بسم الله الرحمن الرحيم

وزارة رئاسة مجلس الوزراء
المركز القومي للمعلومات
الإدارة الفنية

قسم الجـ ـودة والتطوير

وحدة المعـ ـايير

لجنة معايير نظم التشغيل والسرية والتأمين

معيار قواعد الممارسة لإدارة أمن المعلومات

المرجع: المنظمة الدولية للقياس والهيئة الدولية للكهروتقنية
ISO 27002

الطبعة الثانية 15-06-2005

فبراير 2010م

المحتويات:

المقدمة

1.0 ما هو أمن المعلومات؟

تعتبر المعلومات عنصرا اساسيا لأعمال أى منظمة وبالتالي يتوجب حمايتهـا بانتظـام. إن هـذه الحماية يتعاظم دورها خاصة فى ظل عالمنا اليوم الذي يتمتع ببيئة ذات أعمال مترابطة ومتسارعة الخطى ممايزيد من حجم المهددات والمخاطر.

يجب استخدام كافة الوسائل والأساليب المتوفرة لحماية المعلومات فى أشكالها المختلفة سواء أكانت مطبوعة، مكتوبة على الورق، مخزنة الكترونيا، مرسلة بالبريد او عبر وسائط الكترونية، معروضة كافلام او منطوقة فى شكل حديث متبادل.

إن أمن المعلومات يعنى بحماية المعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها وذلك لتاكيد استمرارية الاعمال وتقليل الخسائر ورفع فرص النجاح والارباح.

يمكن تحقيق أمن المعلومات بتنفيذ مجموعة تحكمات تشمل سياسات، معالجات، اجراءات، هياكـل المنظمة ووظائف العتاد والبرمجيات. إن هذه التحكمات تحتاج لإنشاء، تطبيق، مراقبـة، مراجعـة وتطوير للتأكد من ان الأهداف المحددة لأمن وأعمال المنظمة قد تحققت.

أمن المعلومات من زاوية أكاديمية، هو العلم الذي يبحث في نظريـات واسـتراتيجيات تـوفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية تقنيـة، هـو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات مـن الأخطـار الداخليـة والخارجية، ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة.

إن استخدام اصطلاح أمن المعلومات وان كان استخداما قديما سـابقا لإنـشاء وسـائل تكنولوجيـا المعلومات، الا انه وجد استخدامه الشائع في نطاق انشطة معالجة ونقل البيانات بواسـطة وسـائل الحوسبة والاتصال، اذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معهـا عبر شبكات المعلومات- وتحديدا الإنترنت – احتلت ابحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة ، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات.

2.0 لمـاذا نحتاج لأمن المعلومات؟

إن المعلومات وعمليات الدعم، النظم والشبكات تعتبر أصول هامة للعمل. لهذا فـإن تعريـف، وتحقيق وصيانة والحفاظ على أمن المعلومات قد تكون ضرورية للحفاظ علـى القـدرة التنافـسية والتدفقات النقدية والربحية والصورة التجارية.

إن الدوافع لتوفير أمن المعلومات تشمل الاتى:

أ) مواجهة التهديدات الأمنية الناشئة من مجموعة واسعة من المـصادر بمـا فيهـا الاحتيـال بمساعدة الحاسوب، والتجسس، والتخريب، والحرائق أو الفيضانات. كما إن مسببات التلف الناتج من الشيفرات الخبيثة، والقرصنة الحاسوبية، وهجمات تعطيل الخدمة أصبحت أكثـر شيوعا ومتزايدة التعقيد.

ب) أمن المعلومات أصبح مهما لكل من القطاعين العام والخاص لحماية البنى التحتية - التـى تمثلها المعلومات – لهذه القطاعات. فى كلا القطاعين فإن أمن المعلومـات يكـون دافعـا ومنشطا لتقديم العديد من الخدمات مثل الحكومة الإلكترونية أو الأعمال الإلكترونية.

ج) كثير من نظم المعلومات لم تصمم آمنة، إن الأمن الذي يمكن تحقيقه من خلال والوسـائل التقنية محدود، لهذا يجب ان يدعم بإجراءات و إدارة مناسبة.

د) إن عملية تحديد التحكمات المطلوبة تحتاج لإهتمام بالتخطيط وإنتباه للتفاصيل. إن إدارة أمن المعلومات تحتاج كحد أدنى لمشاركة جميع العاملين في المنظمة، وقد تحتـاج لمـشاركة مـن المساهمين والداعمين و العملاء وأى مجموعات أخرى خارج المنظمة. أيضا قـد يكـون مـن المطلوب الحصول على نصائح متخصصين من خارج المنظمة.

3.0 كيفية وضع المتطلبات الأمنية

من الضروري أن تحدد كل منظمة احتياجاتها الأمنية. هناك ثلاثة مصادر رئيـسية للمتطلبـات الأمنية:

1) المصدر الأول مستمد من تقييم المخاطر على المنظمة، مع الأخذ فـي الاعتبـار اسـتراتيجية أعمال وأهداف المنظمة خلال عملية تقييم المخاطر والتهديدات.

2) المصدر الثاني هو الإجراءات القانونية والنظامية والتنظيمية والشروط التعاقدية للمنظمة مع الشركاء التجاريين والمقاولين ومقدمي الخدمات التي تتطلب توفر بيئة عمل معينة على المنظمة الإيفاء بها.

3) المصدر الثالث هو مجموعة المبادئ والأهداف والمتطلبات العملية لمعالجة المعلومات التي وضعتها المنظمة لدعم عملها.

4.0 تقييم المخاطر الأمنية

إن تحديد المتطلبات الأمنية يجب أن يتم باستخدام منهجية لتقييم المخاطر، كما إن استخدام التحكمات يحتاج إلى موازنة مع الضرر الواقع على العمل المحتمل حدوثه كنتيجة للفشل الأمنى .
إن نتائج تقييم المخاطر سوف تساعد في توجيه وتحديد الأفعال الإدارية المناسبة وأولويات إدارة المخاطر الأمنية، وفى تطبيق التحكمات التى تم اختيارها لدرء هذه المخاطر.

إن تقييم المخاطر يجب أن يتم بشكل دوري لمعالجة أية تغيرات نشأت قد تؤثر على نتائج تقييم المخاطر المعمول بها. إن المزيد من المعلومات حول تقييم المخاطر الأمنية يوجد في البند 1.4 "تقييم المخاطر أمنية ".

