سياسة تأمين المعلومات الوطنية

«الطبعة الثانية»

إخلاء مسؤلية و حقوق قانونية

هذه الوثيقة صممت و أُعدت من قبل وزارة المواصلات و الاتصالات بدولة قطر. تحمل هذه الوثيقة عنوان «سياسة تأمين المعلومات الوطنية - الطبعة الثانية» و يشار اليها لاحقاً بكلمة («العمل») ، تعد هذه الوثيقة في المقام الاول وثيقة استرشادية للعاملين بالإدارة العليا، وإدارة المخاطر و إدارة تقنية المعلومات العاملين في أمن تقنية المعلومات. وزارة المواصلات والاتصالات بدولة قطر هي صاحبة الحق الوحيد في في مراجعة و تحديث هذه الوثيقة «العمل»، في حالة استنساخ او توزيع هذا العمل سواء جزئياً او كلياً و بغض النظر عن وسيلة الاستنساخ او التوزيع يجب ذكر وزارة المواصلات و الاتصالات كمصدر و مالك ل«العمل».

يجب الحصول علي إذن كتابي مسبق من وزارة المواصلات و الاتصالات بدولة قطر في حالة الرغبة في إعادة إستنساخ او توزيع هذا «العمل». إن موافقة الوزارة بإعادة استنساخ او توزيع «العمل» كمنتج تجاري او إجراء خدمات من خلال الإشارة إلي إسم او علامة تجارية او مقدم للخدمة او اي شيء اخر لاتعني بالضرورة التوصية به او تفضيله من قبل وزارة المواصلات و الاتصالات ولايجوز للمنتج او صاحب العلامة التجارية او مقدم الخدمة ان يستخدم موافقة الوزارة للدعاية او الترويج

مقدمة

أثّرت وزارة المواصلات و الاتصالات في حياة المواطنين والمقيمين مما أدى إلى تغييرات إيجابية في طريقة التعامل مع عالم الاتصالات وتكنولوجيا المعلومات في شتى المجالات. فمن خلال برامجنا المختلفة مثل «حكومي – الحكومة الالكترونية»، يسّر للمواطنين والمقيمين العديد من الإجراءات الحكومية على شبكة الإنترنت.

وكتوجّه استراتيجي، أكدت الرؤية الوطنية القطرية ٢٠٣٠ على الركائز التالية باعتبارها المفاتيح الأساسية لاستراتيجية تنمية دولة قطر:

- التنمية البشرية
- التنمية الاجتماعية
- التنمية الاقتصادية
- التنمية البيئية

إن مهمة وزارة المواصلات والاتصالات هى العمل على تحقيق هذه الرؤية من خلال التطبيق الناجح والفعّال لتكنولوجيا المعلومات والاتصالات.

فى هذا العالم المترابط، أدى التوسع فى استخدام تكنولوجيا المعلومات إلى تداول كم هائل من المعلومات بحرية بين الهيئات الحكومية والجهات الأخرى، مما يثير بعض التساؤلات عندما يتعلق الأمر بأمن هذه المعلومات وسلامتها. إنّ من واجب كل من يجمع ويستخدم ويشارك في نقل مثل هذه المعلومات، التأكد من حمايتها وسلامتها وتأمين التعامل معها.

لذا، نحن بحاجة للعمل على تحديد الإستراتيجيات السليمة للحوكمة ومجموعة السياسات والإجراءات الفعّالة والمتممة للتكنولوجيا المستخدمة، كما أن التوعية والتعليم فيما يتعلق بحماية المعلومات أثناء استخدامها وتداولها ضرورة ذات أهمية قصوى للمستخدمين والعاملين عليها على حد سواء.

في هذا الصدد، يسر وزارة المواصلات و الاتصالات أن يعلن عن حزمة سياسة تأمين المعلومات الوطنية التي اعتمدت مؤخراً من قبل مجلس إدارة وزارةالمواصلات و الاتصالات.

إنّ سياسة تأمين المعلومات الوطنية تتضمن الأساسيات والأدوات اللازمة ذات الصلة لتطبيق نظام مؤسّسي آمن وفعّال لإدارة المعلومات الوطنية. ويسر الفريق القطري للإستجابة لطوارئ الحاسب الآلي (كيوسيرت) التابع لوزارة المواصلات و الاتصالات أن يتواصل معكم دائماً لتقديم المساعدة والدعم في سعيكم لتطبيق هذه السياسة.

نتطلع دائماً للعمل معاً سعياً لأمن واستقرار دولة قطر.

خـــالد نعم الله الهاشـــمي

المـــدير التنـفيـــذي

وكيل الوزارة المساعد

وزارة المواصلات و الاتصالات

سياسة تصنيف المعلومات الوطنية

[IAP-NAT-DCLS]

جدول المحتويات

المؤلف: وزارة المواصلات و الاتصالات بقطر

الإصدار: ٢,٠

التصنيف: عام

تاريخ الإصدار: اكتوبر ٢٠١٥

١. أهداف السياسة

تحدد هذه السياسة منهجية رفيعة المستوى لتصنيف المعلومات لدى المؤسسات بدولة قطر. الأساس المنطقي لتصنيف المعلومات إلى فئات هو إعطاء قيم أو درجات ملائمة للمعلومات وتحديد مخاطرها وسبل الحماية المناسبة الواجب اتباعها لكل فئة.

تغطي هذه السياسة المخاطر التالية:

- الإفصاح عن المعلومات بدون تفويض
- تعديل المعلومات بدون تفويض
- عدم توفر المعلومات

سوف يؤدي الاستخدام المتسق لنهج تصنيف المعلومات إلى تيسير أنشطة العمل، وضمان الالتزام بأفضل الممارسات المقبولة، والمساعدة على الاحتفاظ بتكاليف أمن المعلومات عند أدنى مستوياتها. وبدون استخدام نظام تصنيف المعلومات، سوف يكون لدي جميع المؤسسات مستويات مختلفة من حماية الأصول، بدون وجود خطوط رئيسية محددة.

٢. نطاق السياسة

تسري هذه السياسة على جميع المؤسسات وأصول المعلومات الخاصة بها، ما لم تكن تتمتع بإعفاء خاص.

يتم استخدام التعريفات التالية المحددة في [IAP-NAT-IAFW][إطار تأمين المعلومات] بهذه السياسة: المؤسسات ، أصول المعلومات والإفصاح عن المعلومات بدون تفويض وتعديل المعلومات بدون تفويض وإتاحة المعلومات.

كما تسري المعايير المرجعية التالية:

[IAP-NAT-IAFW] إطار تأمين المعلومات، ٢٠٠٨

[IAP-NAT-INFA] سياسة تأمين المعلومات الوطنية، ٢٠١٤

[IAP-NAT-CIIP] سياسة حماية البنية التحتية للمعلومات الحرجة، ٢٠١٤

٣. السياسة

٣-١ ينبغي أن تحدد المؤسسات درجة أولوية الالتزام بهذه السياسة من خلال تحديد مدى أهمية عملياتها وفقاً لما يلي:

- الأولوية الأولى: مدى الأهمية لدولة قطر. ينبغي مقارنة العمليات بالملحق «أ»[IAP-NAT-CIIP] [حماية البنية الأساسية المعلوماتية الهامة] للتأكد من مدى أهميتها على المستوى القومي.
- الأولوية الثانية: مدى الأهمية للمؤسسة . ينبغي أن يتم تقييم العمليات اعتماداً على مدى أهميتها في إدارة المؤسسة ، باستخدام تحليل الأثر على العمل. يمكن استخدام الملحق «أ».

٣-٢ ينبغي أن تتولى المؤسسة وضع خطة التزام توضح أولوية التزام العمليات (وفقاً لما هو محدد بالفصل رقم ٣-١) وأصول المعلومات القائمة عليها وجدول تنفيذ عمليات التقييم والرقابة.

٣-٣ بالنسبة لأصول المعلومات، ينبغي على المؤسسة القيام بما يلي:

- تصنيفها وفقاً لنظام التصنيف. يمكن استخدام الملحق «ب».
- تحديد أولويات تنفيذ الضوابط الأمنية اعتماداً على مستوى الأمان الكلي.
- تطبيق الضوابط الأساسية وفقاً لما هو محدد في [IAP-NAT-INFA][سياسة تأمين المعلومات الوطنية] على جميع الأصول المصنفة. ويتم الإشارة إلى الضوابط الرئيسية ضمن [IAP-NAT-INFA] [سياسة تأمين المعلومات الوطنية] باستخدام (*). وعلاوة على ذلك، يمكن تطبيق ضوابط أكثر قوة إذا لزم الأمر.
- حماية أصول المعلومات الخاضعة للرقابة بانتظام على مدار حياتها، منذ إنشائها لحين تدميرها، بما يتناسب مع مدى حساسيتها، بغض النظر عن مكانها أو شكلها أو التكنولوجيا المستخدمة في التعامل معها أو الغرض منها.
- ضمان أن تحظى الأصول ذات متطلبات السرية C1 و C2 وC3 بالعلامة الملائمة وفقاً لما هو محدد في [IAP-NAT-INFA] [سياسة تأمين المعلومات الوطنية].

٤. الالتزام بالسياسة

٤-١ ينبغي أن تخضع جميع المؤسسات للتدقيق والمراجعة بصفة سنوية من قبل هيئة التدقيق والمراجعة بالدولة أو الهيئة التي تحددها للتأكد من التزامها بهذه السياسة.

الملحق «أ» – تحليل الأثر على العمل

لتحديد الأولويات الخاصة بتصنيف أصول المعلومات والمستوى المقابل من الحماية الأمنية، ينبغي إجراء تقييم للأثر بالوسائل المقترحة. ومع ذلك، إذا كان لدى المؤسسات أسلوب لتقييم الأثر على سير العمل، يمكن استخدام ذلك الأسلوب بدلاً من الأسلوب المنصوص عليه بهذا الملحق.

يتم إجراء تحليل الأثر على العمل، الذي يوصي به كتيب تأمين المعلومات الوطنية، عن طريق تقييم أثر فقدان أو تدهور العملية على المؤسسات من خلال عوامل التأثير التالية:

- الأثر على السمعة.
- الأثر الخارجي (الأثر على الهيئات الخارجية والمؤسسات وغيرها).
- الأثر الداخلي (الأثر على الموظفين والؤسسات ذاتها).
- الأثر القانوني (المسؤوليات الناجمة عن عدم الوفاء بالالتزامات القانونية، وعلى سبيل المثال، عدم الالتزام للاتفاقيات واللوائح والتشريعات الخاصة بمستوى خدمة.. إلخ).
- الأثر الاقتصادي (خسائر الإيرادات المباشرة والفرص الاقتصادية الضائعة.. إلخ).
- ينبغي اتخاذ الخطوات التالية لتقييم مدى أهمية العمليات:
- تقييم مدى أهمية كل عامل من عوامل الأثر لدى المؤسسات اعتماداً على التصنيف التالي. ويتم حساب عامل التقييم هذا (a1 to a5) مرة واحدة فقط ويتم استخدامه في كل عملية يتم تقييمها.
- ٠: غير هام
- ١: منخفض الأهمية
- ٢: متوسط الأهمية
- ٣: شديد الأهمية
- ٤: شديد الأهمية للغاية
- لكل عملية يجب أن يتم تحديد الأثر ويُرمز إليه بالرمز (I) على الموسسات فور تعرضها للخسائر أو التدهور من خلال استخدام المقياس التالي. و فيما يتعلق بالعمليات القائمة على عنصر الوقت يجب التأكد من حساب الأثر في أوقات ذروة الاستخدام.
- ٠: لا يوجد تأثير
- ١: تأثير ضئيل
- ٢: تأثير متوسط
- ٣: تأثير كبير
- ٤: تأثير كبير للغاية

استخدام المعادلة التالية لتحديد مدى الأهمية (وفقاً لمقياس حتى ١٠٠) لكل عملية:

قيمة التأثير = 1,25 (α1I1 + α2I2+ α3I3 + α4I4 + α5I5)

مثال عملي

عمليات تقييم عوامل التأثير التنظيمية:

- تقييم الأثر على السمعة: شديد الأهمية (1α=3)
- تقييم الأثر الخارجي: شديد الأهمية (2α=3)
- تقييم الأثر الداخلي: متوسط الأهمية (3α=2)
- تقييم الأثر القانوني: شديد الأهمية للغاية (α 4=4)
- تقييم الأثر الاقتصادي: متوسط الأهمية (5α=2)

اسم العملية: حساب رواتب العاملين والأثر في الأوقات الهامة

- الأثر على السمعة: تأثير كبير (1I=3)
- الأثر الخارجي: تأثير ضئيل (1=2I)
- الأثر الداخلي: تأثير كبير (3=3I)
- الأثر القانوني: تأثير منخفض (I 4=1)

- الأثر الاقتصادي: لا يوجد تأثير (I=1)

قيمة التأثير = (1,25(3x3 + 3x1 + 2x3 + 4x1 + 2x1

يؤدي ذلك إلى أن تصل قيمة الأثر إلى: 30

الملحق ب نموذج تصنيف الأصول

لتحديد تصنيف أصول المعلومات ومستوى الحماية الأمنية المقابل، ينبغي أن يتم اتخاذ الخطوات التالية:

١. تحديد العمليات الرئيسية والقائمين عليها بالمنظمة.

٢. تحديد تبعيات العملية: المعلومات والتطبيقات والأنظمة والشبكات...إلخ.

٣. تحديد التصنيف الأمني لكل من الأصول المعلوماتية بناءً على الجدول رقم ١ أدناه؛ تتمثل مستويات الأمن الكلية فيما يلي: H: مرتفع ، M: متوسط ، L: منخفض

٤. تسجيل التصنيف الكامل (على سبيل المثال: C0I2A2) ومستوى الأمن الكلي (على سبيل المثال: M) لكل من الأصول المعلوماتية.

		A0	A1	A2	A3
I0	C0		L	M	H
	C1	L	L	M	H
	C2	M	M	M	H
	C3	H	H	H	H
I1	C0	L	L	M	H
	C1	L	L	M	H
	C2	M	M	M	H
	C3	H	H	H	H
I2	C0	M	M	M	H
	C1	M	M	M	H
	C2	M	M	M	H
	C3	H	H	H	H
I3	C0	H	H	H	H
	C1	H	H	H	H
	C2	H	H	H	H
	C3	H	H	H	H

مدى إتاحة البيانات

يقصد بإتاحة البيانات وتوافرها إمكانية الوصول إلى البيانات بسهولة وفي المواعيد المحددة خلال ساعات العمل الضرورية واللازمة المتفق عليها مسبقا (أي في اللحظة الضرورية واللازمة وخلال الفترة الزمنية الضرورية واللازمة) من قبل الأشخاص المصرح لهم أو الوسائل التقنية.

Ao: درجة الاعتمادية وزمن الإنتاجية/ التفاعل غير مهم.

A1: درجة الاعتمادية 90% (زمن التوقف ~ 17 ساعة/ أسبوعياً) الحد الأقصى لزمن الاستجابة المسموح به-(1-10) ساعات.

