفير" من أجل حماية المعلومات أثناء انتقالها.

ينبغي أن يبدأ التشفير مع بدء الجلسة ويتضمن هوية وتوثيق جميع المستخدمين ولا ينتهي حتى انتهاء الجلسة.

AM 38 أن يتم تزويد أجهزة الحاسوب المتصلة بالنظام عن بعد بجدار ناري شخصي وبرنامج لمكافحة الفيروسات الضارة على الأقل. ويتم تفعيل هذه الضوابط الأمنية في جميع الأوقات.

تكفل المؤسسة تنصيب جدار ناري شخصي وبرنامج لمكافحة الفيروسات الضارة والكشف عنها وبرنامج للإصلاح على أجهزة الحاسوب المتصلة بالنظام عن بعد. وينبغي أن يتم تفعيل جميع هذه البرامج الأمنية في جميع الأوقات.

يتم تطبيق الضوابط بما يكفل عدم قدرة المستخدمين على تعطيل أو وقف تشغيل هذه الأنشطة. وينبغي أن تتواجد ضوابط إضافية لضمان خلو أجهزة الحاسوب المتصلة بالنظام عن بعد من فيروسات الحاسوب والبرمجيات الضارة قبل الاتصال بشبكة المؤسسة. وينبغي أن تدرس المؤسسة خيارات استخدام حلول رقابة الوصول إلى الشبكة أو الالتزام بنقطة النهاية.

AM 39 أن يتم إصلاح البرمجيات، بما في ذلك برامج الأمن المنصبة على أجهزة الحاسوب، وتحديثها بصفة دائمة.

ينبغي أن تحدد المؤسسة الإجراءات التي تكفل تحديث أجهزة الحاسوب المتصلة بالنظام عن بعد بأحدث توقيعات الفيروسات وتعريفات البرامج الضارة. وبالإضافة إلى ذلك، يتم تطبيق أحدث الحزم الأمنية على أجهزة الحاسوب المتصلة بالنظام عن بعد.

يمكن أن تدرس المؤسسة خيارات، مثل توفير أجهزة الحاسوب المتصلة بالنظام عن بعد.

AM 40 ألا يقوم المستخدمون بالدخول على الأنظمة الداخلية للمؤسسة من خلال أجهزة الحاسوب العامة، على سبيل المثال: أجهزة الحاسوب بمقاهي الإنترنت وغير ذلك أو طباعة المواد من خلال أي أجهزة حاسوب عامة.

ينبغي أن تحدد المؤسسة الإجراءات وأن تتولى توعية المستخدمين لديها بعدم الدخول على الأنظمة الداخلية للمؤسسة من خلال أجهزة الحاسوب العامة، على سبيل المثال: أجهزة الحاسوب بمقاهي الإنترنت واستخدام الطابعات العامة في طباعة المعلومات المصنفة.

AM 41 أن يقتصر دخول الموردين عند بعد إلى الأنظمة على الحالات التي لا تنطوي على أي بدائل أخرى. وفي هذه الحالة، يخضع بدء الاتصال لرقابة ومتابعة المؤسسة. ويكون دخول الموردين عن بعد إلى الأنظمة لفترة زمنية محددة فقط ترتبط بفترة تنفيذ المهمة المراد تنفيذها.

ينبغي أن تحدد المؤسسة السياسات والإجراءات التي تكفل عدم توفير إمكانية الوصول إلى النظام عن بعد، بصورة افتراضية، إلى الموردين.

يوافق مدير أمن المعلومات على أي استثناءات، كما هو حال متطلبات الأعمال، حيث لا يكون هناك بدائل مجدية أخرى متاحة.

يكفل مدير أمن المعلومات وجود ضوابط ملائمة لمراقبة ومتابعة الوصلات عبر مراحلها، وعلى سبيل المثال: بدء التشغيل والتنفيذ والانتهاء. وعلاوة على ذلك، يتم توفير الوصلات لفترة زمنية محددة تخضع للمهام المزمع تنفيذها.

10 - إرشادات حول أمن التشفير [CY]

10-1 أهداف السياسة

10-2 السياسة والضوابط الرئيسية

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

CY 1 أن يفي لوغاريتم التشفير وأجهزة/ برامج التشفير وأنظمة إدارة مفاتيح التشفير والتوقيعات الرقمية بالمتطلبات المحددة بالملحق B من هذا الكتيب حول لوغاريتم وأنظمة التشفير.

ينبغي أن تكفل المؤسسة أن يفي لوغاريتم التشفير وأجهزة/ برامج التشفير وأنظمة الإدارة الرئيسية بالمتطلبات المحددة بالملحق B حول لوغاريتم وأنظمة التشفير المعتمدة.

يحظى لوغاريتم التشفير المختار بقوة مناسبة ويتم التوصية بالاستخدام المحدد له.

سوف يتم تقييم صحة اللوغاريتم المحدد على فترات منتظمة. ويوصي كتيب تأمين المعلومات الوطنية ببدائل و/أو تحديثات للوغاريتم التشفير، متى لزم الأمر. وسوف يتم تحديث الملحق B من كتيب تأمين المعلومات الوطنية كي يعكس بانتظام التغير التكنولوجي ووضع المخاطر الأمنية.

CY 2 أن يتم تحديد عمر المفتاح بصفة رئيسية من خلال التطبيقات والبنية الأساسية للمعلومات التي يتم استخدامه بها. ويتم على الفور إلغاء المفاتيح واستبدالها في حالة الكشف عنها أو الاشتباه في ذلك.