5.0 اختيار التحكمات

بمجرد أن يتم تحديد متطلبات الأمن والمخاطر و يتم إتخاذ القرارات اللازمة لدرءالمخاطر، يجب أن يتم إختيار التحكمات المناسبة وتطبيقها لضمان إنخفاض المخاطر إلى مستوى مقبول.

إن إختيار التحكمات يمكن أن يتم باستخدام هذه الوثيقة المعيارية، أو من غيرها من وثائق التحكمات، أو أن يتم تصميم تحكمات جديدة مناسبة لتلبية احتياجات محددة.

إن اختيار التحكمات الأمنية يجب ان يعتمد على قرارات المنظمة المبنية على أساس قياسات لقبول المخاطر، ولخيارات معالجة المخاطر ولنهج إدارة المخاطر المطبقة فى المنظمة، كما يجب أن يبنى إختيار التحكمات وفقا للتشريعات الوطنية والدولية واللوائح ذات العلاقة.

إن بعض التحكمات في هذه الوثيقة المعيارية يمكن اعتبارها مبادئ توجيهية لإدارة أمن المعلومات قابلة للتطبيق فى معظم المنظمات.

إن المزيد من المعلومات حول اختيار التحكمات وغيرها من خيارات معالجة المخاطر توجد في البند 4.2 "معالجة المخاطر الأمنية".

6.0 نقطة الانطلاق في أمن المعلومات

إن هنالك العديد من التحكمات التى يمكن اعتبارها نقطة انطلاق جيدة لتنفيذ امن المعلومات، فهي إما مبنية على أساس الاحتياجات التشريعية الأساسية أو ينظر إليها على انها ممارسة شائعة فى أمن المعلومات.

التحكمات التي تعتبر ضرورية للمنظمة من وجهة نظر تشريعية - تبعا للتشريعات المعمول بهـا - تشمل:

أ) حماية البيانات والخصوصية والمعلومات الشخصية (انظر4.1.15).

ب) حماية السجلات التنظيمية (انظر 3.1.15).

ج) حماية حقوق الملكية الفكرية (انظر2.1.15).

ما التحكمات التى تعتبر ممارسة شائعة فى أمن المعلومات تشمل:

أ) وثيقة السياسة العامة لأمن المعلومات (انظر 1.1.5)؛

ب) توزيع المسؤوليات الأمنية للمعلومات (انظر 3.1.6)؛

ج) التوعية بأمن المعلومات، والتعليم، والتدريب (انظر 2.2.8)؛

د) المعالجة الصحيحة فى التطبيقات (2.12)؛

هـ) إدارة الثغرات التقنية (انظر 6.12)؛

و) إدارة استمرارية العمل (14)؛

ز) إدارة حوادث أمن المعلومات والتحسينات (2.13).

إن هذه التحكمات تطبق على معظم المؤسسات وفي معظم البيئات.
يجب الإشارة إلى أنه و على الرغم من أن كل التحكمات في هذا معيار هامة وينبغي أخـذها فـى الإعتبار، إلا إن أهمية كل تحكم يجب أن تحدد بناء على المخاطر التى تواجه المنظمة. وبالتـالي، وعلى الرغم من أن النهج المذكور أعلاه يعتبر نقطة انطلاق جيدة، ألا أنها لا تحل محـل اختيـار التحكمات على أساس تقييم المخاطر.

7.0 عوامل النجاح الحاسمة

قد دلت التجربة على أن العوامل التالية غالبا ما تكون حاسمة بالنسبة لنجاح تنفيذ أمن المعلومات داخل المنظمة:

أ) وجود سياسة لأمن المعلومات وأهداف وأنشطة تعبر عن أهداف العمل.

ب) وجود إطار ونهج لتنفيذ وصيانة، ورصد، وتحسين أمن المعلومات منسجمة مع ثقافـة المنظمة؛

ج) الدعم والالتزام من جميع مستويات الإدارة؛

د) وجود فهم جيد لمتطلبات أمن المعلومات، وتقييم و إدارة المخاطر.

هـ) التسويق الفعال للمعلومات والأمن لجميع المديرين والموظفين والأطـراف الأخـرى لتحقيق الوعي بأهمية أمن المعلومات؛

و) توزيع توجيهات بشأن أمن المعلومات والسياسات والمعايير لجميع المديرين، المـوظفين والأطراف الأخرى؛

ز) توفير الأموال لإدارة أمن المعلومات؛

ح) توفير التوعية والتدريب والتعليم؛

ط) إنشاء نظام فعال لأمن المعلومات وإدارة الحوادث العملية؛

ي) تطبيق نظام قياس لتقييم أداء إدارة أمن المعلومات و الاقتراحات المقدمة لتحسين الأمن.

8.0 وضع التوجيهات الخاصة بك

وثيقة قواعد الممارسة هذه يمكن اعتبارها نقطة انطلاق لوضع الموجهات الخاصة بمنظمة. ليس كل التحكمات والتوجيهات في مدونة قواعد الممارسة هذه قد تكون واجبة التطبيق. ذد على ذلك فقد تكون هنالك حاجة لبعض التحكمات والموجهات غير مدرجة في هذا المعيار.

عندما يتم تطوير وثائق تحتوي على موجهات أو تحكمات إضافية سيكون من المفيد أن تدرج إحالات إلى الأحكام الواردة في هذا المعيار عند الاقتضاء لتسهيل عملية إختبار التماثل بين الوثيقة وهذا المعيار من قبل المراجعين وشركاء العمل.

1 المـــدى

إن هذه الوثيقة المعيارية الدولية تضع توجيهات ومبادئ رئيسية لإبتدار، تطبيق، معالجة وتحـسين إدارة امن المعلومات في المنظمة. إن الأهداف التوضيحية في هذا المعيار الدولي تقـدم توجيهـات عامة على الأهداف المقبولة عادة في إدارة امن المعلومات. إن أهداف التحكم وتحكمات هذا المعيار قد قصد منها التطبيق بحيث تفي بالمتطلبات التي حددتها عملية تقييم المخاطر.

إن هذا المعيار يمكن ان يستخدم كموجهه عملي لإنشاء معايير امن للمنظمة ولتطـوير ممارسـات فعالة في إدارة الأمن وللمساعدة في بناء الثقة في الأنشطة الداخلية للمنظمة.

2 المصطلحات والتعاريف

لأغرض هذه الوثيقة، تستخدم المصطلحات والتعاريف التالية:

1.2 الأصل

هو أي شئ ذو قيمة للمنظمة.