A2: درجة الاعتمادية 99% (زمن التوقف ~ 2 ساعة/ أسبوعياً) الحد الأقصى لزمن الاستجابة المسموح به - (1-10) دقيقة.

A3: درجة الاعتمادية 99,9% (زمن التوقف ~ 10 دقيقة/ أسبوعياً) الحد الأقصى لزمن الاستجابة المسموح به - (1-10) ثانية

سلامة البيانات

يقصد بسلامة البيانات ضمان صحة واكتمال وحداثة وموثوقية البيانات وعدم وجود تعديلات غير مصرح بها.

I0: مصدر المعلومات وتوقيت التعديلات لا يشكلان أهمية

١هذه هي العمليات الهامة للغاية لإدارة المؤسسات بفاعلية.

I1: ينبغي أن يكون تحديد مصدر المعلومات وتوقيت التعديلات ممكناً

I2: يتم تحديد مصدر المعلومات وتوقيت التعديلات والتحقق من صحته بصفة دورية

I3: ينبغي أن يكون هناك إمكانية لإثبات مصداقية وسلامة البيانات لأي طرف ثالث

السرية

يقصد بسرية المعلومات إمكانية وصول الأشخاص أو الوسائل التقنية المصرح لهم فقط إلى البيانات.

C0: معلومات عامة. علامة التصنيف: «عام» .

C1: معلومات محظورة: للاستخدام الداخلي. المواد التي يؤدي الإفصاح عنها إلى التسبب في خسائر طفيفة إلى متوسطة لدى الطرف المتضرر. علامة التصنيف» «داخلي»

C2: معلومات محظورة: يستطيع الوصول إليها مستخدمون محددون أو أدوار محددة أو مجموعات مستخدمين محددة وفقاً لقواعد محددة. المواد التي يؤدي الإفصاح عنها إلى التسبب في خسائر شديدة لدى الطرف المتضرر (وعلى سبيل المثال: بيانات الموارد البشرية والبيانات التأسيسة الرئيسية الحساسة ...إلخ). علامة لتصنيف «وصول محدود».

C3: معلومات محظورة: معلومات سرية يمكن الوصول إليها بصورة محدودة من قبل مجموعة صغيرة للغاية من الأشخاص. المواد التي يؤدي الإفصاح عنها إلى التسبب في خسائر فادحة لدى الطرف المتضرر (التعديلات والقرارات الإدارية على مستوى مجالس الإدارة/ الجهات التنفيذية/ الوزراء ...إلخ) علامة التصنيف: «محظور».

C4+: علامات الأمن القومي (خاص، سري، شديد السرية)2

أمثلة عملية

يمكن تصنيف أي موقع حكومي إلكتروني ينشر معلومات تحمل تصنيف «معلومات عامة» وفقاً للتصنيفات الأمنية التالية، أي سرية المعلومات = C0، إتاحة المعلومات = A1. ومع ذلك، نظراً لكونه موقع حكومي إلكتروني، تكون تصنيفات سلامة المعلومات مرتفعة، أي أن سلامة المعلومات =2I .

يسفر ذلك عن الوصول إلى تصنيف أمني عند المستوى M

يمكن تصنيف أي قاعدة بيانات حكومية تتضمن معلومات تحليلية إحصائية حول مواطنيها والمقيمين بها من خلال التصنيفات الأمنية التالية، أي أن سرية المعلومات = C2، وإتاحة المعلومات = A3، وسلامة المعلومات = I3

يسفر ذلك عن الوصول إلى مستوى أمني مرتفع H

كتيب تأمين المعلومات الوطنية

[IAP-NIA-INFA]

جدول المحتويات

أ- نظرة عامة

لا يعتبر أمن المعلومات قضية تقنية فحسب، بل إنه يمثل تحدياً للعمل والحوكمة. ينطوي على إدارة المخاطر وإعداد التقارير والمساءلة. ويعتبر أمن المعلومات عملية يتم إدارتها بدءاً من المستويات العليا وصولاً إلى المستويات الدنيا في المنظمة وتتطلب إستراتيجية شاملة لأمن المعلومات ترتبط بصورة واضحة بأنشطة وأهداف العمل بالمنظمة.

يتطلب الأمن الفعال مشاركة قوية من قبل الإدارة التنفيذية من أجل تقييم المخاطر وتوفير قيادة أمنية إلكترونية. ويتمثل المصطلح المستخدم لوصف مشاركة إدارة الأمن في مصطلح «حوكمة أمن المعلومات». تتضمن حوكمة أمن المعلومات مجموعة من السياسات والضوابط الداخلية التي يتم من خلالها توجيه وإدارة أنشطة أمن المعلومات داخل أي منظمة، بغض النظر عن حجمها أو شكلها. وتعد إدارة المخاطر وإعداد التقارير والمساءلة من الملامح الرئيسية لهذه السياسات والضوابط الداخلية. تعتبر حوكمة أمن المعلومات بمثابة مجموعة فرعية ضمن برنامج الحوكمة المؤسسية الشامل لأي منظمة.

ولكي يتسم الأمن بالفاعلية، لابد أن يتناول العمليات التنظيمية من البداية إلى النهاية – المادية والتشغيلية والتقنية. وينبغي أن يتم تنفيذ إستراتيجية رسمية لأمن المعلومات من خلال وضع سياسات شاملة لأمن المعلومات تتفق مع أهداف ومهمة المنظمة. ولتوفير حوكمة فعالة، لابد من صياغة معايير مؤسسية لكل سياسة من أجل وضع حدود معينة للعمليات والإجراءات المقبولة. ويجب وضع التعليم والتدريب والتوعية في الاعتبار أيضاً بهدف نقل المعلومات إلى جميع العاملين كجزء من برنامج مستمر لتغيير السلوكيات غير المؤدية إلى العمليات الآمنة ذات المصداقية.

ومن ثم، ينبغي تنفيذ الإستراتيجية من خلال برنامج شامل لأمن المعلومات يتضمن سياسات ومعايير مدروسة ومطلقة.

١ – المقدمة ونطاق العمل

يسري هذا الكتيب على جميع المؤسسات وأصولها المعلوماتية المقابلة. وحيثما تقوم المؤسسات بتعهيد أي عمليات أو أنشطة أو التعاقد مع أي مصادر خارجية من أجل تنفيذها من الباطن، لابد أن تكفل التزام تلك الجهات الخارجية بهذا الكتيب والضوابط المتعلقة به.

وبإيجاز، ينبغي أن يشمل برنامج أمن المعلومات عناصر مثل:

- تخصيص الأدوار والمسؤوليات.
- تخصيص ملكية الأصول المعلوماتية.
- تصنيف الأصول المعلوماتية.
- عمليات التقييم الدورية للمخاطر ونقاط الضعف.
- الضوابط الملائمة والفعالة والمدروسة.
- دمج الأمن في جميع العمليات التنظيمية.
- عمليات لرصد ومتابعة عناصر الأمن.
- عمليات فعالة لإدارة هوية ووصول مستخدمي وموردي المعلومات.
- توعية جميع المستخدمين والمديرين وأعضاء مجلس الإدارة بمتطلبات أمن المعلومات.
- التدريب على إدارة عمليات الأمن حسب الاقتضاء.
- وضع واختبار خطط لاستمرارية تصريف الأعمال في انقطاعه أو في حالات الكوارث.
- صيانة برنامج أمن المعلومات بصفة دائمة وتغيير عمليات الإدارة.

٢ – طريقة استعمال هذا الكتيب

يتم تصميم كتيب تأمين المعلومات الوطنية من أجل استخدامه مقترناً مع سياسة تصنيف المعلومات الوطنية [IAP-NAT-DCLS]. ويوفر هذا الكتيب الضوابط الرئيسية من أجل تغطية المجالات الأمنية التالية:

- أمن الرقابة على الوصول [AM]
- التدقيق و إصدار الشهادات [AC]
- إدارة تصريف الأعمال [BC]
- إدارة التغيير [CM]
- أمن الاتصالات [CS]
- أمن التشفير [CY]
- وضع البطاقات التعريفية للبيانات [DL]
- حفظ وأرشفة البيانات [DR]
- التوثيق [DC]
- أمن البوابة [GS]
- هيكل الحوكمة [IG]
- إدارة الحوادث [IM]
- تبادل المعلومات [IE]
- تسجيل الأداء والتدقيق والمتابعة الأمنية [SM]
- أمن الوسائط [MS]
- أمن الشبكات [NS]
- أمن العاملين [PS]
- الأمن المادي [PH]
- أمن الأجهزة المحمولة والعمل خارج الموقع [OS]
- أمن المنتجات [PR]

- إدارة المخاطر [RM]
- التوعية الأمنية [SA]
- أمن البرمجيات [SS]
- أمن استخدام النظام [SU]
- إدارة أمن الأطراف الأخرى [TM]
- المحاكاة [VL]

في إطار هذا الكتيب، تعد بيانات السياسة (التي تحمل عنوان: السياسة) والضوابط الرئيسية (تميز عبر علامة *) إلزامية وينبغي اتباعها وتنفيذها على التوالي. وتمثل هذه بنوداً قابلة للمراجعة والتدقيق سوف يتم السعي وراء تحقيق التوافق معها . يمكنم للمؤسسات ان تقوم بتطبيق ضوابط اضافية للضوابط الرئيسية. في حالة تعارض كتيب تأمين المعلومات الوطنية هذا مع قوانين أخرى، يجب على المؤسسة مراعاة تطبيق جميع النصوص او اتباع الساسة التي توفر فاعلية ثانية بصورة اكبر.

ينبغي إتباع الخطوات التالية من أجل استخدام هذا الكتيب:

أ. استخدام سياسة تصنيف المعلومات الوطنية [IAP-NAT-DCLS] لتصنيف جميع أصول المعلومات لدى المؤسسات . وتعتبر هذه الخطوة إلزامية قبل محاولة تطبيق السياسة والضوابط المحددة بهذه الوثيقة.

ب. لا تتطلب السمات الأمنية المخصصة للأصول I0 و A0 و C0 أي ضوابط رئيسية. وقد يتم تطبيق بعض الضوابط الصغرى.

ت. تتطلب السمات الأمنية المخصصة للأصول I1 أو A1 أو C1 أو السمات المذكورة أعلاه الالتزام بجميع بيانات السياسة الرئيسية ويتم الإشارة إليها بعلامة (*). تحظى جميع فصول الكتيب بتأثير على سلامة وإتاحة وسرية الأصول (إلى حد ما)؛ ومن ثم، ينبغي اختيار الضوابط الرئيسية الملائمة لكل من تلك الأصول.

ث. تتطلب السمات الأمنية المخصصة للأصول I2 أو A2 أو C2 ضوابط إضافية (واحدا أو أكثر) لكل نطاق معمول به اعتماداً على نتائج تقييم المخاطر ونقاط الضعف (انظر الفصل ب2-، إدارة المخاطر [RM] للتعرف على المزيد من التفاصيل). ويتعين إجراء عملية التقييم قبل اختيار هذه الضوابط الإضافية.

ج. تتطلب السمات الأمنية المخصصة للأصول I3 أو A3 أو C3 ضوابط إضافية متعددة (اثنان أو أكثر) لكل نطاق معمول به اعتماداً على نتائج تقييم المخاطر ونقاط الضعف (انظر الفصل ب2-، إدارة المخاطر [RM] للتعرف على المزيد من التفاصيل). ويتعين إجراء عملية التقييم قبل اختيار هذه الضوابط الإضافية.

ح. ينبغي أن يتم تنفيذ الضوابط المختارة على كل من الأصول. ويجب أن تعتمد أولوية التنفيذ على مستوى الأمن الكلي (منخفض، متوسط، مرتفع) (L,M,H)، حيث تحظى الأصول ذات المستوى المرتفع (H) بالأولوية القصوى للتنفيذ 3.

٣ – الملكية والمحافظة

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

٤ – المراجع

[IAP-NAT-DCLS] سياسة تصنيف المعلومات الوطنية، 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 رقم1، 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 لـIP، RFC 4301، ديسمبر 2005

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

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

[RSA] معامل «PKCS#1» ،RSA إصدار 2,1: مواصفات التشغير«RSA» ، يونيو 2002

[SFTP] جالبريث & سارينما، بروتوكول نقل الملفات draft-ietf-secsh-filexfer، SSH، 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 الدولية4408 RFC،(IETF)، أبريل 2006

يتم الإشارة إلى المصطلحات المعرفة بإطار تأمين المعلومات[IAP-NAT-IAFW] . ويتم استخدام المصطلحات المعرفة التالية ضمن هذه الوثيقة: المؤسسات، المعلومات الشخصية، المواقع الساخنة / الدافئة / الباردة، فريق الاستجابة لطوارئ الحاسبات بقطر (Q-CERT)، وزارة المواصلات و الاتصالات بقطر (MOTC)، علامات التصنيف القومي, خطة استمرارية تصريف الأعمال(Business Continuity Plan).

ب- حوكمة الأمن وعمليات الأمن

يستعرض هذا الفصل الضوابط الخاصة بكيفية إقرار حوكمة الأمن داخل للمؤسسة . وتبرز أيضاً بعض الأنشطة الرئيسية الواجب تنفيذها لضمان الحفاظ على الأمن وفقاً لهذا المعيار الرئيسي. وتتمثل الأنشطة التي يتم تغطيتها في إدارة المخاطر وإدارة أمن الأطراف الأخرى، ووضع البطاقات التعريفية للبيانات، وإدارة التغيير، وأمن العاملين، والتوعية الأمنية، وأمن الحوادث، وإدارة استمرارية تصريف الأعمال، وتسجيل الأداء والتدقيق ومتابعة الأمن، وحفظ وأرشفة البيانات، والمصادقة.

١- هيكل الحوكمة [IG]

١-١ أهداف السياسة

تتمثل أهداف هذه السياسة في تعريف هيكل حوكمة أمن المعلومات الخاص بالمؤسسات .

١-٢ السياسة والضوابط الرئيسية

للالتزام بهذه السياسة، يتعين على المؤسسات القيام بما يلي:

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..

IG 2 * تخصيص الموازنة الملائمة للعاملين وإدارة برنامج أمن المعلومات.

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

IG 4 * تعهد رؤساء المؤسسات كتابياً بتقديم الدعم الموثق من أجل تطوير وتنفيذ عمليات الأمن والبنية الأساسية لتكنولوجيا المعلومات والاتصالات وصيانتها بصفة دائمة داخل المؤسسة .

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.

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

IG 7 * ضمان أن يحظى مدير أمن المعلومات بما يلي:

- إمكانية الوصول إلى الإدارة التنفيذية والحصول على الدعم الكامل من قبلها.
- دراية كافية بأمن المعلومات و / أو أمن تكنولوجيا الاتصالات والمعلومات.
- 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.
- قدرة مناسبة لدعم دور مدير أمن المعلومات.

IG 8 إدراج المسؤوليات التالية ضمن دور مدير أمن المعلومات:

ا. 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.