ينبغي أن تكفل المؤسسة تحديد عمر المفاتيح بناءً على متطلبات التطبيقات والبنية الأساسية للمعلومات التي يتم استخدامه بها. ويتضمن ذلك عوامل مثل المتطلبات التشغيلية وسهولة تغيير المفاتيح والسرية ومتطلبات سلامة التطبيقات وغير ذلك. وبالإضافة إلى ذلك، ففي حالة تعرض المفاتيح للخطر أو الاشتباه في تعرضها للخطر، يتم تغييرها على الفور وتسجيل الحادث وإدارته وفقا لإجراءات التعامل مع الحوادث.

CY 3 أن يتم تشفير الأصول المعلوماتية المصنفة عند المستوى C3 من سياسة تصنيف المعلومات الوطنية [IAP-NAT-DCLS] وحمايتها من الإفصاح عنها دون موافقة أثناء تخزينها و/أو نقلها بغض النظر عن أسلوب أو وسائط التخزين. ويمكن أن تطبق المؤسسة ضوابط التشفير هذه على الأصول ذات متطلبات السرية الأدنى، إذا ما تقرر ضرورة ذلك من خلال عملية تقييم المخاطر.

ينص كتيب تأمين المعلومات الوطنية على تشفير الأصول المعلوماتية المصنفة عند المستوى C3 وحمايتها من الإفصاح عنها دون موافقة أثناء تخزينها و/أو نقلها بغض النظر عن أسلوب أو وسائط التخزين.

ويمكن تأمين الأصول المعلوماتية المصنفة عند مستوى أدنى من المستوى C3 من خلال ضوابط التشفير، إذا ما تقرر ضرورة ذلك من خلال عملية تقييم المخاطر.

CY 4 أن يتم تأمين سلامة الأصول المعلوماتية المصنفة عند المستوى I3 من سياسة تصنيف المعلومات الوطنية [IAP-NAT-DCLS] من خلال استخدام تجزئة التشفير. ويمكن أن تطبق المؤسسة ضوابط التشفير هذه على الأصول ذات متطلبات السلامة الأدنى، إذا ما تقرر ضرورة ذلك من خلال عملية تقييم المخاطر. ويحدد الملحق "ب" من هذا الفصل لوغاريتم التجزئة المعتمدة.

ينص كتيب تأمين المعلومات الوطنية على تأمين سلامة الأصول المعلوماتية المصنفة عند المستوى I3 من خلال استخدام تجزئة التشفير.

ويمكن تأمين الأصول المعلوماتية المصنفة عند مستوى أدنى من المستوى I3 من خلال ضوابط التشفير، إذا ما تقرر ضرورة ذلك من خلال عملية تقييم المخاطر.

CY 5 أن يتم استخدام بروتوكولات النقل التالية ذات اللوغاريتم المعتمد المحدد بالملحق "أ" لتأمين البيانات المصنفة عند المستوى C3 أثناء عملية النقل:

أ. لتأمين حركة مرور البيانات عبر الويب : TLS (128 + bits) [RFC4346]

ب. لتأمين نقل الملفات: SFTP [SFTP]

ج. لتأمين الوصول إلى المعلومات عن بعد: SSH v2 [RFC4253] أو IPSEC [RFC 4301]

د. يجب إستخدام بروتوكول التوقيع و تشفير الرسائل : S\MIME vs [RFC 3851] أو أفضل ، انظر CY11 لمعرفة المتطلبات لمرتبطة

ينص كتيب تأمين المعلومات الوطنية على اللوغاريتم المعتمد المحدد بالملحق "ب" لتأمين البيانات أثناء عملية النقل. وينص الكتيب أيضا على ضوابط لتأمين الأنماط المحددة للتطبيقات التي تتعامل مع البيانات أثناء انتقالها.

CY 6 أن يتم تشفير/ تجزئة وحماية كلمات المرور بصفة دائمة من الإفصاح غير المصرح به أثناء تخزينها و/أو نقلها بغض النظر عن أسلوب أو وسائط التخزين. ويتم تشفير كلمات المرور للحسابات ذات الامتيازات الخاصة وتخزينها بعيدا عن الموقع إلى جانب ملفات الدعم كلما تم تغيير كلمة المرور لضمان إمكانية استعادتها بالكامل.

ينص كتيب تأمين المعلومات الوطنية على ضوابط تشفير من أجل حماية كلمات المرور من الإفصاح عنها دون موافقة أثناء تخزينها و/أو نقلها.

CY 7 أن يتم توثيق وحدات أمن الأجهزة، حيثما يتم استخدامها، وفقا للمستوى رقم 2 من مستويات المعهد القومي للمعايير والتكنولوجيا FIPS 140-2 [FIPS 140-2] أو للمعايير العامة [CC3-1] EAL4.

ينص كتيب تأمين المعلومات الوطنية على أنه في حالة استخدام نماذج أمن الأجهزة، يتم اعتمادها وفقا للمستوى رقم 2 على الأقل من مستويات المعهد القومي للمعايير والتكنولوجيا FIPS 140-2 [FIPS 140-2] أو للمعايير العامة [CC3-1] EAL4.

يعد FIPS 140-2 بمثابة متطلبات أمنية لوحدات تشفير، ينشرها المعهد القومي للمعايير والتكنولوجيا. ويوفر الأساس للاختبار والتحقق وفي النهاية توثيق وحدات التشفير.

ويتم حاليا مراجعة المواصفات من قبل المعهد القومي للمعايير والتكنولوجيا من خلال إصدار جديد للوثيقة. ومن المزمع أن يتم نشر FIPS PUB 140-3 عام 2009.

وتوفر المستويات المختلفة للمواصفات مستويات مختلفة للأمن وتحظى، عند المستويات الأعلى، بمتطلبات توثيق مختلفة.

المستوى 1: أدنى مستويات الأمن. ليس هناك حاجة إلى آليات أمن مادية بالوحدة بخلاف الشروط المتعلقة بالأجهزة المُصنفة في فئة الإنتاج.