2.2 التحكم

هي مرافق إدارة المخاطر، بما في ذلك السياسات، الإجراءات الموجهات والممارسات والتي يمكمن ان تكون ذات طبيعة إدارية او تقنية او قانونية.

ملحوظة:

ان مصطلح التحكم أو الضابط يستخدم أيضاً كمرادف لمصطلحي الحامي او المضاد.

3.2 التوجيهات

هو توصيف يوضح ما ينبغي فعله وكيف، ليحقق الأهداف الموضوعة في السياسات.

4.2 مرافق معالجة المعلومات

هي اي نظام لمعالجة المعلومات او خدمة او بنية تحتية.

5.2 امن المعلومات

امن المعلومات هو الحفاظ على سرية، تكامل وتوفر المعلومات بالإضافة لخصائص أخـرى مثـل التوثق، تحديد المسئولية، عدم الإنكار والمصداقية.

6.2 حدث امن المعلومات

إن حدث امن المعلومات هو اي تحديد لحدوث حالة لنظام او لخدمة شبكية تشير لإحتمال تجـاوز للسياسات الأمنية او فشل لتقانات الحماية او حالة غير معروفة سابقاً يمكن ان تكـون لهـا علاقـة بالامن.

7.2 حادثة امن المعلومات

يستدل على حادثة امن المعلومات بوقوع حدث امن معلومات (سواء أكان مـرة واحـدة او بـشكل متتابع) غير متوقع او مرغوب فيه له احتمال مؤثر لإختـراق عمليـات العمـل ومهـدداً لأمـن المعلومات.

8.2 السياسة

هي كل الاهتمام والتوجه الذي تعبر عنه الإدارة رسمياً.

9.2 المخطر

هو احتمال وقوع حدث والآثار المترتبة عليه.

10.2 تحليل المخطر

هو الاستخدام المنظم للمعلومات لتحديد مصادر المخاطر وتقديرها.

11.2 تقييم المخاطر

هو العملية الكلية لتحليل المخاطر وإيجاد قيم لها.

12.2 قيم المخاطر

هي عملية مقارنة المخاطر المقدرة مع مقياس معطى للمخاطر لتحديد أهمية الأثر المترتـب علـى المخاطر.

13.2 إدارة المخاطر

هي الأنشطة المنسقة لتوجيه وضبط المنظمة في تعاملها مع المخاطر.

تنبيه:

إدارة المخاطر عادة تشمل تقييم المخاطر، معالجة المخطر، قبول المخاطر واتصالات المخاطر.

14.2 معالجة المخاطر

هي عملية اختيار وتطبيق قياسات أمنية لدرء المخاطر.

15.2 جهة ثالثة

هي شخص أو جهة اعتبارية ينظر إلى أنها مستقلة عن الجهات المعنية بالقضية او الموضوع.

16.2 المهدد

هو حدوث مؤثر لحدث غير مرغوب فيه مما يترتب عليه أذى للنظام أو المنظمة.

17.2 الثغرات

هي ضعف في أصل أو أصول يمكن استغلاله بأحد المهددات.

3. هيكلية المعيار

إن هذه الوثيقة المعيارية تحتوى على إحدى عشر فصل للتحكم فى الأمن تشتمل مجتمعة على 39 مجموعة امن رئيسية وفصل واحد عبارة عن مقدمة في تقييم ومعالجة المخاطر.

1.3 الفصول

كل فصل يشتمل على عدد من المجموعات الأمنية الرئيسية. الفصول الإحدى عشر مع عدد المجموعة الأمنية الرئيسية التي يحتوي عليها كل فصل هي:

أ) السياسة الأمنية (1).

ب) تنظيم امن المجموعات (2)

ج) إدارة الوصول (2)

د) امن المصادر البشرية (3)

هـ) الأمن الفيزيائي والبيئي(2)

و) إدارة الاتصالات والعمليات (10)

ز) التحكم في الوصول (7)

ح) تجميع، تطوير وصيانة نظم المعلومات(6)

ط) إدارة حوادث امن المعلومات (2)

ي) إدارة استمرارية العمل (1)

ك) الإلتزام (3)

تنبيـه: إن الترتيب الذي جاءت به هذه الفصول في هذا المعيار لا يعبر عن الأهمية. إعتماداً على الظرف فإن كل الفصول قد تكون مهمة، لهذا فإن أي منظمة تقوم بتطبيق هذا المعيار عليها إن تقوم بتحديد الفصول القابلة للتطبيق ومدى أهمية هذه الفصول وكيفية تطبيقها على معالجات العمل.

2.3 *المجموعات الأمنية الرئيسية*

كل مجموعة أمنية رئيسية تشتمل على:

أ) هدف التحكم والذي يوضح ما يجب إن يتحقق، و

ب) واحد أو أكثر من التحكمات (التحكمات) التي يمكن تطبيقها لتحقيق هدف التحكم.
أوصاف التحكم تمت هيكلتها على النحو التالي:

التحكم
يعرف التحكم بجملة محددة تحقق هدف التحكم.

توجيهات التطبيق
يوفر معلومات مفصلة تدعم تطبيق التحكم وتحقق أهدافه. بعض ما يأتي في موجهات التطبيق قد لا يكون مناسباً في كل الحالات لهذا فإن طرق أخرى لتطبيق التحكم قد تكون مناسبة أكثر.

معلومات أخرى
يوفر معلومات إضافية قد يكون من المفيد أخذها في الاعتبار كمثال الاعتبارات القانونية والمرجعية لمعايير أخرى.

4 تقييـم المخاطـر ومعالجتهـا

1.4 *تقييم المخاطـر الأمنية*

إن عملية تقييم المخاطر يجب أن تعرف وتقيس، كما يجب أن تحدد أولوية المخاطر في مقابل مقياس للمخاطر المقبولة والأهداف ذات العلاقة للمنظمة. ان نتائج هذه المقابلة يجب ان تستخدم كموجهات لتحديد أولوية الأفعال الإدارية المناسبة لإدارة مخاطر امن المعلومات ولتطبيق التحكمات المختارة للحماية.

ان عملية تقييم المخاطر واختيار التحكمات (التحكمات) قد تتم عدة مرات لتغطية الأجزاء المختلفة في المنظمة او لتغطية كل نظام معلومات على حدة. كما إن عملية تقييم المخاطر يجب ان تـشتمل على منهج متسق في تقدير حجم المخاطر (هذه العملية تعرف بتحليل المخـاطر)، وعلـى مـنهج لمقارنة المخاطر التي تم تقديرها مع مقياس للمخاطر لتحديد مدى أهمية واثر هذه المخـاطر (هـذه العملية تعرف بإيجاد قيم المخاطر).