د. ضمان التحقيق وتقديم التقارير حول جميع حوادث أمن تكنولوجيا الاتصالات والمعلومات، بالتعاون مع فريق الاستجابة لطوارئ الحاسبات بقطر.

IG 9 ضمان أن يتولى مدير أمن المعلومات المسؤولية عن:

ا. ضمان تطوير وحفظ وتحديث وتنفيذ خطط إدارة مخاطر الأمن وخطط أمن الأنظمة وأي إجراءات أمنية أخرى يتم تطبيقها.

تقديم المشورة الأمنية الفنية حول تطوير وحيازة وتنفيذ وتعديل وإدارة ودعم وبناء الأنظمة.

ب. مساعدة مدير النظام في وضع وصياغة معايير وسياسات أمن الأنظمة.

ج. اعتماد الأنظمة عند الاقتضاء.

د. ضمان أن ينظم الجهاز برنامج توعية وتدريب على أمن تكنولوجيا الاتصالات والمعلومات.

هـ. المراجعة المنتظمة لأمن الأنظمة وعمليات وسجلات تدقيق وسلامة إعدادات الأنظمة.

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.

٢- إدارة المخاطر [RM]

٢-١ أهداف السياسة

تحدد هذه السياسة شروط إجراء عملية تقييم المخاطر من أجل التعرف على الضوابط الملائمة لأصول المعلومات، التي تم تصنيفها باعتبارها

تحظى بمستوى أمن كلي متوسط أو مرتفع [IAP-NAT-DCLS] والحفاظ على المخاطر المتبقية إلى المستوى الأمثل اعتمادا على معدلات تقبل المخاطر المعتمده من قبل المؤسسة.

٢-٢ السياسة والضوابط الرئيسية

للالتزام بمتطلبات هذه السياسة، يتعين على المؤسسات القيام بما يلي:

RM 1	* تحديد إجراءات تنفيذ عملية تقييم مخاطر ونقاط ضعف الأصول المعلوماتية الهامة (التي تم تحديدها في مستوى أمني متوسط أو مرتفع).
RM 2	* بناءً على عملية التقييم يجب وضع خطة مجابهة المخاطر للتعامل مع المخاطر ونقاط الضعف .
RM 3	ضمان الفحص الدقيق لخطة مجابهة المخاطر والمخاطر المتبقية للأصول المعلوماتية المصنفة بمستوى أمني مرتفع، وإعتمادها من قبل الإدارة العليا للمؤسسه.
RM 4	ضمان المتابعة المنتظمة لفاعلية الضوابط المختارة بالفقرتين RM 1 و RM 2.
RM 5	يجب اجراء عملية تقييم المخاطر كل ستة شهور او عند حدوث تغييرات مؤثرة بوحدة العمل او تغييرات في بيئة العمل قد تدعو إلى الحاجة بإجراء عملية تقييم البيانات.

٣- إدارة أمن الأطراف الأخرى [TM]

٣-١ أهداف السياسة

الغرض من هذه السياسة هو ضمان الحفاظ على السياسة الرئيسية والضوابط المحددة بكتيب تأمين المعلومات الوطنية ضمن الخدمة (الخدمات) التي تم تعهيدها إلى أي طرف آخر.

٣-٢ السياسة والضوابط الرئيسية

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

TM 1	* أن تظل المجالات أو الخدمات التي تم تعهيدها تتمثل في مسؤولية المؤسسة عن الحوكمة والالتزام وإدارة المخاطر.
TM 2	* أن تتفهم وتقر المخاطر المتعلقة بتعهيد خدماتها.
TM 3	أن يتم إدراج الضوابط الأمنية والسياسة الرئيسية المحددة بكتيب تأمين المعلومات الوطنية ضمن اتفاقيات أو عقود تقديم الخدمة المبرمة مع أي طرف آخر. ويسري ذلك أيضاً على المتعاقدين من الباطن لدى الطرف الآخر.
TM 4	أن يتعهد الطرف الآخركتابياً بتقديم تقارير منتظمة حول الوضع الأمني للخدمة)الخدمات(الأمنية، بما في ذلك أي حوادث.
TM 5	أن يتم متابعة ومراجعة الخدمات والتقارير والسجلات التي يوفرها الطرف الآخر بصورة منتظمة، وأن يتم إجراء عمليات المراجعة والتدقيق بصورة منتظمة.

٤- وضع البطاقات التعريفية للبيانات [DL]

٤-١ أهداف السياسة

توفر هذه السياسة منهجية وضع بطاقات تعريفية للبيانات بجميع المؤسسات بغرض فهم وإدارة البيانات والأصول المعلوماتية فيما يتعلق بمستوى السرية. وتوضح هذه السياسة المنهجية والعمليات المتعلقة بوضع البطاقات التعريفية بصورة فعالة.

يتمثل الأساس المنطقي لتصنيف المعلومات إلى فئات حسب السرية في ضمان أن تتمكن المؤسسة والمستخدمون المحددون للأصول المعلوماتية من تحديد وتخصيص الموارد بصورة صحيحة وملائمة من أجل حماية سرية الأصول المعلوماتية.

٤-٢ السياسة والضوابط الرئيسية

رغم أن هذه الوثيقة توفر سياسة شاملة لتحقيق التصنيف المتسق للبيانات، قد يكون من المتوقع أن تتولى المؤسسة التوسع في هذه المفاهيم كي تلائم احتياجات علامات التصنيف القومي.

للالتزام بمتطلبات هذه السياسة، يتعين على المؤسسات القيام بما يلي:

DL 1	* أن تقوم بدور هيئة وضع البطاقات التعريفية للبيانات والمعلومات التي تجمعها أو تحتفظ بها.
DL 2	* أن تصنف جميع الأصول المعلوماتية وفقاً لسياسة تصنيف المعلومات الوطنية

[IAP-NAT-DCLS]. ويتم وضع علامة البيانات الملائمة "داخلي" أو "وصول محدود" أو "محظور" على التوالي على جميع الأصول المصنفة وفقاً لتصنيف السرية C1 أو C2 أو C3.

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

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.

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

٥- إدارة التغيير [CM]

٥-١ أهداف السياسة

الهدف من سياسة إدارة التغيير هو إدارة عمليات التغيير في نظم العمل بأسلوب رشيد يمكن التنبؤ به حتى يمكن التقليل من المخاطر الأمنية. ويتطلب التغيير الدراسة الجادة والرصد المتأني وتقييم المتابعة من أجل الحد من التأثير السلبي على مجتمع المستخدمين وزيادة قيمة الموارد المعلوماتية.

٥-٢ السياسة والضوابط الرئيسية

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

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

- 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

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

التغير 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

CM 2 تأسيس لجنة لإدارة التغيير.

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

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

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

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

٦- أمن العاملين [PS]

٦-١ أهداف السياسة

االهدف من هذه السياسة هو ضمان أن جميع الموظفين لدى المؤسسة والمتعاقدين لديها ملمين بمسؤلياتهم الامنية و تطبيق الاوامر بالشكل الامثل لتخفيف المخاطر الناتجة عن العمليات التي يتداخل فيها العنصر البشري.

٦-٢ السياسة والضوابط الرئيسية

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

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

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

PS 3 * تخزين وإدارة المعلومات ذات الصلة بالعاملين من خلال العناية الواجبة بما يتفق مع متطلبات التعامل مع المعلومات الشخصية وفقاً لما هو محدد بسياسة حماية البيانات والخصوصية المقترح.

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

PS 5 * إجراء الفحص الملائم للتأكد من نزاهة المرشحين المحتملين للتوظيف والمتعاقدين (بما في ذلك العاملين المتعاقدين من الباطن). ويمكن أن تتوسع المؤسسات في تطبيق هذه الممارسة لتشمل العاملين الحاليين وفقاً 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".

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

* التزامات السرية وعدم الإفصاح

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

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

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

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

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

- مسجلون وفقاً لبيانات تعريفية
- يحصلون على شارة الزوار
- يرتدون لافتة ملحوظة توضح وضعهم كزوار
- على دراية بالتزاماتهم المتعلقة بالامتثال لسياسات الأمن الخاصة بالمؤسسة
- يصاحبهم موظفو المؤسسة أثناء دخول المناطق الآمنة

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.

٧- التوعية الأمنية [SA]

٧-١ أهداف السياسة

الغرض من هذه السياسة هو تحديد المعايير الخاصة ببرنامج التدريب الأمني والتوعية، الذي تنظمه المؤسسة للعاملين والمتعاقدين والعمالة المؤقتة والهيئات الأخرى التي قد تستخدم أو تتولى إدارة أصول نظام المعلومات الخاصة بالمؤسسة .

٧-٢ السياسة والضوابط الرئيسية

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

SA 1 * تنظيم برنامج توعية أمنية وتخصيص الموازنات اللازمة لتنفيذه.

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.

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

SA 4 يجب تدريب الموظفين على تمييز طرق و محاولات الهندسة الاجتماعية أو ما يعرف بفن اختراق العقول و عدم كشف اي معلومات قد تعرض امن المؤسسة للمخاطر اثناء التدريبات او التجمعات الاجتماعية.

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

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

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

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

٨- إدارة الحوادث [IM]

٨-١ أهداف السياسة

الحادث المتعلق بأمن المعلومات هو حادث يؤثر على سرية أو سلامة أو توافر أي نظام أو شبكة معلومات من خلال إجراء يخالف سياسة الأمن المنصوص عليها. ولأغراض هذه السياسة، يتم تعريف الحادث بأنه انتهاك أو تهديد وشيك بانتهاك سياسات أمن الحاسب الآلي أو سياسات الاستخدام المقبولة أو الممارسات النموذجية للأمن.

تعتزم هذه السياسة توفير مرجع لإدارة المؤسسات والعاملين الفنيين والتشغيليين الآخرين من أجل تيسير عملية تخطيط التعامل مع حوادث أمن المعلومات واستخدامه في الاستعداد لمواجهة حوادث أمن المعلومات والكشف عنها والتصدي لها.

٨-٢ السياسة والضوابط الرئيسية

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

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

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

IM 3 * تحديد إجراءات الكشف عن الحوادث وتقييمها والتصدي لها.

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

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

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

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

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

IM 9 منسق إدارة الحوادث هو المسئول عن تطوير و تطبيق خطة تأمين البيانات السنوية. هذه المسئولية قد تتضمن اجراء بعض العمليات مثل إختبار الإختراق, مراجعة العمليات الامنية و إختبار محاكاة الحادثة.

٩- إدارة استمرارية تصريف الأعمال [BC]

٩-١ أهداف السياسة

تقوم هذه الوثيقة بتحديد معايير وضع وتنفيذ خطة شاملة لاستمرارية تصريف الأعمال تساعد في حالة توقف العمل على استمرارية العمليات

القائمة على تكنولوجيا المعلومات وتقديم الخدمات الضرورية بالمستوى المقبول.

٩-٢ السياسة والضوابط الرئيسية

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

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

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

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

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

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 افضل الممارسات يجب ان يبعد مركز البيانات الخارجي 22 كلم في منطقة مختلفة جغرافياً عن مركز البيانات الرئيسي.

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

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

BC 8 يتم اختبار خطة استمرارية تصريف الأعمال (Business Continuity Plan) بانتظام لمرة واحدة سنوياً على الأقل.

BC 9 * يتم توعية العاملين بخطة استمرارية تصريف الأعمال.

١٠- تسجيل الأداء والمتابعة الأمنية [SM]

١٠-١ أهداف السياسة

يتناول هذا الباب التعريف بسياسة تنفيذ المتابعة الدقيقة لنشاط تكنولوجيا المعلومات وسط مناخ عمل المؤسسة. وتهدف هذه السياسة إلى توفير متطلبات تسجيل الأداء والمتابعة من أجل تعقب البيانات والتطبيقات والتغييرات غير المصرح بها إضافة إلى تعقب الوصول إلى المصادر بدون تصريح وإساءة استخدام امتيازات الوصول للمصادر.

١٠-٢ السياسة والضوابط الرئيسية

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

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

SM 2 * إقرار ممارسات المتابعة وفقا لمدى أهمية البنية الأساسية. وينصح بتوفير متابعة لمدة 42 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]

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

SM 4 * تمكين الدخول على جميع البنية التحتة للامن والبنية التحتية الشبكية و أجهزة معالجة البيانات و التطبيقات التي تتيح الوصول غلى او تعالج أو تحمي المعلومات المصنفة وفقا لمستوى السرية C2 أو أكثر.

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

SM 6 أن تحظى السجلات التي تتضمن معلومات شخصية بالتدابير الملائمة لحماية الخصوصية وفقاً لسياسة حماية البيانات والخصوصية.

SM 7 * أن يتم الاحتفاظ بهذه السجلات لمدة تسعين يوما كحد أدنى, وكحد أقصى اعتمادا على القوانين واللوائح

الخاصة بالقطاع ومدى اهمية تلك السجلات.

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

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

١١- حفظ وأرشفة البيانات [DR]

١١-١ أهداف السياسة

الهدف من هذه السياسة هو توفير الحد الأدنى من المتطلبات الأمنية للمؤسسات لإقرار عمليات حفظ وأرشفة البيانات.

١١-٢ السياسة والضوابط الرئيسية

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

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

- سياسات واحتياجات المؤسسة
- المتطلبات الرقابية والتنظيمية
- المتطلبات القانونية

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

DR 3 ألا يتم الاحتفاظ بالمعلومات الشخصية لفترة أطول مما هو ضروري بمقتضى سياسة حماية البيانات والخصوصية.

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

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

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

١٢- التوثيق [DC]

١٢-١ أهداف السياسة

الهدف من هذه السياسة هو وضع الحد الأدنى لمجموعة الوثائق الأمنية التي يتعين على المؤسسات إصدارها، بالإضافة إلى كيفية حماية والحفاظ على هذه الوثائق.

١٢-٢ السياسة والضوابط الرئيسية

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

DC 1 * إصدار سياسة أمنية للمؤسسة تتضمن متطلبات كتيب تأمين المعلومات الوطنية هذا.

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

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

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

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

١٣- التدقيق وإصدار الشهادات [AC]

١٣-١ أهداف السياسة

الهدف من هذه السياسة هو ضمان وضع وإدارة برنامج ملائم للحوكمة وتحسين الأمن من قبل المؤسسة ، بما يتفق مع سياسة تصنيف المعلومات الوطنية [IAP-NAT-DCLS] وكتيب تأمين المعلومات الوطنية هذا.

١٣-٢ السياسة والضوابط الرئيسية

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

AC 1 * ضمان وضع برنامج للحوكمة وتحسين الأمن بما يتفق مع سياسة تصنيف المعلومات الوطنية-IAP]

[NAT-DCLSوكتيب تأمين المعلومات الوطنية هذا.

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

AC 3 * أن تخضع للمراجعة والتدقيق من قبل جهة المصادقة أو أي هيئة مستقلة تحددها وزارة المواصلات و الاتصالات.

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

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

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 الحصول على 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.

AC 7 * ضمان إصلاح أي تباينات خلال فترة زمنية محددة.

AC 8 * ضمان حصول المؤسسه على موافقة جهة المصادقة على أي إعفاء تود القيام به.