المستوى 2: أمن مادي كاشف للعبث أو أقفال مقاومة للسرقة. ينص المستوى 2 على التوثيق القائم على الأدوار. ويسمح بتشفير البرمجيات بالأنظمة متعددة المستخدمين في مختلف الأوقات عند استخدامها مع مستوى التصنيف C2 أو أي نظام تشغيل موثوق ومعادل.

المستوى 3: أمن مادي كاشف للعبث. ينص المستوى 3 على التوثيق القائم على الهوية.

المستوى 4: يوفر الأمن المادي غطاء حماية حول وحدة التشفير. ويحمي أيضا من التقلبات في بيئة الإنتاج.

المعايير العامة لتقييم أمن تكنولوجيا المعلومات (المشار إليها اختصارا بالمعايير العامة) هي مواصفات دولية (ISO/IEC 15408) لتوثيق واعتماد أمن الحاسوب. وتندرج حاليا ضمن الإصدار 3-1 [1].

تعد المعايير العامة إطارا يمكن أن يحدد مستخدمو نظام الحاسوب من خلاله متطلباتهم الأمنية؛ ويستطيع الموردون بعد ذلك تنفيذ و/أو تقديم المطالبات بشأن السمات الأمنية لمنتجاتهم؛ ويمكن أن تتولى معامل الاختبار تقييم المنتجات لتحديد ما إذا كانت تفي بالفعل بالمطالبات. وبمعنى آخر، تؤكد المعايير العامة على إجراء عملية تحديد مواصفات وتنفيذ وتقييم المنتج الأمني للحاسوب بأسلوب صارم وقياسي.

مستوى توكيد التقييم – التصنيف الرقمي الذي يصف عمق وقوة عملية التقييم. ويتوافق كل مستوى من مستويات توكيد التقييم مع حزمة من حزم متطلبات توكيد الأمن (أنظر أعلاه) التي تشمل التطور الكامل للمنتج مع مستوى الدقة المحدد. وتتضمن المعايير المشتركة سبعة مستويات، حيث يكون المستوى الأول لتوكيد التقييم بمثابة الأساس (وبالتالي الأرخص من حيث التنفيذ والتقييم) والمستوى السابع الاكثر صرامة وتشددا (والأعلى تكلفة).

CY 8 أن يتم نقل مفاتيح التشفير بصورة مادية فقط في HSMs للوفاء بالبند CY5.

تعد وحدة تأمين البرمجيات (والتي غالبا ما يشار إليها اختصارا بمصطلح HSM) نمطا من أنماط معالجات التشفير الآمنة التي تستهدف إدارة المفاتيح الرقمية لتطبيقات الخوادم. وتعتبر أجهزة مادية تأتي في المعتاد في صورة بطاقة برنامج تكميلي أو جهاز أمني خارجي يمكن توصيله بصورة مباشرة بالخادم أو حاسوب الأغراض العامة.

تتمثل أهداف وحدة تأمين البرمجيات فيما يلي: (أ) الإصدار الآمن و(ب) التخزين الآمن و(ج) استخدام مواد بيانات التشفير والبيانات الحساسة. وتوفر وحدة تأمين البرمجيات حماية منطقية ومادية لهذه المواد من الاستخدام غير المصرح به والخصوم المحتملين. وبإيجاز، فهي تحمي مفاتيح التشفير ذات القيمة العالية.

ينبغي أن تكفل المؤسسة استخدام وحدات تأمين البرمجيات، التي تلتزم بالبند CY5 فقط، في تخزين مفاتيح التشفير.

CY 9 أن يتم تحديد عمليات إدارة المفاتيح وفقا لـ [ISO11770-1] واستخدامها في إدارة دورة حياة مفاتيح التشفير، بما يشمل المهام التالية:

- **أدواروومسؤوليات الجهات المسئولة عن حفظ المفاتيح.**
- **إصدار المفاتيح.**
- **الرقابة المزدوجة والمعارف المُقسمة.**
- **تخزين المفاتيح بصورة آمنة.**
- **استخدام المفاتيح.**
- **التوزيع والنقل الآمن للمفاتيح.**
- **دعم واستعادة المفاتيح.**
- **الفحص الدوري لحالة المفاتيح.**
- **الكشف عن المفاتيح.**
- **إلغاء وتدمير المفاتيح.**
- **عمليات المراجعة والتدقيق والتوثيق.**

تحدد المؤسسة السياسات والإجراءات الخاصة بإدارة دورة حياة مفاتيح التشفير. وتشمل الإجراءات، كحد أدنى، المهام المذكورة أعلاه.

CY 10 أن يفي مقدمو خدمة الشهادات المعتمدة من قبل الحكومة ممن يصدرون شهادات الهوية الرقمية بمعايير هيئات التوثيق التي تصدر الشهادات المؤهلة وفقا لما هو محدد في [CWA14167-1]. وفيما يتعلق بالشهادات غير ذات الهوية، يفي مقدمو خدمة الشهادات المعتمدة كحد أدنى بمتطلبات الشهادات غير المؤهلة وفقا لما هو محدد في [CWA14167-1]. وينصح بأن يستخدم مقدمو خدمة الشهادات المعتمدة والمؤسسة أنظمة الإلغاء الإلكتروني للحد من مخاطر التحايل في استخدام الشهادات الرقمية.

ينص كتيب تأمين المعلومات الوطنية على التزام مقدمي خدمة الشهادات المعتمدة من قبل الحكومة بالمتطلبات المذكورة بالبند CY10.

يوصي كتيب تأمين المعلومات الوطنية بأن تتولى المؤسسة ومقدمو خدمة الشهادات المعتمدة تقييم ونشر أنظمة الإلغاء الإلكترونية للحد من مخاطر التحايل في استخدام الشهادات الرقمية. وتتضمن مثل هذه الأنظمة بروتوكول الشهادات الإلكترونية وتصحيح المسار المفوض واكتشاف المسار المفوض وغير ذلك.