يجب ايضاً ان تتم عملية تقييم المخاطر بشكل دوري لمعالجة التغيرات في المتطلبات الامنية وفـي وضعية المخاطر كمثال التغيرات في الأصول، المهددات، الثغرات الامنية، الاثار المترتبـة علـى المخاطر، كما يجب ان تتم اعادة عملية تقييم المخاطر عند حدوث تغييرات جوهرية.

إن عملية تقييم مخاطر امن المعلومات يجب ان تتم في نطاق معرف جيداً داخل المنظمة حتى تكون فاعلة كما يجب ان تشمل عملية التقييم العلاقات مع عمليات تقييم المخاطر في مناطق اخرى اذا كان ذلك مناسباً.

إن نطاق عملية تقييم المخاطر يمكن ان يكون شاملاً لكل المنظمة، اجـزاء مـن المنظمـة، نظـام معلومات بعينه، عناصر نظام محدد او خدمات معينة متى ما كان ذلك عملياً ومفيداً.

2.4 *معالجة مخاطر الأمن*

قبل النظر في معالجة المخاطر، يجب على المنظمة انشاء مقياس لتحديد مـا اذا كانـت المخـاطر مقبولة ام لا. ان المخاطر يمكن القبول بها كمثال، إذا كان تقييم المخطـر مـنخفض او اذا كانـت تكلفة معالجة المخطر غير قياسية للمنظمة.

إن أي مخطر يتم تحديده اثناء عملية تقييم المخاطر يجب ان يتم اتخاذ قـرار بـشأن معالجتـه. ان الخيارات المتاحة لمعالجة المخاطر تشمل:

أ) تطبيق تحكمات مناسبة لتقليص المخاطر.

ب) قبول المخاطر بشرط ايفاءها بوضوح للـسياسة الأمنيـة للمنظمـة ولمقيـاس قبـول المخاطر.

ج) تجنب المخاطر بعدم السماح بالأفعال التي تتسبب في ظهور المخاطر.

د) تحويل امر معالجة المخاطر او الاثار المترتبة عليها لجهات اخرى كمثال موردي العتاد والبرمجيات او شركات التامين.

بالنسبة للمخاطر التي يتم انخاذ قرار بمعالجتها بتطبيق تحكمات مناسبة، فإن هذه التحكمـات يجـب اختيارها وتطبيقها بحيث تحقق المتطلبات التي حددتها عملية تقييم المخاطر. يجب ان تحقـق هـذه التحكمات تقليصاً للمخاطر لمستوى مقبول بالنسبة للمنظمة آخذين في الاعتبار الاتي:

أ) متطلبات وشروط القوانين واللوائح القانونية الوطنية والدولية.

ب) أهداف المنظمة

ج) متطلبات التشغيل وشروطه.

د) كلفة التطبيق والتشغيل للتحكمات في مقابل المخاطر.

هـ) الموازنة بين الاستثمار في تطبيق وتشغيل التحكمات والأذى المتوقع حدوثـه مـن الفشل الأمني.

إن التحكمات يمكن أن يتم اختيارها من هذه الوثيقة المعيارية او من اي مجموعة تحكمـات (تحكمات) أخرى، او ان تصمم تحكمات جديدة لتلبي الحاجات المحددة للأنظمة. مـن الـضروري التركيز بان هنالك بعض التحكمات التي لا يمكن تطبيقها على اي نظام معلومات او بيئة وربمـا لا تكون مناسبة لكل المنظمات. كمثال فإن البند (3.10) يصف كيف يمكن تقسيم الاعباء والواجبـات لمنع التزوير والأخطاء. بالنسبة للمنظمات الصغيرة قد لا تكون عملية التقسيم للاعباء والواجبـات ممكنة، وكمثال اخر فإن البند (10.10) يصف كيف تتم مراقبة استخدام نظام وتجميـع الادلـة. إن

التحكمات الموصوفة مثل راصد الاحداث ربما يتعارض مع القوانين واللوائح المطبقة مثل حماية خصوصية العملاء او العاملين.

يجب ان يتم اخذ تحكمات امن المعلومات في الاعتبار عند تحديد مواصفات ومتطلبات النظم وفي مرحلة التصميم. ان عدم القيام بذلك يترتب عليه تكاليف إضافية وحلول اقل فعالية، وربما في الحالة الأسوأ عدم القدر على الحصول على الأمن المطلوب والمناسب.

يجب ايضاً ن يكون معلوماً انه لا يمكن لأي مجموعة من التحكمات ان تحقق أمناً كاملاً، لهذا فإن إجراءات وأفعال إدارية إضافية يجب ان تطبق من اجل مراقبة، تقييم، وتطوير كفاءة وفاعلية التحكمات الأمنية لدعم رغبات المنظمة في مجال الأمن.

5 السياسة الأمنية

1.5 سياسة أمن المعلومات

الغرض: إن الغرض من السياسة الأمنية للمعلومات هو توجيه إدارة المنظمة ودعمها فى طريقة تعاملها مع أمن المعلومات المطلوب للعمل ومع القوانين واللوائح ذات العلاقة.

1.1.5 وثيقة سياسة أمن المعلومات

التحكم

يجب أن تجاز وثيقة سياسة أمن المعلومات من قبل الإدارة العليا للمنظمة وأن توزع لكافة العاملين بالمنظمة والجهات الخارجية ذات العلاقة.

توجيهات التطبيق:

يجب أن تنص وثيقة سياسة أمن المعلومات على موافقة الإدارة العليا وان تضع رؤية المنظمة فى إدارة أمن المعلومات، لهذا يجب ان تشتمل الوثيقة على:

أ) تعريفا لأمن المعلومات وللأهداف التى يحققها وتحديدا لمداه وأهميته كأداة مفعلة ومنشطة للتشارك فى المعلومات.

ب) نصا يعبر عن دعم الإدارة العليا للمنظمة لأهداف ومبادئ أمن المعلومات المنسجمة مع إستراتيجية العمل وأهداف المنظمة.

ج) إطارا لوضع التحكمات وأغراضها بما فى ذلك هيكلية تحسس وإدارة المخاطر.
د) توضيحا للسياسات الأمنية، المبادئ، القياسات، ومتطلبات التوافق ذات الأهمية الخاصة للمنظمة وتشمل:
1- التوافق مع متطلبات القوانين واللوائح والتعاقدات.
2- متطلبات تعلم الأمن، التدريب و التوعية.
3- إستمرارية إدارة العمل.
4- عواقب تجاوز سياسة أمن المعلومات.