ج- الضوابط الأمنية

يغطي هذا الفصل من كتيب تأمين المعلومات الوطنية، بصفة رئيسية، مجالات الضوابط التقنية التي ينبغي أن تتولى المؤسسات تنفيذها كنقاط أمن رئيسية كي تتوافق مع كتيب تأمين المعلومات الوطنية هذا. وتتمثل المجالات التي يتم تغطيتها أمن الاتصالات وتبادل المعلومات وأمن المنفذ / البوابة وأمن المنتجات وأمن البرمجيات وأمن استخدام النظام وأمن الوسائط والرقابة على الوصول إلى المعلومات وأمن التشفير، و أمن الأجهزة المحمولة والعمل خارج الموقع و المحاكاة.

١- أمن الاتصالات [CS]

١-١ أهداف السياسة

الهدف من هذه السياسة هو ضمان أن تتخذ المؤسسات التدابير اللازمة التي تكفل أمن تدفق المعلومات والحد من نقاط ضعف الأمن المادي المتعلقة بتمديد الكابلات.

١-٢ السياسة والضوابط الرئيسية تمديد الكابلات

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

CS 1 أن يتم استخدام أنابيب (قنوات أو مواسير أو مجارى) 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.

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

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.

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

- رقم تعريف الكابل
- التصنيف
- المصدر
- المقصد
- الرسم التخطيطي للموقع

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

CS 6 ان تقوم المؤسسة توفير اكثر من مسار للإتصلات لضمان استمرار الاتصال.

١-٣ السياسة والضوابط الرئيسية الهواتف والفاكسات

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

CS 7 إخطار المستخدمين بالحد الأقصى لمستوى التصنيف المسموح به فيما يتعلق بالمحادثات باستخدام كل من خطوط الهاتف الداخلية والخارجية، وفقاً لما يحدده اختبار نظام الهاتف الداخلي ومستوى التشفير، إن وجد، بالخطوط الخارجية.

CS 8 * ضمان تعطيل خاصية مكبر الصوت خلال المحادثات الهاتفية المسموعة / المرئية، حيث من المحتمل أن يتم مناقشة المعلومات المصنفة عند المستوى C3 والاستماع إليها خلسة.

CS 9 * ضمان تعطيل خاصية تشغيل أجهزة المحادثات الجماعية عن بعد حيثما يتم تنصيبها في أحد المواقع الحساسة.

CS 10 * ضمان عزل الغرف المخصصة لتبادل المواد الحساسة بالصورة الملائمة من أجل منع تسرب الصوت.

CS 11 * ضمان تأمين أجهزة الفاكس لدى كلا الطرفين باستخدام أجهزة التشفير أثناء إرسال المعلومات المصنفة عند المستوى C2 أو أكثر.

CS 12 ضمان الوفاء بجميع معايير استخدام أجهزة الفاكس لدى كلا الطرفين عند مستوى التصنيف الواجب إرساله؛ ويجري المرسل الترتيبات للمستقبل كي:

- يجمع المعلومات من جهاز الفاكس بأسرع ما يمكن عقب استلامه.
- يخطر المرسل في حالة عدم وصول الفاكس خلال الفترة الزمنية المتفق عليها، على سبيل المثال: 10 دقائق.

٢- أمن الشبكات [NS]

٢-١ أهداف السياسة

تقر هذه السياسة أساس الاستخدام العام والاتصال بين شبكات تكنولوجيا المعلومات. فقد فتحت الشبكات الباب أمام المعالجة غير المحدودة من خلال المشاركة والاتصال بين الأجهزة واستحداث مفاهيم مثل التطبيقات الموزعة وأنظمة الشبكات...إلخ. ومع ذلك، فقد أدى استحداث الشبكات إلى مجموعة من المخاوف؛ ويحظى أمن العديد من الأنظمة وأمن شبكة الربط بذات الأهمية، وخاصة في حالة استخدام شبكات الوصول العام.

لابد من إجراء مقارنة بين مخاطر ومزايا الربط بالشبكات الخارجية. وقد يكون من المستحب أن يتم قصر الربط بالشبكات الخارجية على تلك الأجهزة المضيفة التي لا تقوم بتخزين مواد حساسة وتحتفظ بالأجهزة الهامة في معزل.

٢-٢ السياسة والضوابط الرئيسية إدارة الشبكات

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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 غيرمصرح لهم.

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]

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

- التصديق من خلال عملية رسمية لمراقبة التغيير وفقاً لما هو محدد بالفصل B-5 "إدارة التغيير" [CM] .
- التوثيق والالتزام بسياسة أمن الشبكات والخطة الأمنية وفقاً لما هو محدد بالفصل B-12 بعنوان "التوثيق" [DC].
- المراجعة المنتظمة. يتم الاحتفاظ بالإعدادات القديمة المتبعة وفقا لإجراءات المؤسسة كجزء من مراجعة التغيير. معدل تكرار المراجعة يعتمد على مخاطر و عمليات المؤسسة.

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

- رسم تخطيطي رفيع المستوى يوضح جميع توصيلات الشبكة.
- رسم تخطيطي للشبكة المنطقية يوضح جميع أجهزة الشبكة.
- عمليات تحديث NS4 (أ) و(ب)، مع حدوث تغييرات بالشبكة.
- وضع ملصق "حالي <بتاريخ>"على كل صفحة.

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. أجهزة تحويل بدلا من المحاور.

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 2 من بروتوكول الإنترنت.

هـ. التشفير على مستوى التطبيقات.

و. أداة آلية تقارن الإعدادات الحالية لأجهزة الشبكة بالإعدادات الموثقة

ز. توثيق حدود الشبكة

ح. تقييد و إدارة إتصال مستخدمي النظام بشبكة المؤسسة من خلال عدة تقنيات متوفرة, مثال تصفية عناوين (MAC address Filtering) MAC

ط. تفعيل انظمة منع الإختراق و انظمة كشف الإختراق بالشبكة.

ي. تقييد الدخول الى الشبكة عن طريق السماح فقط بأيام واوقات محدده

NS 6 * تتبنى شبكات الإدارة تدابير الحماية التالية:

• يتم استخدام الشبكة المخصصة لأجهزة الإدارة، أي تنفيذ شبكة محلية افتراضية مستقلة للإدارة أو بنية أساسية مادية مستقلة. VLAN

• قنوات آمنة، على سبيل المثال: عن طريق استخدام الشبكات الافتراضية الخاصة SSH.. الخ. VPNs و

٢-٣ السياسة والضوابط الرئيسية الشبكات المحلية الافتراضية

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

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

NS 8 * ألا يتم السماح بالوصول الإداري للمعلومات إلا من خلال الشبكة المحلية الافتراضية ذات التصنيف الأعلى إلى شبكة أخرى تحظى بنفس مستوى التصنيف أو تصنيف أقل.

NS 9 * تنفيذ جميع التدابير الأمنية التي تنصح بها عملية تقييم المخاطر في المؤسسة والإرشادات المتصلة الصادرة عن مورد جهاز التحويل.

NS 10 * ألا يتم استخدام مراكز تحويل البيانات أو تقنية نسخ المنافذ بأجهزة التحويل التي تدير الشبكات المحلية الافتراضية للتصنيفات المختلفة.

٢-٤ السياسة والضوابط الرئيسية الأجهزة متعددة الوظائف ()

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

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

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

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

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

• * يمكن أن تحدد البوابة المعلومات وتتولى تنقيتها وفقاً للمتطلبات الخاصة بتصدير البيانات.

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:

• مهام التحكم في تدفق المعلومات لمنع تدفق البيانات غير المتعمد وغير المصرح به.

• ضوابط تصدير البيانات القادرة على حصر المعلومات بناءً على تصنيف المعلومات.

• التوثيق وإصدار وحماية بيانات التدقيق.

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

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.

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

٢-٥ السياسة والضوابط الرئيسية خوادم أسماء النطاقات ()

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

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 جزءاً من الشبكة الحكومية مثل خادم أسماء النطاقات الرئيسي.

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

NS 20 * أن يتم توقيع ملفات المناطق رقمياً وتوفير توثيق التشفير المتبادل وسلامة بيانات التحويل بين المناطق والتحديثات الديناميكية.

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

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

NS 23 * مهام التشفير ذات الصلة ب NS20 و NS21 أعلاه، واستخدام وحدة أمن الأجهزة لكل من الإدارة الرئيسية والمعالجة التشفيرية وفقا لما هو محدد بالفصل C-10 ، بعنوان «أمن التشفير» [CY] .

٢-٦ السياسة والضوابط الرئيسية أمن شبكة الإنترنت

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

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

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:

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

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.

٢-٧ السياسة والضوابط الرئيسية أمن البريد الإلكتروني

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

NS 28 أن يتم دعم خوادم البريد الإلكتروني وفقاً 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 مجدياً من الناحيتين التقنية والتشغيلية، من أجل تجنب الإفصاح عن المعلومات الخاصة بالنظام إلى الأطراف الخارجية.

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

NS 30 * أن تقوم بتنفيذ إطار سياسة مرسل البريد الإلكتروني .[RFC4408] (SPF) 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.

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.

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.

٢-٨ السياسة والضوابط الرئيسية الأمن اللاسلكي

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

NS 34 * أن يتم إستخدام بروتوكولات الأمن اللاسلكية الأكثر قوة، مثل WPA2 وEAP-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.

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.

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

NS 38 إعدادات العميل لل 802.1x يجب ان تكون أمنة. بعض التقنيات المتاحة: التحقق من صحة شهادة الخادم من خلال تحديد شهادة المصادقة، تحديد عنوان الخادم ومنعه من دفع المستخدمين لقبول الثقة بشهادات أو خادمات جديدة.

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.

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 أيضاً النظر في تنقية عنوان MAC حسب الاقتضاء.

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.

NS 42 تفعيل انظمة منع و رصد إختراق الشبكات اللاسلكية ذات التصنيف C3 وما فوق لمراقبة التهديدات التي تنشأ من الاجهزة المتواجدة داخل نطاق الشبكة اللاسلكية و ليست لديها صلاحية الإتصال بالشبكة rogue Aps و هجمات الحرمان من الخدمة DOS attacks و غيرهما.

NS 43 إستخدام اكثر من معرف لمجموعة خدمات الشبكة اللاسلكية SSID بمكونات مختلفة لمختلف الشبكات المحلية الظاهرية VLANS وأساليب إثبات هوية العميل, إلخ. مثال: الموظفين و الضيوف يمكن ان يرتبطوا بشبكات لاسلكية مختلفة. الشبكة اللاسلكية للضيوق يكمن ان تحتوي على خصائص امنية أقل و تسمح فقط بالإتصال على شبكة الإنترنت.

٢-٩ السياسة والضوابط الرئيسية التزامن

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

NS 44 يجب تأمين خوادم بروتوكول وقت الشبكة NTP servers وفقا لأفضل الممارسات.

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. ونظراً لأن بعض الساعات تخالف التوقيت بمرور الوقت، فلابد من وجود إجراء يتولى فحص وتصحيح أي تباين في التوقيت.

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

NS 47 أن يتم تحقيق التزامن بين جميع الخوادم وأجهزة الشبكة مع خادم بروتوكول زمن الشبكة الرئيسي NTP المتزامن وفقاً لما هو محدد في NS43 وNS44.

٢-١٠ السياسة والضوابط الرئيسية الشبكات الافتراضية الخاصة (VPN)

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

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

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.

NS 51 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.

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.

٢-١١ السياسة والضوابط الرئيسية الأمن الصوتي لبروتوكول الإنترنت (□□□□)

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

NS 53 يعد الصوت والبيانات شبكتين منفصلتين. وينبغي أن يكون الفصل بينهما مادياً؛ 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.

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

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

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

NS 57 * أن يتم تنفيذ المتابعة الملائمة لسجل المكالمات.

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

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

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

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

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

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

٢-١٢ السياسة والضوابط الرئيسية الإصدار رقم ٦ لبروتوكول الإنترنت

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

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

NS 66 أن يتم المطالبة بإعادة المصادقة حيث تتولى المؤسسة نشر IPv6 داخل الشبكات الخاصة بها.

٣- تبادل المعلومات [IE]

٣-١ أهداف السياسة

الهدف من هذه السياسة هو توفير المتطلبات الأمنية الرئيسية حينما تقوم المؤسسة بتبادل المعلومات السرية مع الأجهزة الوطنية الأخرى أو مع الأطراف الأخرى.

٣-٢ السياسة والضوابط الرئيسية

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

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

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

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

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

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.

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

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

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

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

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

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 افضل من او مكافئ الى البروتوكول الآمن متعدد الأغراض للتوسع في البريد الإلكتروني وفقا لما هو محدد بالفقرة CY7 ، 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 .

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

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 وفقاً لما هو محدد في CY4، الفصل C-10 بعنوان "أمن التشفير" [CY].

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

٤– أمن البوابة [GS]

٤–١ أهداف السياسة

الهدف الرئيسي من هذه السياسة هو توفير الحد الأدنى لمتطلبات الأمن من أجل حماية البوابات المستخدمة في الاتصالات بين المؤسسات بالإضافة إلى الاتصالات بالروابط الخارجية.

يمكن استخدام عملية نشر البوابة الخاضعة للرقابة 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 الوكيلة.

٤-٢ السياسة والضوابط الرئيسية عام

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

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

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

- من خلال جهاز الشبكة الملائم للتحكم في تدفق البيانات.
- من خلال التحكم في تدفق البيانات بالصورة الملائمة.
- من خلال وضع مكونات البوابة بصورة مادية داخل غرفة الخادم المؤمنة بالصورة الملائمة.

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

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

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

GS 6 أن يتم استخدام منطقة 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.

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.

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

- البرمجيات الضارة ونقاط الضعف.
- الإعدادات الخاطئة أو السيئة.
- تسوية الحسابات وزيادة الامتيازات.
- متابعة الشبكات الضارة.
- رفض الاعتداءات على الخدمة.
- تسرب المعلومات / البيانات.

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 "تسجيل الأداء ومتابعة الأمن" [SM].

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

- * اللغة أو المرفقات البذيئة أو العدائية.
- المضمون المفعم بالبرامج الخبيثة.
- الاعتداءات على الخدمة.
- *فئات المواقع الإلكترونية / المضمون التي تعتبرها [IAP-NAT-CRIM] غير ملائمة، بما في ذلك المواقع الإلكترونية التي تستضيف المواد الإباحية ومواقع المقامرة...الخ.

٤-٣ السياسة والضوابط الرئيسية تصدير البيانات

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

GS 11 مستخدمو النظام:

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

GS 12 صادرات البيانات إما أن:

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

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

GS 14 * أن يتم فحص صادرات البيانات بما يكفل:

- البحث عن الكلمات الرئيسية في جميع البيانات النصية.
- حظر أي بيانات محددة لحين مراجعتها والموافقة على إصدارها من قبل أي مصدر موثوق بخلاف جهة إصدار البيانات.