CY 11 أن تفي أنظمة مقدمي خدمات الشهادات المعتمدة التي توفر البطاقات الأمنية الذكية بالمتطلبات الخاصة بخدمات توفير الأجهزة وفقا لما هو محدد في [CWA14167-1].

تفي أنظمة التوثيق الأمني/ مقدمي خدمات الشهادات المعتمدة التي توفر البطاقات الأمنية الذكية بالمتطلبات الخاصة بخدمات توفير الأجهزة وفقا لما هو محدد في [CWA14167-1].

تحدد اتفاقية ورشة عمل CEN (CWA) المتطلبات الأمنية للمنتجات ومكونات التكنولوجيا التي يستخدمها مقدمو خدمات الشهادات المعتمدة من أجل إصدار شهادات مؤهلة وغير مؤهلة. ويتم استخدام هذه الشهادات بالإضافة إلى التوقيعات الإلكترونية والتوقيعات الإلكترونية المتقدمة وفقا للقرار EC/93/1999 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 13 ديسمبر 1999 بشأن الإطار المجتمعي للتوقيعات الإلكترونية [Dir.1999/93/EC].

تحظى اتفاقية CWA بأهمية خاصة لمصنعي الأنظمة الجديرة بالثقة المستخدمة في إدارة الشهادات. وتوفر نظرة عامة حول نظام مقدمي خدمات الشهادات المعتمدة المقسم إلى عدد من الخدمات. وتعد بعض هذه الخدمات إلزامية ويطلق عليها مصطلح "الخدمات الرئيسية"، بينما تكون الأخرى اختيارية ويطلق عليها مصطلح "الخدمات التكميلية".

تشمل الخدمات الرئيسية خدمات مقدمي خدمات الشهادات المعتمدة التالية:

أ- خدمة التسجيل – التحقق من الهوية وأي خصائص محددة للخاضعين للدراسة، إن أمكن ذلك.

ب- خدمة إصدار الشهادات – إصدار الشهادات.

ت- خدمة النشر – تقديم الشهادات ومعلومات السياسة إلى الخاضعين للدراسة والأطراف الموثوقة.

ث- خدمة إدارة الإلغاء – السماح بمعالجة طلبات الإلغاء.

ج- خدمة حالة الإلغاء – توفير معلومات حول حالة إلغاء الشهادات إلى الأطراف الموثوقة.

تشمل الخدمات التكميلية خدمتين اختياريتين من خدمات مقدمي خدمات الشهادات المعتمدة:

أ- خدمة توفير الأجهزة للخاضعين للخدمة – إعداد وتقديم جهاز إنشاء التوقيعات إلى الخاضعين للخدمة. ويتضمن ذلك توفير جهاز إنشاء التوقيعات الآمن.

ب- خدمة الخاتم الزمني – تقديم خدمة الخاتم الزمني الذي قد يكون مطلوبا لأغراض التحقق من التوقيعات الالكترونية.

ينبغي أن يقوم مقدمو خدمات الشهادات المعتمدة بتطبيق الأنظمة التي توفر جميع الخدمات الرئيسية.

توفر هذه المواصفات معايير للأنظمة الجديرة بالثقة التي تقدم الخدمات الرئيسية والتكميلية وتصدر كل من الشهادات المؤهلة وغير المؤهلة. ويعني الوفاء بشروط إصدار الشهادات المؤهلة أنه قد تم بطبيعة الحال الوفاء بشروط إصدار الشهادات غير المؤهلة.

CY 12 أن يتم إصدار أي شهادات رقمية مستخدمة بنظام الإنتاج من قبل مقدمي خدمة الشهادات المعتمدة من قبل الحكومة.

ينص كتيب تأمين المعلومات الوطنية على أن يتم إصدار الشهادات المستخدمة في أي نظام إنتاج من قبل مقدمي خدمة الشهادات المعتمدة من قبل الحكومة. وتعد وزارة الداخلية هي الجهة الحكومية الوحيدة المنوطة حاليا بإصدار الشهادات.

11 - إرشادات حول أمن الأجهزة المحمولة والعمل خارج الموقع [OS]

11-1 أهداف السياسة

11-2 السياسة والضوابط الرئيسية – عام

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

OS 1 أن تتولى وضع السياسات التي تحكم ما إذا كان يمكن استخدام أجهزة الهواتف المحمولة والحاسوب المحمول في منظماتهم وكيفية استخدامها.

ينبغي أن تحدد المؤسسة السياسات والإجراءات التي تحكم استخدام أجهزة الهواتف المحمولة والحاسوب المحمول في منظماتهم. ويجب أن تشمل السياسات، ضمن أمور أخرى، ملكية تلك الأجهزة والضوابط الأمنية التي تتماشى مع تصنيف الأصول وتتبعها والالتزام بها.

OS 2 ألا تقوم بإجراء محادثات مصنفة باستخدام أجهزة الهواتف المحمولة وأجهزة الحاسوب المحمول المزودة بإمكانية إجراء المحادثات الهاتفية من خلال استخدام الملحقات التي تعمل من خلال البلوتوث.

لا يوصي كتيب تأمين المعلومات الوطنية باستخدام بروتوكول البلوتوث. وفي حالة استخدامه، ينبغي أن يكفل المستخدمون عدم استخدامه في في إجراء المحادثات المصنفة ويتضمن ذلك استخدام سماعات الرأس التي تعمل من خلال البلوتوث.

OS 3 ألا يتم تفعيل منافذ أجهزة الهواتف المحمولة والحاسوب المحمول ذات وصلات منافذ البلوتوث التسلسلية إذا كان الجهازيحمل معلومات مصنفة.