(هـ) تعريفا للمسئوليات العامة والخاصة لإدارة امن المعلومات بالمنظمة.
(و) تسمية مراجع تدعم وثيقة سياسة أمن المعلومات، كمثال المراجع التى تحتوى على السياسات الأمنية المفصلة والإجراءات لنظم معلومات معينة.

معلومات أخرى

إن سياسة أمن المعلومات يمكن أن تكون جزءا من وثيقة عامة لسياسات المنظمة.
إذا تم توزيع وثيقة أمن المعلومات خارج المنظمة يجب الإنتباه لضرورة عدم إحتواءها على معلومات حساسة عن المنظمة.

2.1.5 مراجعة سياسة أمن المعلومات

التحكم

يجب ان تتم مراجعة وثيقة سياسة أمن المعلومات بعد فترات محددة أو عند حدوث تغيرات مهمة فى المنظمة للتأكد من أن الوثيقة مناسبة وفاعلة.

توجيهات التطبيق:

يجب أن تكون هنالك جهة مالكة لوثيقة سياسة أمن المعلومات موافق عليها من الإدارة العليا للمنظمة ومخولة لإنشاء السياسة ومراجعتها وتقييمها.

إن عملية المراجعة يجب أن تشتمل على بحث فرص تطوير سياسة أمن المعلومات بالمنظمة وعلى طرق إدارة أمن المعلومات كاستجابة للتغير في بيئة المنظمة، في ظروف العمل، فى الشروط القانونية أو فى البيئة التقنية. يجب أن تكون هنالك إجراءات مراجعة معرفة بما فى ذلك جدولة او فترات المراجعة. إن المدخلات المطلوبة لعملية المراجعة الإدارية تشمل:

أ) ملاحظات من الجهات المعنية
ب) نتائج مراجعات من جهات مستقلة
ج) نتائج مراجعات إدارية سابقة
د) التغيرات التى يمكن أن تؤثر على طريقة إدارة المنظمة لأمن المعلومات بما فى ذلك تغيرات بيئة العمل فى المنظمة، ظروف العمل، توفر الموارد، الشروط القانونية والتنظيمية والبيئة التقنية
هـ) التوجهات الجديدة فى مجال المخاطر والثغرات الأمنية
و) التقارير الراصدة لأحداث أمن المعلومات
ز) التوصيات التى تقدمها الجهات ذات العلاقة

إن مخرجات عملية المراجعة الإدارية يجب ان تشتمل على القرارات والأفعال ذات العلاقة بالأتى:

أ) تطوير توجهات المنظمة فى إدارة سياسة أمن المعلومات وعملياتها.
ب) تطوير أهداف وأدوات التحكم.
ج) تطوير تخصيص الموارد والمسئوليات.

يجب ان يكون هنالك سجل لعمليات المراجعة الإدارية، كما يجب الحصول على موافقة الإدارة العليا على سياسة أمن المعلومات بعد مراجعتها.

6 تنظيم أمن المعلومات

1.6 التنظيم الداخلي

الهـدف : إدارة أمن المعلومات داخل المنظمة

ينبغي أن يتم إنشاء إطار عمل للمبادرة والتحكم في تطبيق امن المعلومات داخل المنظمة.

يجب أن تصادق الإدارة على سياسة أمن المعلومات، تخصيص إسناد الأدوار الأمنية ، وتنسيق ومراجعة تطبيق الأمن في جميع أنحاء المنظمة .

وإذا لزم الأمر فينبغي انشاء كيان استشاري متخصص يكون متاحاً داخل المنظمة، كما ينبغي تطوير الاتصالات مع افراد وجماعات امن متخصصة من خارج المنظمة بما في ذلك الهيئات ذات العلاقة، من اجل مواكبة التوجهات الصناعية، مراقبة المعايير وطرق التقييم وذلك بغرض توفير نقاط للاتصال مناسبة عند التعامل مع حوادث أمن المعلومات.

يجب تشجيع إتباع نهج متعدد التخصصات في مجال أمن المعلومات.

1.1.6 التزام الإدارة بأمن المعلومات

التحكـم

ينبغي للإدارة أن تدعم أمن المعلومات داخل المنظمة من خلال تبني اتجاه واضح المعالم، والتزام ثابت، وممارسة مهام وظيفية جلية، والإقرار بوجود مسئوليات أمن المعلومات .

توجيهات التطبيق

يجب إيفاء الإدارة بالمهام الآتية :

أ) ضمان تحديد أهداف أمن المعلومات، وتلبية الاحتياجات التنظيمية التي يجب أن تتكامل مع بعضها في نسق عمليات متسقة.

ب) الصياغة والمراجعة، والموافقة على سياسة أمن المعلومات .

ج) استعراض فعالية تنفيذ سياسة أمن المعلومات .

د) تقديم التوجيه الواضح وتوفير الدعم الإداري لمبادرات الأمن.

هـ) توفير الموارد اللازمة لأمن المعلومات .

و) الموافقة (التصديق) على تخصيص المهام والمسؤوليات المحددة في مجال أمن المعلومات في كل المنظمة.

ز) الشروع في إنشاء خطط وبرامج للحفاظ على استدامة استمرارية الوعي بأمن المعلومات.

ح) ضمان ان تنفيذ تحكمات أمن المعلومات قد تم بتناسق في جميع أنحاء المنظمة (أنظر 2.1.6) .

يجب أن تحدد الإدارة الحاجة للإستشارة الداخلية أو الخارجية المتخصصة في أمن المعلومات، وعلى الإدارة مراجعة وتنسيق نتائج المشورة في كافة أنحاء المنظمة.

إعتماداً على حجم المنظمة، يمكن معالجة المسئوليات من قبل منتدى إدارة متخصص ، أو من قبل هيئة إدارية قائمة مثل مجلس الإدارة.

معلومات أخرى

للمزيد من المعلومات أنظر ISO/IEC /13335 -1: 2004 .

2.1.6 تنسيق أمن المعلومات

التحكم

ينبغي أن يقوم ممثلو الأقسـام المختلفة في المنظمة بتنسيق أنشطة أمن المعلومات اعتماداً على الأدوار والمهام ذات الصلة بوظائفهم.