٤-٤ السياسة والضوابط الرئيسية استيراد البيانات

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

GS 15 مستخدمو النظام:

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

GS 16 واردات البيانات إما أن:

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

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

٥- أمن المنتجات [PR]

٥-١ أهداف السياسة

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

٥-٢ السياسة والضوابط الرئيسية

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

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

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

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.

د. قدرة المورد على تطبيق و/أو الحفاظ على الاوامر التي حددها تقرير تقييم المخاطر.

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

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.

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

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

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

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

٦- أمن البرمجيات [SS]

٦-١ أهداف السياسة

الهدف من هذه السياسة هو تحديد أهمية تضمين الأمن داخل عملية تطوير وحيازة البرمجيات، بدلاً من إضافتها في صورة برنامج إضافي. وتتولى هذه السياسة تعريف الأمن باعتباره يسري على المراحل المتعددة لدورة حياة تطوير البرمجيات / النظام. وتغطي هذه السياسة أيضاً الضوابط الأمنية للتطبيقات التجارية المنتشرة داخل أي من المؤسسة .

٦-٢ السياسة والضوابط الرئيسية تطوير وحيازة البرمجيات

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

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.

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

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

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 وفقاً لسياسة محددة وموثقة، بحيث يحظى مستخدمو النظام فقط بإمكانية الوصول إلى المعلومات ويتم تعطيل إمكانية الوصول إلى المصدر الإداري للبرمجيات.

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.

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

- الالتزام بأفضل الممارسات، وعلى سبيل المثال أخطر 25 خطأ برمجي [Mitre].
- تصميم البرمجيات كي تستخدم أدنى مستويات التميز من أجل تحقيق مهمتها.
- رفض الوصول إلى المعلومات افتراضياً.
- فحص قيمة عائدات جميع مكالمات النظام.
- التحقق من سلامة جميع المدخلات.

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.

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

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

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

SS 11 أن يتم اعتماد التطبيقات قبل تنفيذها وفقاً لما محدد بالفصل B-13 بعنوان "الاعتماد" [AC].

٦-٣ السياسة والضوابط الرئيسية تطبيقات البرمجيات

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

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

SS 13 * أن تخضع محطات العمل لبيئة عمل قياسية مدعمة تغطي ما يلي:

- إلغاء البرمجيات غير اللازمة.
- تعطيل أسلوب العمل غير المستغل أو غير المستحب في البرمجيات وأنظمة التشغيل التي تم تركيبها.
- تطبيق ضوابط الوصول إلى المعلومات على البنود ذات الصلة لقصر إمكانية وصول مستخدمي النظام والبرامج على الحد الأدنى اللازم لأداء المهام والواجبات.
- تنصيب الجدران النارية القائمة على البرمجيات والتي تحد من الاتصالات الصادرة والواردة من وإلى الشبكة.
- تهيئة تسجيل الأداء عن بعد أو نقل سجلات الأداء المحلية إلى خادم مركزي.

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

- إلغاء عملية تبادل الملفات غير اللازمة.
- ضمان تحديث عملية تعديل البرمجيات.
- تعطيل إمكانية الوصول إلى أسلوب عمل المدخلات / المخرجات غير الضرورية.
- إلغاء الحسابات غير المستخدمة.
- إعادة تسمية الحسابات الافتراضية.
- استبدال كلمات المرور الافتراضية.

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:

- الفصل الوظيفي الفعال بين الخوادم بما يسمح لتلك الخوادم بأن نعمل بصورة مستقلة.
- الحد من الاتصالات بين الخوادم بكل من الشبكة ومستوى نظام الملفات، حسب الاقتضاء.
- قصر وصول مستخدمي النظام والبرامج على الحد الأدنى اللازم لأداء المهام والواجبات.

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 بدلاً من النظام ذاته.

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

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

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 .

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

SS 21 * أن تتم مراجعة جميع التطبيقات البرمجية لتحديد ما إذا كانت تحاول تأسيس أي وصلات خارجية. وفي حالة إدراج أسلوب العمل الآلي للوصلات الصادرة، يتعين على المؤسسات اتخاذ قرار عملي لتحديد ما إذا كان ينبغي السماح بهذه الوصلات أو رفضها، بما في ذلك تقييم المخاطر التي ينطوي عليها ذلك القرار.

٦-٤ السياسة والضوابط الرئيسية تطبيقات الويب

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

SS 23 أن يتم خفض الاتصال والوصول بين كل من مكونات تطبيقات الويب إلى الحد الأدنى.

SS 24 أن تتم حماية المعلومات الشخصية والبيانات الحساسة أثناء التخزين والنقل باستخدام ضوابط التشفير الملائمة.

SS 25 أن تستخدم المواقع الوطنية الإلكترونية التي ينبغي توثيقها شهادات SSH التي يوفرها مقدم خدمة الشهادات الذي يحظى بترخيص داخل دولة قطر.

SS 26 يجب إستخدام الجدار الناري لتطبيقات الويب للتطبيقات ذات معدل المخاطرة العالي او المتوسط.

٦-٥ السياسة والضوابط الرئيسية قواعد البيانات

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

SS 27 أن ترتبط جميع المعلومات التي يتم تخزينها داخل أي قاعدة بيانات بتصنيف ملائم إذا كانت تلك المعلومات:

- يمكن تصديرها إلى نظام مختلف أو
- تتضمن تصنيفات مختلفة و /أو متطلبات معالجة مختلفة.

SS 28 ينبغي أن تكفل المؤسسة تطبيق التصنيفات بمستوى من التفاصيل يكفي لتحديد متطلبات معالجة أي معلومات يتم استرجاعها أو تصديرها من أي قاعدة بيانات بوضوح.

SS 29 * أن يتم حماية ملفات قواعد البيانات من الوصول إليها بما يتجاوز ضوابط الوصول الطبيعية لقاعدة البيانات.

SS 30 أن توفر قواعد البيانات أسلوب العمل بما يسمح بتدقيق إجراءات مستخدمي النظام.

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 المؤسسات ضمان سلامة جميع نتائج البحث من أجل الوفاء بالحد الأدنى لمتطلبات الأمن لدى مستخدمي النظام.

SS 32 يجب استخدام تقنية قناع البيانات للبيانات الحساسة ذات التصنيف C3 أو اكثر.

٧- أمن استخدام النظام [SU]

٧-١ أهداف السياسة

تقر هذه السياسة الحاجة إلى أن تحدد المؤسسات بوضوح السلوكيات والإجراءات المسموح بها وغير المسموح بها داخل أنظمتها. وينبغي أن تكفل المؤسسة أن يحظى مستخدمو النظام بالتدريب على التوعية لضمان تفهمهم لالتزاماتهم.

٧-٢ السياسة والضوابط الرئيسية

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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 .

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.

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.

SU 4 أن يتم توفير إمكانية الوصول إلى الويب من خلال الخوادم الوكيلة وبوابات التنقية وفقا لما هو محدد بالفصل C-4 بعنوان "أمن البوابة" [GS].

SU 5 * أن يكون العاملون على دراية بأنماط المضمون المصرح به والمحظور داخل المؤسسة وفقاً لما هو محدد بالفصل B-4 بعنوان "أمن البوابة" [GS]. وينبغي أن تنظر المؤسسة في إيجاد حل فعال لمتابعة مضمون القنوات المشفرة.

SU 6 أن يقوم العاملون باستخدام البريد الإلكتروني بهمة ونشاط وإدراج علامات التصنيف اللازمة اعتماداً على المضمون / المرفقات وفقاً لسياسة تصنيف المعلومات الوطنية [IAP-NAT-DCLS].

SU 7 أن يتم اتخاذ التدابير الملائمة لحماية البريد الإلكتروني من المخاطر المحتملة كالفيروسات وفيروس طروادة والرسائل التطفلية والتزوير والهندسة الاجتماعية (Social Engineering) .

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 .

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.

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 .

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].

٨- أمن الوسائط [MS]

٨-١ أهداف السياسة

الهدف من هذه السياسة هو مساعدة المؤسسات على تعريف كيفية تصنيف الوسائط ووسمها وتسجيلها من أجل تقديم العون في تحديدها وتفسيرها بالصورة الملائمة. وتدرس السياسة دورة الحياة الكاملة للوسائط بدءاً بالاستخدام والإصلاح والتطهير والتدمير إلى التخلص منها.

٨-٢ السياسة والضوابط الرئيسية تصنيف ووسم الوسائط

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

MS 2 أن يتم تصنيف الوسائط غير المعرضة للتأثر وفقاً لأعلى مستوى تصنيف تحظى به المعلومات المختزنة بها.

MS 3 * أن يتم تصنيف الوسائط سريعة التأثر التي تشتمل 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.

MS 4 أن يتم إعادة تصنيف وسائط التخزين إذا:

- كانت المعلومات المنقولة إلى تلك الوسائط تحظى بمستوى تصنيف مرتفع.
- كانت المعلومات التي تتضمنها تلك الوسائط تخضع لإمكانية تطوير مستوى التصنيف.

MS 5 يمكن إلغاء تصنيف الوسائط التي تحمل معلومات مصنفة عقب:

- إلغاء تصنيف المعلومات المختزنة على الوسائط من قبل المنشئ
- تطهير الوسائط وفقاً للفصل رقم C-8-3 بعنوان "السياسة والضوابط الرئيسية – تطهير الوسائط".

MS 6 في حالة عدم إمكانية تطهير وسائط التخزين، لا يمكن إلغاء تصنيفها ويتعين تدميرها.

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 وفقاً لما هو محدد بالفصل رقم B-4، بعنوان "وسم البيانات" [DL] .

MS 8 يمكن التعرف على تصنيف جميع الوسائط بوضوح. وعند استخدام الضمانات غير النصية لعلامات التصنيف نتيجة لأمن التشغيل، يتعين على المؤسسات توثيق خطة التوسيم وتدريب أعضاء فريق العمل بالصورة الملائمة.

٨-٣ السياسة والضوابط الرئيسية تطهير الوسائط

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

MS 9 * أن تتولى توثيق الإجراءات الخاصة بتطهير الوسائط، التي يتم اختبارها بانتظام

MS 10 أن يتم تدمير جميع أنماط الوسائط التالية التي تتضمن معلومات مصنفة عن المستوى C1 أو أكثر قبل التخلص منها، امثلة لذلك:

- الميكروفيش والميكروفيلم.
- الأقراص الضوئية.
- شرائط الطابعات وسطح التأثير المواجه للاسطوانة.
- الذاكرة القراءة فقط القابلة للبرمجة.
- ذاكرة القراءة فقط.
- الوسائط الخاطئة التي لا يمكن تطهيرها بنجاح.

MS 11 أن يتم تطهير الوسائط سريعة التأثر عن طريق:

- فصل الطاقة عن الوسائط لمدة 10 دقائق على الأقل أو
- إحلال جميع مواقع الوسائط من خلال نمط عشوائي يليه إعادة قراءة الوسائط للتحقق من عملية الإحلال.

MS 12 * أن يتم تطهير الوسائط المغناطيسية غير المعرضة للتأثر عن طريق:

أ. إحلال الوسائط بالكامل، إذا ما كانت صادرة قبل عام 2002 أو كانت أقل من 22 جيجابايت بأسلوب عشوائي يليه إعادة قراءة الوسائط للتحقق من عملية الإحلال لثلاثة مرات.

ب. إحلال الوسائط بالكامل، إذا ما كانت صادرة بعد عام 2002 أو كانت أكبر من 22 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 المغنطيسية قد تجعل بعض الوسائط الحديثة غير صالحة للإستعمال).

MS 13 أن يتم تطهير وسائط EPROM ذات ذاكرة القراءة القابلة للبرمجة والمسح عن طريق المسح وفقاً 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.

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.

٨-٤ السياسة والضوابط الرئيسية إصلاح وصيانة الوسائط

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

MS 15 * أن يقوم العاملون المطلعون الخاضعون للفحص الملائم بتنفيذ عمليات إصلاح وصيانة الأجهزة التي تتضمن معلومات مصنفة.

MS 16 أن يتم إجراء عمليات إصلاح الأنظمة التي تشتمل على معلومات مصنفة عند المستوى C3 أو أكثر في ظل الإشراف.

٨-٥ السياسة والضوابط الرئيسية تدمير الوسائط والتخلص منها

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

MS 17 أن تتولى توثيق الإجراءات الخاصة بتدمير الوسائط والتخلص منها

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.

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.

MS 20 أن يتم تطهير الوسائط لأقصى درجة ممكنة، بما في ذلك الوسائط الخاطئة، التي تشتمل على معلومات مصنفة قبل التخلص منها.

MS 21 * ألا تجتذب عملية التخلص من الوسائط ومخلفات الوسائط اهتماما غير مستحق.

٩- أمن الرقابة على الوصول [AM]

٩-١ أهداف السياسة

الهدف من هذه السياسة هو إقرار استخدام ونشر مجموعة متنوعة من حلول الرقابة على الوصول إلى المعلومات لضمان سرية وسلامة وإتاحة الأصول المعلوماتية للمؤسسة . وتحدد هذه السياسة القواعد اللازمة لتحقيق هذه الحماية وضمان إدارة أنظمة معلومات الأجهزة الوطنية بصورة آمنة وفعالة.

٩-٢ السياسة والضوابط الرئيسية عام

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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".

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.

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.

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.

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.

AM 6 * أن يتم اعتبار أي محاولة غير مفوضة للتحايل على رقابة الوصول إلى معلومات المؤسسة بمثابة حادث أمني ويتم التعامل معه وفقاً للإجراءات المقررة للتعامل عن الحوادث و /أو سياسات وإجراءات الموارد البشرية الملائمة.

AM 7 أن يتم تفعيل والحفاظ على سجلات التدقيق بأسلوب يسمح بمتابعة الالتزام بالسياسة الوطنية ويساعد

في إدارة الحوادث.

AM 8 * أن يخضع الوصول المنطقي لشبكات المؤسسة للرقابة التقنية. وقد يكون ذلك باستخدام خدمات / أجهزة الرقابة على الوصول إلى الشبكات.

AM 9 * أن يتم الحفاظ على سجلات آمنة لما يلي:

- جميع مستخدمي النظام المفوضين.
- هوية المستخدم الخاصة بهم.
- الأشخاص الذين منحوهم الموافقة على الوصول إلى النظام.
- موعد منح الموافقة والتفويض.
- الحفاظ على السجل على مدار فترة تواجد النظام الذي تم منح إمكانية الوصول إليه.

AM 10 * أن يتم عرض شعار تسجيل الدخول قبل منح إمكانية الوصول إلى النظام. وينبغي أن تشمل هذه الشعارات ما يلي:

- السماح لمستخدمي النظام المفوضين فقط بالوصول إلى النظام.
- موافقة مستخدم النظام على الالتزام بسياسات الأمن ذات الصلة.
- دراية مستخدم النظام بإمكانية متابعة استخدام النظام.
- تعريف الاستخدام المقبول للنظام.
- التبعات القانونية لانتهاك السياسات ذات الصلة.
- طلب استجابة مستخدم النظام، متى أمكن، على سبيل الإقرار.