بالإضافة إلى البند OS2، يتم تعطيل وصلات البلوتوث التسلسلية بأجهزة الهواتف المحمولة والحاسوب المحمول التي تحمل معلومات مصنفة من أجل تجنب الكشف عنها باعتبارها نقاط هوم.

OS 4 ألا يتم السماح بدخول الهواتف المحمولة المزودة بأجهزة تسجيل إلى المناطق ذات الخطورة العالية دون موافقة مسبقة من قبل مدير أمن المعلومات.

تحدد المؤسسة الإجراءات والضوابط بما يكفل عدم السماح بدخول الهواتف المحمولة المزودة بأجهزة تسجيل إلى المناطق الخاضعة للرقابة دون موافقة مسبقة من قبل مدير أمن المعلومات.

OS 5 يجب أن تقوم جميع أجهزة الهواتف المحمولة والحاسوب المحمول بتشفير المعلومات التي تحملها وحمايتها بكلمة مرور.

ينبغي أن تكفل المؤسسة أن تقوم جميع أجهزة الهواتف المحمولة والحاسوب المحمول بتشفير المعلومات (متى أمكن). ويحظى التشفير بقوة ملائمة ويتماشى مع المتطلبات المحددة بالفصل C10، بعنوان "التشفير".

OS 6 يجب أن يتم وضع جميع أجهزة الهواتف المحمولة والحاسوب المحمول تحت الإشراف المباشر والمستمر أثناء الاستخدام أو المحافظة عليها في مأمن في حالة عدم الاستخدام.

ينبغي أن تتولى المؤسسة توعية المستخدمين بإمكانية تعرض أجهزة الهواتف المحمولة والحاسوب المحمول للسرقة بسهولة. ومن ثم، ينبغي أن يقوم المستخدمون بحماية أجهزة الهواتف المحمولة والحاسوب المحمول وعدم تركها دون رقابة. ويجب الحفاظ على أجهزة الهواتف المحمولة والحاسوب المحمول في مكان آمن عند عدم استخدامها.

وعلى سبيل المثال، ينبغي أن ينظر المستخدمون خلال السفر في استخدام أقفال كابلات أجهزة الحاسوب المحمول من أجل توفير الحماية المادية لأجهزة الحاسوب المحمول.

OS 7 ألا يتم استخدام أجهزة الهواتف المحمولة والحاسوب المحمول غير المملوكة بصورة مباشرة للمؤسسة أو الخاضعة لرقابة المؤسسة داخل أنظمة المؤسسة. وينبغي أن تتم إدارة ومساءلة وتوثيق أجهزة الهواتف المحمولة والحاسوب المحمول غير المملوكة للمؤسسة أو الخاضعة لرقابة المؤسسة بنفس الأسلوب الذي تخضع له الأجهزة المملوكة للمؤسسة. ويمكن أن تكون أجهزة الهواتف المحمولة والحاسوب المحمول المملوكة للمؤسسة متصلة بصورة مؤقتة بإحدى الشبكات غير المملوكة للمؤسسة، بشرط استخدام جدار ناري مناسب لحماية الجهاز من أي مخاطر محتملة تنشأ عن الشبكة غير الخاضعة لرقابة المؤسسة.

تتولى المؤسسة تحديد السياسات والإجراءات وتطبيق الضوابط بما يكفل عدم استخدام أجهزة الهواتف المحمولة والحاسوب المحمول غير المملوكة بصورة مباشرة للمؤسسة أو غير الخاضعة لرقابتها داخل أنظمة المؤسسة.

يهدف ذلك إلى ضمان وجود بيئة عمل قياسية خاضعة للرقابة بتلك الأجهزة والحد من نقاط الضعف ذات الصلة بتلك الأنظمة.

يتم تنصيب برنامج لمكافحة الفيروسات الضارة والكشف عنها وبرنامج للإصلاح على جميع أجهزة الهواتف المحمولة والحاسوب المحمول المملوكة للمؤسسة والخاضعة لرقابتها وتزويدها بأحدث ملفات توقيعات الفيروسات وتعريفات البرمجيات الضارة من أجل تجنب فيروسات الحاسوب والبرمجيات الضارة.

وفي حالة أجهزة الهواتف المحمولة والحاسوب المحمول غير المملوكة بصورة مباشرة للمؤسسة أو غير الخاضعة لرقابتها، ولكن مسموح لها بالدخول على أنظمة المؤسسة، فإنها تخضع للإدارة والرقابة والتوثيق بنفس الأسلوب الذي تخضع له الأجهزة المملوكة للمؤسسة.

ويمكن أن تكون أجهزة الهواتف المحمولة والحاسوب المحمول المملوكة للمؤسسة متصلة بصورة مؤقتة بإحدى الشبكات غير المملوكة للمؤسسة، بشرط استخدام جدار ناري مناسب لحماية الجهاز من أي مخاطر محتملة تنشأ عن الشبكة غير الخاضعة لرقابة المؤسسة.

ينبغي أن يكفل المستخدمون مسح أجهزة الهاتف المحمول والحاسوب المحمول للكشف عن البرامج الضارة قبل إعادة توصيلها بشبكة المؤسسة.

OS 8 ألا تتصل أجهزة الهواتف المحمولة والحاسوب المحمول غير الموثقة بأنظمة المؤسسة أو تتولى تخزين المعلومات الخاصة بالمؤسسة. ومع ذلك، يتم السماح لأجهزة الهواتف المحمولة والحاسوب المحمول المتصلة بصفة مؤقتة بشرط أن يتم فصلها عن الشبكات الرئيسية عن طريق جدار ناري.

ينبغي أن تحدد المؤسسة الإجراءات التي تكفل عدم توصيل أجهزة الهواتف المحمولة والحاسوب المحمول غير الموثقة بأنظمة المؤسسة أو تتولى تخزين المعلومات المصنفة الخاصة بالمؤسسة.