موجهات التطبيق

يجب أن يشتمل تنسيق أمن المعلومات على مضامين التعاون والتعاضد ما بين المدراء، المستخدمين، الإداريين ومصممي التطبيقات، المدققين، أفراد شئون الأمن، وذوي المهارات المتخصصة في مجالات مثل التأمين والشئون القانونية، الموارد البشـرية، وتقنية المعلومات أو إدارة المخاطـر.

يجب ان يؤدي هذا النشاط التنسيقي الى:

أ) ضمان ان يتم تنفيذ الأنشطة الأمنية متسقة مع السياسة الأمنية متسقة مع سياسة أمن المعلومات.

ب) تحديد كيفية التعامل مع حالات التنفيذ غير المتسقة مع السياسة الأمنية.

ج) المصادقة على منهجيات وعمليات أمن المعلومات كمثال تقييم المخاطر وتصنيف المعلومات.

د) التعرف على التغيرات الكبيرة الخطيرة في مجال تهديد أمن المعلومات ورصد قابلية تعرض المعلومات ومرافق ومرافق معالجتها للتهديدات .

هـ) تقييم مدى ملائمة تحكمات امن المعلومات وتنسيق تنفيذها.

و) التطوير الفعال للتعليم، التدريب، والتوعية بأمن المعلومات في جميع أنحاء المنظمة.

ز) تقييم المعلومات الواردة من رصد ومراجعة حوادث أمن المعلومات، والتوصية باتخاذ الإجراءات المناسبة استجابة لحوادث أمن المعلومات التي تم التعرف عليها.

إذا كانت المنظمة لا تستخدم مجموعة منفصلة ذات مهام وظائفية متداخلة للإضلاع بالمهام الموصوفة اعلاه لاسباب مثل أن تلك المجموعة غير ملائمة مع حجم المنظمة، فإن المهام اعلاه يجب ان توكل مهمة تنفيذها إلى هيئة إدارية اختصاصية مناسبة أو تعهدها إلى مدير مفرد.

3.1.6 توزيع مسئوليات أمن المعلومات

التحكم

يجب أن تكون مسؤوليات أمن المعلومات محددة بوضوح.

توجيهات التطبيق

يجب أن يتم توزيع مسؤوليات أمن المعلومات وفقاً لسياسة أمن المعلومات (انظر الفصل 4) كما ينبغي أن تكون مسؤوليات حماية كل أصل من أصول المنظمة و العمليات الأمنية الواجب القيام بها محددة بوضوح.

أن هذه المسؤولية يجب ان تكون مدعومة (عند الضرورة) لمواقع محددة ولمرافق معالجة المعلومات. كما ينبغي أن تكون المسؤوليات المحلية لحماية الأصول وللقيام بتنفيذ عمليات أمنية معينة مثل تخطيط استمرارية الأعمال معرفة بوضوح تام.

يمكن للأفراد من ذوي المسؤوليات الأمنية تفويض مهام أمنية إلى غيرهم. ولكن يظل أولئك الأفراد مسئولون، وعليهم التأكد من ان المهام المفوضة من قبلهم قد تم ادائها بالشكل الصحيح. ان المجال المسئول عنه كل فرد يجب ان يحدد بوضوح وعلى وجهة الخصوص يجب:

أ) أن تكون الأصول والعمليات الأمنية المرتبطة بكل نظام معين محددة ومعرفة بوضوح.

ب) تعيين وتحديد الجهة المسئولة عن أى أصل موجود وعن أي عملية أمنية، وينبغي أن تكون تفاصيل هذه المسئولية موثقة (أنظر أيضاً 2.1.7) .

ج) أن تكون مستويات تفويض المهام محددة بوضوح وموثقة .

معلومـات أخـرى

في العديد من المنظمات يتم تعيين مدير أمن المعلومات ليحمل المسؤولية الشاملة من أجل تطوير وتنفيذ الأمن ودعم تحديد التحكمات . ومع ذلك ستكون مسؤولية تأصيل وتنفيذ التحكمات غالباً ملقاة على عاتق المديرين الأفراد القائمين بالأمر.

من الممارسات الشائعة أن يتم تعيين مالك واحد لكل أصل موجود بحيث يكون هو المسئول عن حمايته يوماً بيوم .

4.1.6 عملية ترخيص مرافق معالجة المعلومات

التحكم

يجب أن تكون عملية ترخيص الإدارة للمرافق الجديدة لمعالجة المعلومات معرفة ومطبقة.

توجيهات التطبيق

يجب مراعاة التوجيهات التالية عند عملية الترخيص:

أ) ينبغي أن تكون المرافق الجديدة مرفقة بالترخيص الإداري المناسب الذي يخول استخدامها وأغراضها. ويجب الحصول على الترخيص من المدير المسئول عن الحفاظ على بيئة أمن نظم المعلومات المحلية للتأكيد بأن كل السياسات الأمنية والمتطلبات ذات الصلة بها قد تمت تلبيتها .

ب) عند اقتضاء الضرورة، ينبغي فحص مجموعة الأجهزة والبرمجيات للتأكد من أنها متوافقة تشغيلياً مع مكونات النظم الأخرى.

ج) إن استخدام مرافق معالجة المعلومات الشخصية أو الخاصة مثل أجهزة الحاسوب المحمولة، وأجهزة الحاسوب المنزلية، أو المحمولة باليد التي تُستخدم في معالجة معلومات الأعمال من الممكن ان تتسبب في ثغرات امنية جديدة، لذا يجب تحديد التحكمات اللازمة وتطبيقها.

5.1.6 الاتفاقات السرية

التحكم

إن متطلبات السرية أو اتفاقات عدم كشف المعلومات التي تعكس مدى حاجة المنظمة إلى حماية معلوماتها ينبغي مصطلحات ومراجعتها بصفة منتظمة.

توجيهات التطبيق

يجب ان تعالج السرية أو اتفاقات عدم كشف المعلومات الاحتياجات اللازمة لحماية المعلومات السرية باستخدام مفاهيم قانونية واجبة النفاذ.

لتحديد احتياجات السرية أو اتفاقات عدم كشف المعلومات ينبغي وضع العناصر التالية في الاعتبار:

أ) وضع تعريف للمعلومات التي يجب حمايتها (مثلاً المعلومات السـرية) .

ب) المدة المتوقعة لسريان الاتفاق، على أن تشمل الحالات التي تكون فيها المحافظة على سرية المعلومات ضرورية إلى أجل غير مسمى.

ج) الإجراءات اللازمة عند إنهاء الاتفاق المبرم.