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:

- تحديث المعلومات / الوصول إلى المعلومات دون تفويض.
- تاريخ البدء والانتهاء وزمن النشاط بالإضافة إلى محدد النظام.
- هوية المستخدم (لتسجيل الدخول غير القانوني).
- نشاط تسجيل الدخول والخروج (لتسجيل الدخول غير القانوني).
- الجلسة / المحطة الطرفية أو الاتصال عن بعد.

٩-٣ السياسة والضوابط الرئيسية تحديد الهوية والتوثيق

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

AM 12 أن تضع وتحتفظ بمجموعة من السياسات والخطط والإجراءات المشتقة من سياسة التصنيف الوطنية [IAP-NAT-DCLS]تشمل مستخدمي النظام فيما يتعلق بما يلي:

- تحديد الهوية.
- التوثيق.
- التفويض.

AM 13 أن تتولى توعية مستخدمي النظام لديها بسياسات وإجراءات المؤسسة .

AM 14 جميع مستخدمي النظام:

- يمكن تحديد هويتهم بصورة فريدة.
- يتم توثيقهم في كل مناسبة يتم خلالها منح إمكانية الوصول إلى النظام.

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.

AM 16 * أن تكون هناك وسائل بديلة لتحديد هوية مستخدم النظام عند استخدام حسابات مشتركة / غير محددة.

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.

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.

AM 19 * سياسة كلمة المرور التي تفرض حد أدنى لكلمة المرور يصل إلى 12 رمز بدون أي شروط معقدة أو حد أدنى يصل إلى سبعة رموز تتألف من ثلاثة على الأقل من مجموعات الرموز التالية:

- حروف صغيرة (a-z).
- حروف كبيرة (A-Z).
- أرقام(0-9) .
- علامات الترقيم والرموز الخاصة.

AM 20 * أن يتم تغيير كلمات المرور مرة واحدة على الأقل كل 90 يوماً.

AM 21 * ألا يستطيع مستخدمو النظام تغيير كلمة المرور لأكثر من مرة يومياً ويجبر النظام المستخدم على تغيير كلمة المرور المنتهية الصلاحية عند تسجيل الدخول المبدئي أو عند إعادة التشغيل.

AM 22 * أن يتم فحص كلمات المرور المختارة لمنع ما يلي:

- كلمات المرور التي يمكن التنبؤ بها عند إعادة التشغيل.
- إعادة استخدام كلمات المرور عند إعادفقة تشغيل الحسابات المتعددة.
- كلمات المرور التي يتم إعادة استخدامها بعد إجراء ثمانية تغييرات لها.
- استخدام المستخدمين لكلمات المرور التسلسلية أو المتعاقبة.

AM 23 * ضبط إعدادات قفل الشاشة / الجلسة على:

- التشغيل بعد 15 دقيقة كحد أقصى من توقف مستخدم النظام عن العمل.
- التشغيل يدوياً من قبل مستخدم النظام عند الرغبة في ذلك.
- الإقفال لإخفاء جميع المعلومات الظاهرة على الشاشة تماما.
- ضمان عدم ظهور الشاشة كما لو كانت مغلقة في حالة الإقفال.
- قيام مستخدم النظام بإعادة التوثيق من أجل فتح النظام.
- عدم السماح لمستخدم النظام بتعطيل آلية الإقفال.

AM 24 * أن يتم تعليق الوصول إلى النظام بعد عدد محدد من محاولات تسجيل الدخول أو بمجرد عدم حاجة أي من أعضاء فريق العمل إلى الدخول على النظام نتيجة لتغيير الأدوار أو ترك العمل بالمؤسسة .

AM 25 * كلمات المرور المفقودة أو المسروقة أو المعرضة لخطر الكشف عنها:

- يتم إبلاغ مدير أمن المعلومات عنها كي يكفل تعليق العمل بالحساب الخاص بها.
- يتم تغييرها بمجرد التحقق من هوية المستخدم.

AM 26 * أن يتم تعليق العمل بالحسابات التي تكون غير عاملة لمدة تتجاوز ثلاثة (3) شهور.

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 العملة كل ستة (6) شهور.

٩-٤ السياسة والضوابط الرئيسية الوصول إلى النظام

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

AM 28 أن تتولى سياسات الأمن توثيق شروط الوصول إلى النظام والتراخيص الأمنية والتعليمات اللازمة من أجل الوصول إلى النظام.

AM 29 * أن يتم فحص مستخدمي النظام وفقاً لما هو محدد بالفصل B-6 بعنوان "الأمن الشخصي" [PS] قبل منح أي منهم تصريح بالدخول على النظام.

AM 30 * أن يتلقى مستخدمو النظام أي تعليمات لازمة قبل منح أي منهم تصريح بالدخول على النظام.

٩-٥ السياسة والضوابط الرئيسية الوصول المتميز إلى النظام

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

AM 32 أن يتم إسناد حساب فردي إلى مديري النظام من أجل الاضطلاع بمهامهم الإدارية.

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 لإستثناء هذه السياسة.

AM 34 * أن يتم تحديث سجل إدارة النظام من أجل تدوين المعلومات التالية:

- أنشطة التطهير.
- بدء تشغيل النظام وإغلاقه.
- إخفاق المكونات أو الأنظمة.
- أنشطة الصيانة.
- أنشطة الدعم والأرشفة.
- أنشطة استعادة قدرة النظام على العمل.
- الأنشطة الخاصة أو الأنشطة خارج ساعات العمل.

٩-٦ السياسة والضوابط الرئيسية الوصول إلى النظام عن بعد

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

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.

AM 37 * أن يتم تأمين جلسات الدخول عن بعد باستخدام التشفير الملائم من البداية إلى النهاية وفقاً لما هو محدد بالفصل C-10 بعنوان "أمن التشفير" [CY].

AM 38 أن يتم تزويد أجهزة الحاسوب المتصلة بالنظام عن بعد بجدار ناري شخصي وبرنامج لمكافحة الفيروسات الخبيثة على الأقل. ويتم تفعيل هذه الضوابط الأمنية في جميع الأوقات.

AM 39 أن يتم إصلاح البرمجيات، بما في ذلك برامج الأمن المنصبة على أجهزة الحاسوب، وتحديثها بصفة دائمة.

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.

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.

١٠- أمن التشفير [CY]

١٠-١ أهداف السياسة

تقر هذه السياسة أسس استخدام تكنولوجيات التشفير من أجل الحفاظ على سرية و /أو سلامة الأصول المعلوماتية. ويتعين على المؤسسة ، باعتبارها أميناً على المعلومات العامة والسرية، حماية البيانات / المعلومات الخاصة والحساسة أيضاً من جميع المخاطر ونقاط الضعف الداخلية والخارجية التي تتهدد المؤسسة .

١٠-٢ السياسة والضوابط الرئيسية

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

CY 1 أن يفي لوغاريتم التشفير وأجهزة / برامج التشفير وأنظمة الإدارة الرئيسية والتوقيعات الرقمية بالمتطلبات المحددة بالملحق B من هذا الكتيب حول لوغاريتم وأنظمة التشفير.

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.

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.

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.

CY 5 * أن يتم استخدام البروتوكولات التالية ذات اللوغاريتم المعتمد المحدد بالملحق "ب" لتأمين البيانات المصنفة عند المستوى C3 أثناء عملية النقل:

- لتأمين حركة مرور البيانات عبر الويب : TLS (128 + bits) [RFC4346]
- لتأمين نقل الملفات: SFTP [SFTP]
- لتأمين الوصول إلى المعلومات عن بعد: IPSEC [RFC 4301] وأ SSH v2 [RFC4253]
- يجب إستخدام بروتوكول التوقيع و تشفير الرسائل: S\MIME vs [RFC3851] أو أفضل، انظر CY11 لمعرفة المتطلبات المرتبطة

CY 6 * أن يتم تشفير / تجزئة وحماية كلمات المرور بصفة دائمة من الإفصاح عنها دون موافقة أثناء تخزينها و /أو نقلها بغض النظر عن أسلوب أو وسائط التخزين. ويتم تشفير كلمات المرور المتميزة وتخزينها بعيداً عن الموقع إلى جانب ملفات الدعم كلما تم تغيير كلمة المرور لضمان إمكانية استعادتها بالكامل.

CY 7 * أن يتم توثيق وحدات أمن الأجهزة، حيثما يتم استخدامها، وفقاً للمستوى رقم 2 من مستويات المعهد القومي للمعايير والتكنولوجيا [FIPS 140-2] FIPS 140-2 أو للمعايير العامةEAL4 [CC3-1].

CY8 أن يتم نقل مفاتيح التشفير بصورة مادية فقط في HSMs.

CY 9 أن يتم تحديد عمليات إدارة المفاتيح وفقاً لـ [ISO11770-1] واستخدامها في إدارة دورة حياة مفاتيح التشفير، بما يشمل المهام التالية:

- أدوار ومسؤوليات 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.

CY 10 على المؤسسات القيام بضمان توافق الشهادات الرقمية مع المعايير المحددة من قبل إدارة البنية التحتية للمفاتيح العامة و مقدمي خدمة الشهادات CSP-PMA بوزارة المواصلات و الاتصالات. ويجب على المؤسسات ضمان استخدام أنظمة إبطال الشهادات الرقمية على الانترنت لتقليل مخاطر الاحتيال في استخدام الشهادات الرقمية

CY 11 أن تفي أنظمة مقدمي خدمات الشهادات المعتمدة التي توفر البطاقات الأمنية الذكية بالمتطلبات الخاصة بخدمات توفير الأجهزة وفقاً لما هو محدد في [CWA14167-1].

CY 12 * أن يتم إصدار أي شهادات رقمية مستخدمة بنظام الإنتاج من قبل مقدمي خدمة الشهادات المعتمدين بدولة قطر.

١١- أمن الأجهزة المحمولة والعمل خارج الموقع [OS]

١١-١ أهداف السياسة

الهدف الرئيسي من هذه السياسة هو وضع الحد الأدنى لمتطلبات الأجهزة المحمولة [أجهزة الهاتف المحمول والحاسوب المحمول] عند استخدامها داخل المؤسسة أو في أي أماكن أخرى غير خاضعة للرقابة.

١١-٢ السياسة والضوابط الرئيسية عام

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.

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.
OS 3	ألا يتم تفعيل منافذ أجهزة الهواتف المحمولة والحاسوب المحمول ذات وصلات منافذ البلوتوث التسلسلية إذا كان الجهاز يحمل معلومات مصنفة.
OS 4	ألا يتم السماح بدخول الهواتف المحمولة المزودة بأجهزة تسجيل إلى المناطق ذات الخطورة العاليةدون موافقة مسبقة من قبل مدير أمن المعلومات.
OS 5	* يجب أن تقوم جميع أجهزة الهواتف المحمولة والحاسوب المحمول بتشفير المعلومات التي تحملها ، و حمايتها بكلمة مرور.
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.
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 شبكات المؤسسة ، بشرط استخدام جدار ناري مناسب لحماية الجهاز من أي مخاطر محتملة تنشأ عن الشبكة غير الخاضعة لرقابة 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.
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].
OS 10	*أن يكون هناك خطة للإتلاف/ الإغلاق / المسح عن بعد / التدمير التلقائي في حالات الطوارئ فيما يتعلق بجميع أجهزة الهواتف والحواسيب المحمولة.

١٢– الأمن المادي [PH]

١٢–١ أهداف السياسة

الهدف من هذه السياسة هو ضمان منع الوصول المادي غير المصرح أو إلحاق الخسائر المادية بمقار ومعلومات المؤسسة . وينبغي على للمؤسسة أن تكفل تبني تدابير وضوابط الأمن المادي من أجل الوفاء بالمتطلبات الرئيسية لهذه السياسة.

١٢–٢ السياسة والضوابط الرئيسية

للوفاء بمتطلبات هذه السياسة، يتعين على المؤسسات 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.
PH 2	أن يتم تقسيم الأماكن المادية اعتماداً 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: CoIoAo). 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».

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 تضيف المؤسسة ضوابط إضافية إلى جانب تلك الضوابط التي تقرها هذه السياسة.

PH 4 تنفيذ سياسة "المكتب النظيف" و"الشاشة النظيفة".

PH 5 أن تفي غرف الخوادم / البيانات بمتطلبات الحماية المتوسطة.

PH 6 * أن تكون الكابلات التي تحمل المعلومات المصنفة عند المستويات C1-C3 منفصلة مادياً (بما في ذلك كابلات الألياف الضوئية) وأن تمر في أنابيب منفصلة عن الكابلات التي تحمل المعلومات المصنفة على المستوى القومي القومي(C4).

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:

- ملخص لعملية تقييم مخاطر الأمن الوقائي.
- أدوار ومسؤوليات مسؤول وأعضاء فريق عمل المرفق أو مسؤول وأعضاء فريق عمل أمن تكنولوجيا الاتصالات والمعلومات.
- إدارة وتشغيل وصيانة نظام مراقبة الوصول الإلكتروني إلى المعلومات و /أو نظام الإنذار الأمني.
- الإدارة الرئيسية وانضمام وإلغاء مستخدمي النظام وإصدار الهوية الشخصية.
- تراخيص أعضاء فريق العمل وتدريب التوعية الأمنية وإصدار التعليمات المنتظمة.
- فحص عمليات المراجعة والتدقيق والسجلات الصادرة.
- عمليات الفحص والمتابعة في نهاية اليوم.
- الإبلاغ عن حوادث وخرق أمن تكنولوجيا الاتصالات والمعلومات.

– ألمحاكاة [VL]

١٣–١ أهداف السياسة

الهدف من هذه السياسة هو توفير ضوابط لتأمين البيئة التقنية الإفتراضية للمؤسسة. يتعين على المؤسسات ان تتأكد بأن تلك البيئات الإفتراضية مومنة على نحو كافٍ.

في حالة أن البيئة الإفتراضية خدمة مقدمة من طرف ثالث خارج المؤسسة، على المؤسسة ان تستعين بسياسة تأمين الحوسبة السحابية (مقترح).

١٣–٢ السياسة والضوابط الرئيسية عام

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

VL1 * تقييم المخاطرة المتعلقة بالتكنولوجيا الافتراضية

- تقييم المخاطر في سياق السياسات القانونية والتنظيمية والتشريعات ذات الصلة
- تقييم تأثير إدخال التكنولوجيا الإفتراضية على بنيتك المعلوماتية التحتية الموجودة و الموقف الامني المرتبط.

VL2 * 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.

VL3 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 الإداري المباشر إلى طبقة إدارة الانظمة الإفتراضية 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 السر على إثنين او اكثر من المسئولين.

VL4 * ضمان الأمن المادي النافي لمنع الوصول غي الما ح قه إلى البيئة التطنية الافت اضية

VL5 بيئة تكنولوجيا الافتراضية يجب ان تعدل بحيث يضاف إليها طرق امنية أخري لتوفير التحكم الامن على طبقات (نهج الدفاع من العمق) لاستكمال الضوابط المقدمة من الموردين والتكنولوجيا.

VL6 فصل الأجهزة الإفتراضية بناء على تصنيف البيانات التي يتم معالجتها و / أو مواقع تخزينها.