ومع ذلك، يمكن توصيل أجهزة الهواتف المحمولة والحاسوب المحمول غير الموثقة بصفة مؤقتة بالشبكة الضيف بالمؤسسة لأغراض مثل الدخول على شبكة الإنترنت أو الطباعة أو غير ذلك. ويتم فصل تلك الشبكات عن الشبكة الرئيسية عن طريق جدار ناري.

OS 9 في حالة فقدان أو سرقة أجهزة الهواتف المحمولة والحاسوب المحمول، ينبغي أن يتم إبلاغ مدير/ مكتب أمن المعلومات وأجهزة تطبيق القانون المعنية على الفور. ويتم التعامل مع حالات الفقدان/ السرقة بمقتضى الإرشادات الخاصة بإدارة الحوادث [IM].

يتم توعية العاملين بضرورة إبلاغ مدير/ مكتب أمن المعلومات وأجهزة تطبيق القانون المعنية على الفور عن فقدان أو سرقة أجهزة الهواتف المحمولة والحاسوب المحمول. وتتعامل المؤسسة مع جميع هذه الحوادث بما يتماشى مع السياسات والإجراءات المحددة لإدارة الحوادث.

OS 10 أن يكون هناك خطة للإتلاف/ الإغلاق/ المسح عن بعد /التدمير الذاتي في حالات الطوارئ فيما يتعلق بأي أجهزة هواتف محمولة وحاسوب محمول يتم استخدامها في المواقف التي ترتفع بها احتمالية الفقدان أو الخسائر. وينبغي أن تتم هذه القدرة عن بعد فيما يتعلق أجهزة الهواتف المحمولة.

ينبغي أن تقوم المؤسسة بتوعية المستخدمين لديها حول كيفية تدمير أو إغلاق أي أجهزة هواتف محمولة وحاسوب محمول في المواقف التي ترتفع بها احتمالية الفقدان أو الخسائر. وينبغي أن تحدد المؤسسة الإجراءات الخاصة بتدمير وإغلاق أجهزة الهواتف المحمولة والحاسوب المحمول وأن تكفل تدريب المستخدمين لديها على استخدامها.

ينبغي أن تنظر المؤسسة في الضوابط التي تيسر الوفاء بالمتطلبات المذكورة أعلاه. ويجب أن تسمح أجهزة الهواتف المحمولة بتشغيل هذه الخاصية عن بعد.

12 - إرشادات حول الأمن المادي [PH]

12-1 أهداف السياسة

12-2 إرشادات حول السياسة والضوابط الرئيسية

للوفاء بمتطلبات هذه السياسة، يتعين على **المؤسسة** أن تكفل ما يلي:

PH 1 أن يتم إقرار الحماية المناسبة للأماكن المادية بناءً على عملية تقييم المخاطر. وينبغي أن تتم عملية التقييم خلال مرحلة تصميم البناء الجديد أو، فيما يتعلق بأماكن العمل القائمة، كجزء من عملية إدارة المخاطر المستمرة.

ينص كتيب تأمين المعلومات الوطنية على أن تقر المؤسسة توجها قائما على المخاطر لتحديد وتعريف متطلبات الأمن المادي. وتتم عمليات تقييم المخاطر تلك خلال مرحلة تصميم أي بناء جديد. وفي حالة الهياكل المادية التي تم بناؤها بالفعل، يتولى تقييم المخاطر تقييم مدى ملاءمة الهيكل وتحديد الضوابط الملائمة للتخفيف من حدة المخاطر.

قد تتضمن الضوابط إجراءات عمل قياسية محددة وأجهزة المتابعة والرقابة.

يتم تقييم الأمن المادي كجزء من عملية مستمرة لإدارة المخاطر .

PH 2 أن يتم تقسيم الأماكن المادية اعتمادا على متطلباتها الأمنية. ويتم تخصيص مستوى أمن مادي لكل منطقة. ويحدد الجدول أدناه المستويات:

الحد الأدنى للحماية	يوفر مستوى الحماية المصمم للرقابة على الأصول غير المصنفة (على سبيل المثال: ColoAo). ويعتبر غير ملائم بصفة عامة للعمليات الحكومية (غير العامة).
الحماية الأولية	يوفر مستوى الحماية المصمم للرقابة على الأصول ذات القيمة المعتدلة أو الأصول المصنفة عند مستوى "منخفض". وعادة ما يتم استخدامها كأساس للعمليات الحكومية.
الحماية المتوسطة	يوفر مستوى الحماية المصمم للرقابة على الأصول ذات القيمة المتوسطة أو الأصول المصنفة عند مستوى "متوسط".
الحماية المرتفعة	يوفر مستوى الحماية المصمم للرقابة على الأصول ذات القيمة المرتفعة أو الأصول المصنفة عند مستوى "مرتفع".

ينص كتيب تأمين المعلومات الوطنية على أن تتماشى الضوابط التي يتم تطبيقها من أجل الرقابة الأمنية مع أسلوب تقسيمها/ تصنيفها. وسوف يؤدي تقسيم أي منطقة مادية إلى نطاقات إلى مساعدة المؤسسة على تحديد الضوابط المناسبة واستخدام الموارد المتاحة تحت تصرفها بفاعلية.

PH 3 أن يتم تنفيذ ضوابط الأمن المادي الملائمة في كل منطقة. ويوفر الملحق "أ" تفاصيل ضوابط الحماية الدنيا والأولية، بالإضافة إلى التوصيات الخاصة بالضوابط الإضافية. وتتطلب الحماية المتوسطة فئة إضافية من الضوابط، بينما تتطلب الحماية المرتفعة فئتين إضافيتين من الضوابط. ويمكن أن تدمج المؤسسة ضوابط إضافية إلى جانب تلك الضوابط التي تقرها هذه السياسة.