د) المسؤوليات والإجراءات التي تتخذها الأطراف الموقعة على الاتفاقية لتفادي كشف المعلومات دون تصريح (مثلاً عند الحاجة لمعرفة المعلومات) .

هـ) ملكية المعلومات، والأسرار المهنية التجارية، والملكية الفكرية وكيفية ربطها بحماية المعلومات لسرية.

و) الاستخدام المسموح به للمعلومات السرية، وحقوق الأطراف الموقعة على استخدام المعلومات.

ز) الحق في مراجعة ورصد الأنشطة التي تنطوي على معلومات سرية.

ح) عملية الإخطار والإبلاغ عن الإفشاء غير المرخص به أو كشف المعلومات السرية.

ط) مصطلحات المعلومات التي ترجع أو التي ينبغي إتلافها عند عدم إكمال الاتفاق.

ي) الإجراءات المتوقع اتخاذها عند الإخلال بهذه الاتفاقية.

استناداً على المتطلبات الأمنية للمنظمة، فأنه من المحتمل وجود حاجة إلى عناصر أخرى في مجال السرية أو اتفاق عدم الكشف. يجب أن تكون السرية واتفاقات عدم الكشف متسقة مع كافة القوانين واللوائح المعمول بها لدى الولاية القضائية والمنطبقة عليها (انظر أيضاً 1.1.5).

يجب إعادة النظر دورياً في متطلبات السرية واتفاقات عدم الكشف عند حدوث التغييرات التي تؤثر على هذه المتطلبات.

<u>معلومات أخرى</u>

إن السرية واتفاقات عدم الكشف تحمي المعلومات التنظيمية، وستطلع الأطراف الموقعة على دورهم في حماية، واستعمال وكشف المعلومات بصورة مسئولة وبنهج مصرح به.

قد تكون هناك ثمة حاجة للمنظمة لإستخدام أشكال مختلفة من السرية أو اتفاقات عدم الكشف في الظروف المختلفة.

6.1.6 الاتصال مع الهيئات الأخرى

التحكم

يجب المواظبة على إجراء الاتصالات المناسبة مع الهيئات المختصة.

توجيهات التطبيق

يجب أن تكون في المنظمة إجراءات معمول بها تمكن من تحديد متى، وما هي الجهة المختصة التي ينبغي الاتصال بها كمثال الجهة المختصة بتنفيذ لقانون، وحدة المطافئ،...الخ)، وكيفية الإبلاغ عن حوادث أمن المعلومات التي تم تحديدها في الوقت المناسب.

المنظمات التي تكون عرضة للهجوم بوسائل الإنترنت فإنها ستحتاج إلى أطراف ثالثة خارجية لحمايتها (مثلاً مزودي خدمات الإنترنت أو مشغلي أجهزة الاتصالات السلكية واللاسلكية) وإتخاذ الإجراءات الوقائية ضد مصدر الهجوم.

معلومات أخـرى

الحفاظ على إجراء مثل هذه الاتصالات قد تكون شرطاً مطلوباً لدعم إدارة حوادث أمن المعلومات (انظر 2.13) أو استمرارية العمل وعملية التخطيط للطوارئ (انظر الفصل 14) إن إجراء الاتصالات مع الهيئات المنظمة سيكون ايضاً مفيد حتى يتسنى للمنظمة الإحاطة والاستعداد لحدوث التغييرات المرتقبة في القانون أو اللوائح التي يجب أن تتبعها المنظمة.

الاتصال مع الهيئات الأخرى يشمل ، خدمات الطوارئ، والصحة والسلامة كمثال إدارات إطفاء النار (التي لها ارتباط باستمرارية الأعمال)، ومزودي أجهزة الاتصالات السلكية واللاسلكية (الذين لهم علاقة بالتوجيه وتوفير الخطوط)، وموردي المياه (الذين لهم ارتباط بمرافق تبريد المعدات) .

7.1.6 الاتصال مع المجموعات ذات الاهتمامات الخاصة

التحكم

ينبغي الحفاظ على إجراء الاتصالات المناسبة مع المجموعات ذات الاهتمام الخاص أو المحافل الأمنية المختصة والاتحادات المهنية الأخرى.

توجيهات التطبيق

يجب أن يعتبر اكتساب العضوية في مجموعات الاهتمام الخاص أو المحافل الامنية المختصة وسيلة لتحقيق الآتي:-

أ) تحسين المعرفة حول أفضل الممارسات، ولمواكبة المعلومات الأمنية ذات العلاقة بالامن.

ب) ضمان توفر الفهم الحديث الكامل عن مجال بيئة أمن المعلومات.

ج) تلقي التحذيرات المبكرة من تنبيهات، نشرات الأنباء ومكافحات الهجوم والثغرات الامنية.

د) الحصول على نصائح أشخاص متخصصين فى امن المعلومات.

هـ) المشاركة وتبادل المعلومات حول التقنيات الجديدة، والمنتجات، والتهديدات أو الثغرات الامنية.

و) توفير نقاط ارتباط مناسبة عند التعامل مع حوادث أمن المعلومات (انظر أيضاً 1.2.13).

معلومات أخـرى

يمكن إنشاء اتفاقات للتشارك في المعلومات من أجل تحسين التعاون والتنسيق في مجال القضايا الأمنية. ويجب أن تحدد هذه الاتفاقات الاحتياجات اللازمة لحماية المعلومات الحساسة.

8.1.6 المراجعة المستقلة لأمن المعلومات

التحكم

يجب مراجعة منهج المنظمة في إدارة امن المعلومات ونسق تنفيذها (كمثال أهداف التحكم، التحكمات، السياسات، العمليات، وإجراءات أمن المعلومات) بشكل مستقل في فترات مخطط لها مسبقاً أو عند حدوث تغييرات كبيرة ذات مغزى في مجال تنفيذ الأمن .

توجيهات التطبيق

يستوجب أن تنشئ الإدارة آلية مراجعة مستقلة. إذ أن مثل هذه المراجعة المستقلة ستكون ضرورية لضمان استمرار صلاحية وكفاءة منهج ادارة امن المعلومات. كما يجب أن تشمل المراجعة تقييم

الفرص المتاحة لتحسين الأداء، والحاجة إلى إجراء تغييرات في منهج الأمن، والسياسة الأمنية وأهداف التحكمات.

وينبغي ان يقوم بالمراجعة أفراد مستقلون يعملون خارج المجال الخاضع للمراجعة مثل المراجعة الداخلية، مدير مستقل أو جهة أخرى مستقلة متخصصة في المراجعة.