VL7 * 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 الأوقات.

• ينبغي الحرص على صيانة وتحديث للاجهزة الافتراضية التي ليست في حالة نشطة (نائمة أو لم تعد تستخدم).

VL8 * 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).

الملحق أ (قياسي) الضوابط المادية

مستوى الحماية		
الضوابط المتوسطة والمرتفعة	الحماية الأولية (إلزامي بالكامل)	
• جميع الضوابط الأساسية أو الأولية. • بناء جدران متماسكة لفصل المناطق؛ مصنوعة من المعدن أو الخشب المصمت، بسمك لا يقل عن ٤٤,٤٥ مم. • أدلة مرئية للاختراق غير المصرح به. • بناء جدران من الأرضية إلى الأسقف. • حماية خارجية للنوافذ. • تنصيب نظام الكشف عن الدخلاء لتغطية جميع الأبواب الخارجية والنوافذ التي يمكن الوصول إليها.	• جميع الضوابط الدنيا • جدران سليمة من الناحية المادية دون وجود فجوات في المحيط الخاص بها. • منطقة استقبال مزودة بأفراد أمن أو وسائل أخرى للرقابة على الدخول. • فصل مرافق معالجة المعلومات عن تلك المرافق الخاضعة لإدارة أي طرف آخر.	
• جميع الضوابط الأساسية أو الأولية. • الأقفال الإلكترونية على مداخل المناطق (رمز أو إشارة ورقم تعريف PIN والسمات البيولوجية) . • سجلات المراجعة والتدقيق (التاريخ والتوقيت) لجميع نقاط الوصول (بما في ذلك الوصول إلى الخزانات وغير ذلك) . • ينبغي أن يتم تجهيز المدخل الرئيسي والأبواب الداخلية الخاضعة للرقابة بجهاز إغلاق تلقائي. • أجهزة الكشف عن المعادن. • الفحص بأشعة إكس X-Ray. • حواجز إضافية خاضعة للرقابة المادية. • حواجز لمنع الدخول إذا كانت فتحات الأنابيب وفتحات التهوية والمواسير وغيرها أكبر من ٦١٩ سم مربع . • استخدام الخزائن/ القباء.	• جميع الضوابط الدنيا. • الأقفال الإلكترونية على مداخل المناطق (بطاقة/ رمز فقط). • سجلات المراجعة والتدقيق (التاريخ والتوقيت) لنقاط الوصول فقط. • الأبواب المحيطة المقاومة للاقتحام. • الإشراف على جميع الزوار، الدخول لغرض محدد. • تعريف مرئي واضح لجميع العاملين والمتعاقدين والأطراف الأخرى بما في ذلك الزوار. • منح الأطراف الأخرى/ المتعاقدين إمكانية الدخول المقيد لتأمين المناطق أو مرافق المعالجة الحساسة. • أقفال تقاوم سهولة اقتحام الأماكن.	
• جميع الضوابط ا الأساسية أو الأولية. • ينبغي أن تكون النوافذ التي تساعد على الرقابة البصرية غير شفافة أو مزودة بستائر. • ينبغي ألا يسهل اقتحام المرافق من قبل الجمهور.	• جميع الضوابط الدنيا. • ينبغي تحديد موقع المرافق لتجنب الوصول إليها. • ينبغي ألا تحمل المباني لافتات واضحة توضح الغرض منها أو تبين وجود مرافق لمعالجة المعلومات بها. • سياسة المكاتب النظيفة.	
• جميع الضوابط الأساسية أو الأولية. • يبلغ تصنيف فئة انتقال الصوت ٤٥ أو أكثر بين المناطق.	• جميع الضوابط الدنيا. • وضع الأجهزة وبيانات الدعم خارج المناطق. • تخزين المواد الخطرة أو القابلة للاحتراق على بعد آمن من المناطق.	
• جميع الضوابط الأساسية أو الأولية. • إغلاق المناطق الآمنة الخالية وفحصها بصفة دورية. • حظر دخول أجهزة ومعدات التصوير والفيديو والأجهزة السمعية أو أجهزة التسجيل الأخرى، ما لم يتم الموافقة على ذلك بصورة صريحة. • الإشارة المرئية إلى تواجد الزوار في أي منطقة آمنة.	• ينبغي أن يتم تجنب العمل غير الخاضع للإشراف.	

	الحماية الدنيا (إلزامي بالكامل)		
	• تركيب أجهزة إنذار على الأبواب المقاومة للحرائق ومتابعتها واختبارها. • ينبغي بناء جدران وأرضية وأسقف المكان المحيط بصفة دائمة وربطها ببعضها البعض. • ينبغي الحد من عدد مداخل ومخارج المرفق	محيط الأمن المادي	فئة الرقابة
	• الأقفال.	ضوابط الدخول المادي	
	• ينبغي ألا يتم السماح لجمهور العامة بالوصول إلى دليل الهاتف العام وسجلات الهواتف الداخلية.	تأمين المكاتب والغرف والمرافق	
	• توفير أجهزة إطفاء الحرائق ووضعها في الأماكن المناسبة.	الحماية من المخاطر الخارجية والبيئية	
		العمل في مناطق آمنة	

الملحق أ (قياسي) الضوابط المادية تكملة

مستوى الحماية	
الضوابط المتوسطة والمرتفعة	الحماية الأولية (إلزامي بالكامل)
• جميع الضوابط الأساسية أو الأولية • قصر الدخول على الأشخاص/ السيارات التي يتم التحقق من صحة أوراقها • قصر الدخول على الأشخاص/ السيارات بموجب موعد مسبق • فحص السيارات للتحقق من خلوها من الأجهزة المشبوهة	• جميع الضوابط الدنيا • الفصل بين الشحنات الواردة والصادرة بصورة مادية
• جميع الضوابط الأساسية أو الأولية • ينبغي أن يتم عزل البنود التي تتطلب حماية خاصة وحمياتها بالصورة الملائمة • ينبغي أن تتم حماية الأجهزة المسؤولة عن معالجة المعلومات الحساسة للحد من مخاطر تسرب المعلومات	• جميع الضوابط الدنيا • ضوابط للحد من مخاطر التهديدات المحتملة والمادية، مثل السرقة والحرائق والمتفجرات والدخان والمياه والأتربة والترددات والتأثير الكيميائي وتعطيل الطاقة الكهربائية وتعطيل الاتصالات والإشعاع الكهرومغناطيسي والتخزيب المتعمد • ينبغي أن تتم متابعة درجات الحرارة والرطوبة في جميع مرافق معالجة المعلومات (على سبيل المثال: غرف الخوادم.. إلخ)
• جميع الضوابط الأساسية أو الأولية • ينبغي أن يتم تركيب مولد احتياطي لجميع الأنظمة الحساسة واختباره بصفة منتظمة • ينبغي أن يتم توصيل أجهزة الاتصالات من خلال مسارين مختلفين لمنع حدوث أي إخفاق في الخدمة	• جميع الضوابط الدنيا • ينبغي أن يتم توصيل إمدادات الطاقة المتواصلة بلا انقطاع بجميع الأنظمة الحساسة واختبارها بصفة منتظمة • ينبغي صدور إنذار في حالة إخفاق إمدادات المياه
• جميع الضوابط الأساسية أو الأولية • الأنابيب المدرعة والغرف والصناديق المغلقة عند نقاط الفحص/ انتهاء الأعمال • استخدام الدروع الكهرومغناطيسية لحماية الكابلات • بدء عمليات المسح التقني لفحص المادي للكشف عن أي أجهزة غير مصرح بها	• جميع الضوابط الدنيا • ينبغي أن يتم فصل كابلات الطاقة عن كابلات الاتصالات • ينبغي استخدام علامات الكابلات والأجهزة المحددة بوضوح • ينبغي الاحتفاظ بقائمة إصلاحات موثقة • ينبغي قصر الدخول إلى غرف الإصلاحات والكابلات على فريق العمل المصرح له
• جميع الضوابط الأساسية أو الأولية • ينبغي أن يتم تنفيذ عمليات الصيانة داخل مقر المؤسسة أو في مكان يخضع للرقابة الأمنية • يتم إجراء عمليات الإصلاح وصيانة الأجهزة من قبل أفراد فريق العمل المعتمد والمصرح له والذين تتولى المؤسسة التحقق من أوراق الهوية الخاصة بهم	• جميع الضوابط الدنيا. • يتم إجراء عمليات الإصلاح وصيانة الأجهزة من قبل فريق العمل المعتمد والمصرح له فقط • ينبغي أن يتم مسح المعلومات من الأجهزة عند إرسالها إلى أي طرف آخر من أجل الإصلاح/ الصيانة

	الحماية الدنيا (إلزامي بالكامل)		
	• يقتصر الوصول إلى منطقة التسليم والتحميل من خارج النطاق على فريق العمل المصرح له والمحدد • تأمين الأبواب الخارجية المؤدية إلى منطقة التسليم/ التحميل حينما يكون أي باب داخلي مفتوح • تسجيل المواد الواردة وفحصها للتأكد من خلوها من أي أخطار محتملة	الوصول العام والتسليم ومناطق التحميل	فئة الرقابة
	• ينبغي وضع إرشادات خاصة بتناول الأطعمة والشراب والتدخين بالقرب من مرافق معالجة المعلومات • ينبغي وضع أنوار وحماية بالأسلاك الشائكة على جميع المباني وجميع خطوط الطاقة والاتصالات الواردة	تحديد مواقع الأجهزة والمعدات وحمايتها	
	• ينبغي أن تكون إمدادات الكهرباء والمياه وتكييف الهواء والصرف والتدفئة / التهوية ملائمة للأنظمة التي تتولى دعمها • ينبغي أن يتم تركيب أنوار الطوارئ	مرافق الدعم	
	• ينبغي أن تكون خطوط الطاقة والاتصالات المتصلة بمرافق معالجة المعلومات تحت الأرض أو أن تخضع للحماية البديلة الملائمة • ينبغي أن تتم حماية كابلات الشبكة من أي اعتراض غير مصرح به أو أي خسائر وتلفيات	تأمين الكابلات	
	• يتم إجراء عمليات الإصلاح وصيانة الأجهزة من قبل فريق العمل المصرح له فقط • ينبغي أن يتم حفظ السجلات الخاصة بجميع الأخطاء المشتبهه والفعلية وجميع عمليات الصيانة الوقائية/ التصحيحية	صيانة الأجهزة والمعدات	

الملحق أ (قياسي) الضوابط المادية تكملة

مستوى الحماية	
الضوابط المتوسطة والمرتفعة	الحماية الأولية (إلزامي بالكامل)
• جميع الضوابط الأساسية أو الأولية • ينبغي عدم إخراج أجهزة الحاسوب المحمولة ذات البيانات الحساسة بعيداً عن الموقع	• جميع الضوابط الدنيا • ينبغي أن يتم تحديد ضوابط العمل المنزلي (على سبيل المثال: استخدام الخزائن القابلة للإقفال والاتصالات الآمنة وغير ذلك) • ينبغي أن تستخدم أجهزة الحاسوب المحمولة ذات البيانات الحساسة عملية تشفير الوسائط
• جميع الضوابط الأساسية أو الأولية • ينبغي أن يتم تدمير الأجهزة التالفة التي تتضمن معلومات حساسة • ينبغي أن يتم تدمير الوسائط التي تشتمل على معلومات حساسة	• ينبغي أن يتم تدمير الأجهزة التي تحتوي على معلومات حساسة (بما في ذلك الوسائط وكلمات المرور الثابتة.. الخ) أو تدمير المعلومات أو حذفها أو إحلالها باستخدام تقنيات تساعد على عدم استرجاع المعلومات الأصلية
• جميع الضوابط الأساسية أو الأولية • ينبغي أن يتم تركيب مولد احتياطي لجميع الأنظمة الحساسة واختباره بصفة منتظمة • ينبغي أن يتم توصيل أجهزة الاتصالات من خلال مسارين مختلفين لمنع حدوث أي إخفاق في الخدمة	• جميع الضوابط الدنيا • ينبغي أن يتم توصيل إمدادات الطاقة المتواصلة بلا انقطاع بجميع الأنظمة الحساسة واختبارها بصفة منتظمة • ينبغي صدور إنذار في حالة إخفاق إمدادات المياه
• جميع الضوابط الأساسية أو الأولية • ينبغي وضع الحدود الزمنية لصرف الأجهزة والمعدات من الموقع وفحصها عند إعادتها إلى الموقع للتأكد من مدى التزامها • يتطلب إخراج المعلومات المصنفة عن المستوى «C3» الحصول على موافقة مدير أمن المعلومات	• جميع الضوابط الدنيا • ينبغي أن يتم تحديد العاملين والمتعاقدين والمستخدمين التابعين للأطراف الأخرى ممن لديهم سلطة الموافقة على نقل الأصول إلى خارج الموقع
• منطقة دوريات الحراسة، بالإضافة إلى حراسة المداخل. • مركز المراقبة الأمنية • الكشف عن الدخلاء والمتطفلين (على سبيل المثال: الكشف عن طريق التصوير والإنذارات) داخل الموقع	• حراسة عند المداخل على مدار ٢٤ ساعة يومياً طيلة الأسبوع • متابعة مرئية للأماكن المحيطة • متابعة مرئية عند مداخل المنطقة الأمنية • الاحتفاظ بالتسجيلات لمدة ٣٠ يوماً

	الحماية الدنيا (إلزامي بالكامل)		
	• ينبغي عدم ترك الأجهزة/ الوسائط التي يتم نقلها إلى خارج الموقع دون رقابة • ينبغي أن يتم حمل أجهزة الحاسوب المحمولة في صورة حقيبة يد • ينبغي إجراء تغطية تأمينية مناسبة	أمن الأجهزة والمعدات خارج المقر	فئة الرقابة
		التخلص الآمن من الأجهزة والمعدات أو إعادة استخدامها	
	• ينبغي ألا يتم نقل الأجهزة أو المعلومات أو البرامج إلى خارج الموقع دون تصريح مسبق • ينبغي أن يتم تسجيل المعدات عند نقلها إلى خارج الموقع وتسجيلها ثانية عند إعادتها	صرف واستبعاد الممتلكات	
	• ينبغي أن تكون خطوط الطاقة والاتصالات المتصلة بمرافق معالجة المعلومات تحت الأرض أو أن تخضع للحماية البديلة الملائمة • ينبغي أن تتم حماية كابلات الشبكة من أي اعتراض غير مصرح به أو أي خسائر وتلفيات	تأمين الكابلات	
	• حراسة فعلية عند المداخل خلال ساعات العمل	المتابعة	

الملحق ب (قياسي)

لوغاريتمات وبروتوكولات التشفير المعتمدة

تسري جميع لوغاريتمات التشفير الموصى بها في هذا الملحق «B» لمدة عام واحد من تاريخ إصدار هذا الكتيب. وينصح كتيب تأمين المعلومات الوطنية بإجراء تحديث أو وضع بدائل لهذه اللوغاريتمات حسب الاقتضاء.