بالإضافة إلى البند PH2، ينص كتيب تأمين المعلومات الوطنية على تصنيف كل منطقة مادية وتطبيق الضوابط الأمنية اللازمة. ويوفر الملحق "أ" من كتيب تأمين المعلومات الوطنية تفاصيل الضوابط الدنيا والأولية. ويوصي أيضا بضوابط إضافية لمستوى الحماية المتوسطة والعليا. ويمكن أن تجمع المؤسسة بين هذه الضوابط وتلك الضوابط التي تنص عليها هذه السياسة.

PH 4 تنفيذ سياسة "المكتب النظيف" و"الشاشة النظيفة".

تتولى المؤسسة تنفيذ سياسة "المكتب النظيف" و"الشاشة النظيفة" في جميع الأوقات، بما يكفل عدم ترك المواد المحظورة دون مراقبة أو دون حماية على مكاتبها أو غير ذلك. وتؤدي سياسة "المكتب النظيف" و"الشاشة النظيفة" إلى غرس أهمية الأمن بين المستخدمين والتخفيف من حدة المخاطر المتعلقة بسرقة المعلومات من خلال التوسع في مفاهيم "تحقيق الأمن من خلال الغموض".

ينبغي أن تكفل المؤسسة توفير الأدوات اللازمة للمستخدمين لديها من أجل الالتزام بفاعلية بهذه السياسة. وقد يتضمن ذلك:

أ. استخدام الخزانات والصناديق المغلقة لحماية الوثائق الحساسة أثناء ساعات العمل. ويعتمد اختيار الصناديق على مستوى المخاطر. وينبغي وضع عوامل المخاطر في الاعتبار، مثل الوصول إلى عمال صيانة المبنى دون رقابة عقب انتهاء ساعات العمل الرسمية.

ب. ينبغي أن يتم إغلاق مكاتب العاملين التي يتم تخزين المعلومات أو الأصول الحساسة بها عند تركها دون رقابة.

ج. تدريب العاملين على مراقبة والإبلاغ عن المكاتب التي يتم تركها مفتوحة دون قصد أو الأصول المعلوماتية التي يتم تركها دون حماية.

د. الشاشات ولوحات المفاتيح التي يتم وضعها بأسلوب لا يمكن للأشخاص غير المصرح لهم رؤيتها.

هـ. استخدام الزجاج غير الشفاف أو الستائر المثبتة على النوافذ من الداخل والحواجز الزجاجية لمنع إمكانية الرؤية من الخارج.

PH 5 أن تفي غرف الخوادم/ البيانات بمتطلبات الحماية المتوسطة.

ينص كتيب تأمين المعلومات الوطنية على أن تكون غرف الخوادم/ البيانات أو غرف معالجة/ تخزين المعلومات المماثلة تفي، كحد أدنى، بمتطلبات الحماية المتوسطة.

PH 6 أن تكون الكابلات التي تحمل المعلومات المصنفة عند المستويات C1-C3 منفصلة ماديا (بما في ذلك كابلات الألياف الضوئية) وأن تمر في أنابيب منفصلة عن الكابلات التي تحمل المعلومات المصنفة على المستوى القومي.

يتم فصل الكابلات التي تحمل المعلومات المصنفة عند المستوي C4 أو أكثر منفصلة ماديا عن الكابلات التي تحمل المعلومات المصنفة عند المستوى C3 أو أقل. ويتم حماية الكابلات من خلال مواسير مستقلة ماديا. ويهدف ذلك إلى توفير الحماية المناسبة من الاعتراض والخسائر.

وعلاوة على ذلك، يتم تطبيق ضوابط إضافية لحماية الكابلات التي تحمل المعلومات المصنفة عند المستوى C4 أو أكثر. وقد يتضمن ذلك:

أ. تركيب المواسير المصفحة والغرف أو الصناديق المغلقة عند نقاط التفتيش والنهاية.
ب. استخدام المسارات البديلة و/أو ووسائط النقل التي توفر الحماية المناسبة.
ج. استخدام الدروع الكهرومغناطيسية لحماية الكابلات.
د. مراقبة الوصول إلى لوحات التحكم وغرف الكابلات.

PH 7 **أن يتم وضع وتنفيذ خطة أمن للمواقع وإجراءات تشغيل قياسية لجميع المناطق الآمنة، حسب الاقتضاء. وتشتمل المعلومات التي يتم تغطيتها، على سبيل المثال لا الحصر، على:**

أ. ملخص لعملية تقييم مخاطر الأمن الوقائي.

ب. أدوار ومسؤوليات مسؤول وأعضاء فريق عمل المرفق أو مسؤول وأعضاء فريق عمل أمن تكنولوجيا الاتصالات والمعلومات.

ج. إدارة وتشغيل وصيانة نظام مراقبة الوصول الإلكتروني إلى المعلومات و/أو نظام الإنذار الأمني.

د. الإدارة الرئيسية وانضمام وإلغاء مستخدمي النظام وإصدار الهوية الشخصية.

هـ. تراخيص أعضاء فريق العمل وتدريب التوعية الأمنية وإصدار التعليمات المنتظمة.

و. فحص عمليات المراجعة والتدقيق والسجلات الصادرة.

ز. عمليات الفحص والمتابعة في نهاية اليوم.

ح. الإبلاغ عن حوادث وخرق أمن تكنولوجيا الاتصالات والمعلومات.

تضع المؤسسة خطة أمنية شاملة يتم استكمالها من خلال إجراءات تشغيل قياسية للمنطقة الآمنة داخل المنظمة. وتتناول الخطة الأمنية، كحد أدنى، تفاصيل النقاط المحددة أعلاه.