هذه الخوارزميات و البروتوكولات تستخدم للتشفير ,التوقيع الرقمي ,توليد الارقام العشوائية ,اتفاق المفتاح, نقل المفتاح, إلتفاف المفتاح, اشتقاق مفاتيح إضافية من مفتاح التشفير , الارقام المزوجة ,التحكم بالوصول إلى الوسائط.

المفتاح المتماثل/ المفتاح الخاص:

اسم اللوغاريتم	المراجع	الاستخدام المعتمد	الطول اللازم للمفتاح
معيار التشفير المتقدم AES	شفرة مجموعة معايير التشفير المتقدم بناءً على لوغاريتم «Rijndael» [AES]	تشفير البيانات العامة	مفاتيح 256 بايت
معيار التشفير الثلاثي للبيانات TDES/3DES	شفرة مجموعة معايير التشفير الثلاثي للبيانات [SP800-67]	تشفير البيانات العامة	ثلاثة مفاتيح فريدة 56 بايت
ملاحظة: ينبغي أن يتم استخدام معيار التشفير المتقدم AES ما لم ذلك غير ممكن من الناحية التقنية. وينبغي أن يقتصر استخدام معيار التشفير الثلاثي للبيانات TDES على الأنظمة التي لا تدعم معيار التشفير المتقدم AES.			

المفتاح غير المتماثل/ المفتاح العام:

ينبغي أن تلتزم المهام التشفيرية التي تستخدم شفرات المفاتيح غير المتماثلة (والمعروف أيضاً باسم «تشفير المفتاح العام») من خلال مفاتيح تشفير مزدوجة تتألف من مفتاح عام ومفتاح خاص المواصفات التالية:

اسم اللوغاريتم	المراجع	الاستخدام المعتمد	الطول اللازم للمفتاح
RSA	لوغاريتم «Rivest-Shamir-Adleman»لتشفير المفتاح العام [RSA]	التوقيعات الرقمية، نقل التشفير.	مفاتيح 1024بايت
لوغاريتم التوقيعات الرقمية [DSA]	لوغاريتم التوقيعات الرقمية [FIP186-2]	التوقيعات الرقمية	مفاتيح 1024بايت

لوغاريتمات الاختزال

يمكن استخدام لوغاريتمات الاختزال في دعم تنفيذ عملية توثيق رسائل الاختزال ذات المفاتيح. وبصفة عامة، يتم استخدام وظائف الاختزال في التعجيل بتنفيذ مهام المقارنة بين البيانات – مثل العثور على البنود في أي قاعدة بيانات والكشف عن تكرار السجلات أو السجلات المماثلة ضمن ملف أو نظام كبير.

اسم اللوغاريتم	المراجع	الاستخدام المعتمد	الطول اللازم للمفتاح
SHA-n	لوغاريتمات اختزال آمنة توفر حجم اختزال «n»، وعلى سبيل المثال: (SHA 224, 256, 384, 512) [SHA]	جميع أغراض الاختزال.	n ≥ 256
ألإصدار الخامس من دورية الرسائل MD 5	الإصدار الخامس من دورية الرسائل [RFC 1321]	جميع أغراض الاختزال	الحالة النمطية 128 بايت
ملاحظة: ينبغي أن يتم استخدام SHA-n ما لم ذلك غير ممكن من الناحية التقنية. وينبغي أن يقتصر استخدام الإصدار الخامس من دورية الرسائل على الأنظمة التي لا تدعم عائلة SHA			

الملحق ج (قياسي)

تصنيف أهمية وحساسية إدارة الحوادث

التصنيف	فئات التصنيف القياسية
C1	• رفض الخدمة • الأصول المعرضة للمخاطر • القرصنة الداخلية (فعالة) • القرصنة الخارجية (فعالة) • الفيروس/ الدودة (انتشار) • تدمير الممتلكات (حساسة)
C2	• القرصنة الداخلية (فعالة) • القرصنة الخارجية (فعالة) • الوصول إلى المعلومات دون تصريح • انتهاكات السياسة • النشاط غير القانوني • المعلومات المعرضة للمخاطر • الأصول المعرضة للمخاطر (غير حساسة) • تدمير الممتلكات (غير حساسة)
C3	• البريد الإلكتروني • طلب الطب الشرعي • الاستخدام غير الملائم للممتلكات • انتهاكات السياسة

* زمن الاستجابة المبدئي – يحدد ذلك الحد الأقصى من الزمن الذي يتعين مروره قبل أن تقوم الإدارة بإخطار فريق الاستجابة لطوارئ الحاسبات في قطر.

مصفوفة الحوادث	C1	C2	C3
CSO+CII	CL1	CL1	CL3
CSO+ Non CII	CL1	CL2	CL3
Non CSO + CII	CL1	CL2	CL3
Non CSO + Non CII	CL3	CL3	CL3

CSO الاقسام الحرجة بالمؤسسة كما تم تعريفها بسياسة معلومات البنية التحتية الحرجة

CII معلومات البنية التحتية الحرجة كما تم تعريفها بسياسة معلومات البنية التحتية الحرجة

مصفوفة الاستجابة	زمن الاستجابة الابتدائي	ملاحظات
مستوي الاهمية CL1	٦٠ دقيقة	
مستوي الاهمية CL2	التقارير غير مطلوبة	التحقيقات حول الموظفين المرتبطة بجدول زمني حساس تنتمي لهذا المستوى
مستوي الاهمية CL3	التقارير غير مطلوبة	امثلة: الحوادث او التحقيقات حول الموظفين الغير مرتبطة بجدول زمني حساس التحقيقات طويلة المدى ذات البحث المكثف

زمن الاستجابة الابتدائي : اقصى مدة يمكن ان تنقضي قبل ان تقوم المؤسسة بتبليغ فريق الاستجابة لطوارئ الحاسب الآلي بدلة قطر ـ كيوسيرت

الملحق د (قياسي)

عينة اتفاقية عدم الإفصاح عن المعلومات

تم إبرام هذه الاتفاقية بتاريخ <اذكر التاريخ> بين <منظمة العمل> (ويشار إليها فيما يلي بمصطلح «المالك») والمؤسسة .

حيث يحظى المالك بملكية وحيازة معلومات سرية محددة (يشار إليها فيما يلي بمصطلح «المعلومات السرية»).

وحيث تطلب المؤسسة من المالك توفير المعلومات السرية المذكورة من أجل تقديم خدمات أو تنفيذ مشروعات محددة قد تتضمن التزامات قانونية.

الآن، وبالتالي، تشهد هذه الاتفاقية أنه بالنظر إلى قيام المالك بالإفصاح عن المعلومات السرية إلى المؤسسة وبالنظر إلى الاتفاقيات الثنائية والاعتبارات الأخرى الجيدة القيمة أو الاسمية التي يتم إقرار استلامها وكفايتها بموجب ذلك، تتعهد المؤسسة وتتفق مع المالك وفقاً لما يلي:

١- التعريف

أ- اتفاقية

أي إشارة ضمن هذا الكتيب إلى أي اتفاقية يقصد بها هذه الاتفاقية التي تمثل التفاهم الكامل بين الأطراف وتحل محل جميع الاتفاقيات الأخرى الصريحة أو الضمنية بين الأطراف فيما يتعلق بالإفصاح عن المعلومات السرية.

ب- المعلومات السرية

في هذه الاتفاقية، يقصد بـ«المعلومات السرية» تلك المعلومات ذات الصلة بالمنتجات أو الخدمات أو الأفكار أو الأعمال أو العاملين أو العلامات التجارية أو حقوق الطبع والنشر أو الملكية الفكرية أو الأنشطة التجارية الخاصة بالمالك؛ ويشتمل ذلك، على سبيل المثال لا الحصر، على المعادلات والأنظمة والعروض والمؤلفات والأجهزة والمفاهيم والتقنيات والاستراتيجيات التسويقية والتجارية والعمليات والبيانات والمعلومات التي قد تكون أو لا تكون سرية والتي لا تكون معروفة بصفة عامة لدى جمهور العامة وتستمد القيمة الاقتصادية الفعلية أو المحتملة من كونها غير معلومة بصفة عامة أو تحظى بميزة تجعل المالك يهتم بصورة قانونية بالحفاظ على سريتها. وعلاوة على ذلك، سوف يتم اعتبار جميع الوثائق التي يقدمها المالك إلى المؤسسة معلومات سرية، سواء كانت تحمل أو لا تحمل أي علامة ملكية حينما يتم الإفصاح عنها. ولا تتضمن المعلومات السرية أي ملكية فكرية موجودة مسبقا ومملوكة للمؤسسة وأي معارف أو خبرات تكتسبها المؤسسة خلال تقديم الخدمات أو تنفيذ الأنشطة بصالح المالك.

٢- الأطراف الأخرى

لا تتولى المؤسسة الإفصاح عن أي معلومات سرية إلى الأطراف الأخرى. وفي حالة وجود ضرورة ملحة للإفصاح عن أي معلومات سرية إلى الأطراف الأخرى أو الإفصاح عنها لأي سبب من الأسباب، تسعى المؤسسة وراء الحصول على تصريح كتابي مسبق من قبل المالك وتمنح المالك فرصة إبرام اتفاقية عدم إفصاح مع الأطراف الأخرى بحيث تكون مطابقة تماما لهذه الاتفاقية.

لا تقوم المؤسسة بالإفصاح عن المعلومات السرية، إلا في الحالات التالية:

- أن يوافق المالك كتابياً على الإفصاح عن المعلومات السرية.
- أن يكون الإفصاح مطلوباً بموجب إجراء قانوني أو قضائي.
- أن الإفصاح مطلوبا بموجب القانون.
- أن تكون المعلومات معروفة لدى الجمهور.

٣- إقرار الملكية والسرية

تقر المؤسسة وتوافق على أن تكون المعلومات السرية، التي يتم الإفصاح عنها من قبل المالك أو التي تتطلبها المؤسسة أو ترى أو تعلم بكونها نتيجة مباشرة أو غير مباشرة للمناقشات الدائرة وجميع المعاملات والصفقات التي تستتبع تلك المناقشات أو تنتج عنها، ملكاً مطلقا للمالك وسوف تحتفظ المؤسسة بسرية تلك المعلومات.

٤- عدم نقل ملكية الحقوق

تقر المؤسسة وتوافق على عدم اكتساب أي حق أو مصلحة بالمعلومات السرية وعلى أن يظل المالك هو صاحب الحق المطلق في تلك المعلومات السرية، ويشتمل ذلك، على سبيل المثال لا الحصر، على جميع براءات الاختراع وحقوق الطبع والنشر والعلامات التجارية والأسرار المهنية والأسماء التجارية وحقوق الملكية الأخرى المتعلقة بها في أي مكان في العالم. ولا يقوم متلقي هذه المعلومات السرية بتصنيع أو استخدام أو بيع أو توزيع تلك المعلومات السرية دون موافقة كتابية مسبقة من قبل المالك.

٥- عدم الطرح للبيع

تقر وتوافق الأطراف على ألا يكون إفصاح المالك عن المعلومات السرية إلى المؤسسة بمثابة عرض من قبل المالك ببيع أو ترخيص أو نقل ملكية هذه المعلومات السرية. وبخلاف ما يتم النص عليه صراحة بهذا الكتيب، لا يلتزم أي من الأطراف تجاه الأطراف الأخرى بأي التزامات مالية تتعلق بالمعلومات السرية. ويتم أي عرض ببيع أو ترخيص أو نقل ملكية تلك المعلومات السرية بمقتضى اتفاقية مستقلة ومنفصلة.

٦- التعويضات

يوافق كل طرف على أنه في حالة قيامه بخرق هذه الاتفاقية، يحق للطرف الآخر، بالإضافة إلى جميع التعويضات الأخرى التي يخولها له القانون، أن يتقدم إلى أي محكمة ذات اختصاص من أجل مساعدته عن طريق النظر في شكواه وتسويتها بمقتضى أحكام هذه الاتفاقية.

٧- التعديل

لا يستطيع أي طرف تعديل أي من شروط وأحكام هذه الاتفاقية إلا من خلال موافقة كتابية على تلك التعديلات يوقع عليها كلا الطرفين.

٨- الأطراف المتعاقبة

تكون هذه الاتفاقية ملزمة وسارية لصالح كلا الطرفين وكل ورثة وخلفاء وممثلي هذين الطرفين وكل من يتم إسناد حقوق هذه الاتفاقية إليهم.

٩- التنازل

لا تؤثر أي تنازلات أو تأخيرات أو تسهيلات أو إخفاقات من قبل أي طرف فيما يتعلق بأي إهمال أو تقصير من الطرف الآخر على أي حقوق أو تعويضات تتعلق بذلك الإهمال أو التقصير أو أي إهمال أو تقصير يتم التنازل عنه صراحة وبصورة كتابية.

١٠- القانون الحاكم

يتم تفسير وتأويل هذه الاتفاقية وفقاً لقوانين دولة قطر. وتخضع النزاعات التي تنشأ عن عدم الالتزام بأي من شروط وأحكام هذه الاتفاقية لاختصاص محاكم دولة قطر.

١١- بدء إجراءات التقاضي

يوافق أطراف هذه الاتفاقية إمكانية بدء رفع الدعوى أو التقاضي أو اتخاذ الإجراءات القانونية أمام أي محكمة بدولة قطر عن طريق تسليم إخطار شخصي إلى الطرف المعارض بهذه الاتفاقية أو إلى وكيل ذلك الطرف.

١٢- استمرارية الالتزام

تظل أي حقوق والتزامات تنشأ بموجب هذه الاتفاقية وتكون من طبيعتها أن تسري إلى ما بعد انتهاء الفترة الزمنية لهذه الاتفاقية قائمة بعد فسخ أو انتهاء هذه الاتفاقية وتظل تلك الحقوق والالتزامات سارية لمدة عامين عقب عملية فسخ أو انتهاء الاتفاقية. ومع ذلك، يجوز أن يطلب أي من الطرفين تطبيق فترة سرية أطول على معلومات محددة وإبلاغ الطرف الآخر بها.

١٣- أتعاب المحاماة

في حالة رفع أي دعوى قضائية من جراء هذه الاتفاقية، يحق للطرف المتغلب الحصول على أتعاب وتكاليف ونفقات المحاماة، بالإضافة إلى أي تعويضات أخرى قد تستحق لذلك الطرف.

١٤- العناوين

يتم وضع جميع الفهارس والعناوين ورؤوس الموضوعات وعناوين الفصول والمصطلحات المماثلة لأغراض مرجعية وأغراض الملاءمة ولا تهدف إلى أن تكون شاملة أو حاسمة أو أن تؤثر على مغزى أو نطاق هذه الاتفاقية.

١٥- سلطة التنفيذ

يشهد الأشخاص الموقعون أدناه أنهم مفوضون في تحرير هذه الاتفاقية نيابة عن الطرف الذي يوقعون عنه.

وإشهادا على ذلك، يقوم الطرفان بتحرير هذه الاتفاقية.

المالك (<منظمة العميل>)	المؤسسة:
توقيع:	توقيع:
الاسم:	الاسم:
الوظيفة:	الوظيفة
التاريخ:	التاريخ