13 – ألمحاكاة [VL]

13-1 أهداف السياسة

13-2 إرشادات حول السياسة والضوابط الرئيسية

VL 1 تقييم المخاطرة المتعلقة بالتكنولوجيا الافتراضية

•تقييم المخاطرفي سياق السياسات القانونية والتنظيمية والتشريعات ذات الصلة

•تقييم تأثيرإدخال التكنولوجيا الإفتراضية على بنيتك المعلوماتية التحتية الموجودة والموقف الامني المرتبط.

يتعين على المؤسسات تقييم إيجابيات وسلبيات استخدام الافتراضية. يجب إجراءعملية تقييم مخاطر شاملة لتقييم المزايا والعيوب، هذه العملية ينبغي أن تتجاوز إجراءات ال ROI الطبيعية وأن تشمل الحالات في تتدخل في العمية.مثل التأثيات القانونية والتنظيميةلدى المؤسسة. كما ينبغي أن تضمن توافر المهارات اللازمة والخبرات داخل المؤسسة.

VL 2 تقوية الطبقة الوسيطة البرمجية التي تقوم بإدارة الانظمة الإفتراضية و جميع الانظمة والاجهزة المرتبطة بها بناءً على افضل الممارسات و التوجهات الامنية المتبعة إضافة إلى توصيات العميل.

يتعين على المؤسسات تقوية الطبقة البرمجية الوسيطة إعتماداً على توصيات البائع والتوجهات الأمنية. وهذا يتطلب تقوية الطبقة الوسطية البرمجية بصورة مستقلة عن الخطوات العادية لتقوية الطبقة البرمجية الوسيطة لنظام التشغيل. الإعدادات غيرالصحيحة على مقوي الطبقة البرمجية الوسطية قد تسمح للأجهزة الظاهرية الاتصال و الارتباط بأجهزة ظاهرية أخرى مستضافة على نفس الحاسوب.

VL 3 فرض الامتيازات الأقل وفصل الواجبات (ارجع إلى القسم C-9 إدارة الوصول) لإدارة بيئة افتراضية

- **تحديد أدوار معينة والامتيازات المطلوبة لكل مسؤول في إدارة البرامج الافتراضية المركزية.**
- **تقييد الوصول ا لإداري المباشر إلى طبقة إدارة الانظمة ا لإفترا ضية إلى أقصى حد ممكن.**
- **اعتمادا على المخاطر وتصنيف المعلومات التي يتم التعامل معها، يجب على المؤسسات النظر في إمكانية استخدام عوامل التوثيق المتعددة أو تقسيم التحكم في إدارة كلمات ال سر على إثنين.**

VL 4 ضمان الأمن المادي الكافي لمنع الوصول غير المصرح به إلى بيئة تقنية افتراضية.

بما ان الإعداد الافتراضي هو عدد من الأنظمة التي ربما تتفاوت في تصنيفها و خصائصها الامنية ،لذا من الاهمية بمكان التأكد من أن يتم التحكم في الوصول، التنظيم والإدارة بإحكام.

الأمن المادي للآلة التي تستضيف البيئة الافتراضية مهم للغاية. سيساعد الوصول المادي من تمكين شخص من اسقاط البيئة الافتراضية أو نسخ الجهاز الظاهري ليتم استخدامها في مكان آخر مما يؤدي إلى تسرب المعلومات.

VL 5 بيئة التكنولوجيا الافتراضية يجب ان تعدل بحيث يضاف إليها طرق امنية أخري لتوفير التحكم الامن على طبقات) نهج الدفاع من العمق(لإستكمال الضوابط المقدمة من الموردين والتكنولوجيا.

تكنولوجيا أمن الطرف الثالث مثل برامج مكافحة الفيروسات، يجب أن تستخدم في جميع إعدادات البيئات الافتراضية، إضافة إلى الضوابط الأمنية المستخدمة في الجهاز المضيف. لا ينبغي أن يفترض أن ضوابط المضيف ستكون كافية لحماية جميع البيئات الافتراضية المستضافة.

VL 6 فصل الأجهزة الإفتراضية بناء على تصنيف البيانات التي يتم معالجتها و / أو مواقع تخزينها.

الاجهزة الظاهرية التي تحتوي على بيانات ذات مستوى التصنيف الامني"مرتفع" لا يجب استضافتها على نفس البيئة الإفتراضية مع اجهزة ظاهرية ذات مستوى تصنيف امني "منخفض" وذلك لتقيد الجهزة ذات التصنيف الامني "منخفض" بضوابط اقل مقارنة بتلك التي تنصف "مرتفع". لذا يسهل مهاجمتها و إختراقها و الحصول على البيانات ذات

التصنيف "مرتفع" الموجودة بنفس البيئة الإفتراضية. يجب تصنيف البيئة الفتراضية المضية بنفس تصنيف الجهاز الظاهري ذو مستوى التصنيف الامني الاعلى بها.

VL 7 إدارة التغيير (أنظر القسم B-6 إدارة التغيير) عملية تشمل بيئة التكنولوجيا الافتراضية.

- **تتأكد من تحديث بيانات الجهاز الافتراضي والحفاظ على اكتمال صورة الجهاز الافتراضي في جميع ا لأوقات.**
- **ينبغي الحرص على صيانة وتحديث للاجهزة الافتراضية التي ليست في حالة نشطة (نائمة أو لم تعد تستخدم).**

يجب متابعة البيئات الإفتراضية عند عملية إدارة التغيير للحفاظ على سلامة وإمتثال البيئة الافتراضية.

VL 8 يجب أن يتم تسجيل ومتابعة سجلات من بيئة التكنولوجيا الافتراضية جنبا إلى جنب مع البنية التحتية لتقنية أخرى (أنظر القسم B-10 تسجيل الأداء والمتابعة الأمنية).

التسجيل والرصد في البيئة افتراضية يماثل التسجيل والرصد في البنية التحتية المعلوماتية الحقيقية.