إن الأفراد الذين يضطلعون بهذه المراجعات ينبغي أن تتوفر لديهم المهارات والخبرات المناسبة. ويجب تسجيل وإبلاغ نتائج تلك المراجعة المستقلة إلى الإدارة المسؤولة عن المراجعة و الاحتفاظ بسجلات للمراجعة. وإذا بينت المراجعة المستقلة أن منهج المنظمة في أمن المعلومات غير مناسب، أو أنه غير متناسق مع توجهات أمن المعلومات المبينة في وثيقة سياسة أمن المعلومات (انظر 1.1.5) فعلى الإدارة عندئذ النظر في اتخاذ اجراءات تصحيحية.

معلومات أخـرى

إن المجال الذي يجب أن يقوم المدراء بمراجعته بانتظام(انظر 1.2.15) يمكن أيضاً أن يراجع من جهة مستقله. يمكن أن تتضمن أساليب المراجعة مقابلات مع الإدارة، والتدقيق في السجلات، أو مراجعة وثائق السياسة الأمنية. يمكن أن توفر المبادئ التوجيهية الصادرة من آيـزو لعام 2002م ISO/9011:2002 للجودة ومراجعة نظم إدارة البيئة مرجعية مفيدة للاضطلاع بمهام المراجعة المستقلة، بما في ذلك إنشاء وتطبيق برنامج للمراجعة. يحدد البند(3.15) التحكمات ذات الصلة بالمراجعة المستقلة لنظم المعلومات التشغيلية و استخدام أدوات مراجعة النظم.

2.6 الأطراف الخارجية

الهـدف : الحفاظ على أمن معلومات المنظمة وعلى مرافق معالجة المعلومات التي يمكن الوصول إليها او تلك التي تعالج او تتصل او تدار من قبل أطراف خارجية.

يجب ان لا يضعف مستوى أمن معلومات المنظمة ومرافق معالجة معلوماتها بإدخال منتجات أو خدمات طرف خارجي.

كما يجب السيطرة والتحكم في الوصول للمعلومات لمرافق معالجة معلومات المنظمة بواسطة أطراف خارجية وكذلك معالجتها او الاتصال بها.

عندما تقتضي دواعي العمل التعامل مع أطراف خارجية قد تحتاج للوصول لمعلومات المنظمة ومرافق معالجة معلوماتها، او عندما تحتاج او توفر المنظمة منتج او خدمة إلى أو من طرف

خارجي فيجب القيام بعملية تقييم للمخاطر لتحديد الاثار المترتبة والتحكمات اللازمة. كما يجب ان يتم الاتفاق على التحكمات وتعريفها في الاتفاق مع الاطراف الخارجية.

6.2.1 تحديد المخاطر ذات الصلة بالأطراف الخارجية

التحكم

إن المخاطر التي تتعرض لها معلومات المنظمة ومرافق معالجة معلوماتها أثناء عمليات تنفيذ الأعمال مع الأطراف الخارجية يجب تحديدها، ووضع التحكمات الملائمة لها قبل الضلوع في إتاحة الوصول اليها.

توجيهات التطبيق

حيثما كانت هناك حاجة للسماح لطرف خارجي للوصول إلى معلومات او مرافق معالجة معلومات المنظمة ، فأنه يجب ان تتم عملية تقييم للمخاطر لتحديد التحكمات اللازمة (انظر أيضاً الفصل 4). عند تحديد المخاطر ذات الصلة بالسماح لطرف خارجي للحصول للمعلومات ينبغي أخذ القضايا التالية بعين الاعتبار:

أ) تحديد مرافق معالجة المعلومات التي تود المنظمة أن تُتيحها للطرف الخارجي للوصول إليها.

ب) نوع الوصول المتاح للطرف الخارجي للوصول إلى المعلومات ومرافق معالجة المعلومات على سبيل المثال : -

1) الوصول المادي مثلاً الى المكاتب، أو قاعات الحواسيب أوخزائن حفظ الملفات.

2) الوصول المنطقي مثـلاً: إلى قواعد بيانات المنظمة ونظم المعلومات.

3) الاتصالية المتاحة لشبكة الربط ما بين المنظمة وشبكة (شبكات) الاتصال التي يملكها الطرف الخارجي مثلاً الاتصال الدائم والوصول عن بعد (ولوج عن بعد).

4) ما إن كان الولوج يتم من داخل الموقع أو من خارج الموقع.

ج) مدى قيمة وحساسية المعلومات المعنية، ودرجة حرجيتها لعمليات الأعمال.

د) التحكمات اللازمة لحماية المعلومات التي لا ينبغي أن تصل إليها الأطراف الخارجية.

هـ) مجموعة الموظفين في دائرة الطرف الخارجي الذين يتناولون معلومات المنظمة.

و) كيفية تحديد تفويض المنظمة أو مجموعة الموظفين المخولين وكيفية مراجعة التفويض لإعادة توكيد التخويل.

ز) تحديد المرافق والتحكمات المختلفة التي يستخدمها الطرف الخارجي عند تخزين ومعالجة وتوصيل المعلومات، ومشاركة وتقاسم المعلومات مع الجهات الأخرى.

ح) تأثير عدم تمكن الطرف الخارجي من الوصول إلى المعلومات عند حاجته لها وأيضاً اثر وصول الطرف الخارجي الى معلومات غير دقيقة أو مضللة.

ط) الممارسات والإجراءات المطلوبة للتعامل مع حوادث أمن المعلومات، والأضرار المحتملة، والأحكام والشروط التي ينبغي الموافقة عليها لاستمرار الطرف الخارجي في الوصول إلى المعلومات عند وقوع حادثة أمن المعلومات.

ي) المتطلبات القانونية والتنظيمية والالتزامات التعاقدية المناسبة الأخرى التي ينبغي أن تُؤخذ بعين الاعتبار عند التعاقد مع الطرف الخارجي.

ك) كيفية تأثير الترتيبات المتخذة على مصالح أصحاب المصلحة الآخرين .

ينبغي عدم إتاحة الفرصة للأطراف الخارجية للوصول إلى معلومات المنظمة إلا بعد تنفيذ التحكمات الملائمة، وإن كان مجدياً يجب توقيع عقد يحدد أحكام وشروط الاتصال أو الوصول إلى المعلومات وترتيبات العمل. عموماً، فإن جميع الاحتياجات الأمنية الناجمة عن العمل مع أطراف خارجية يجب أن تعكس في الاتفاقية مع الطرف الخارجي (انظر أيضاً 2.2.6 و 3.2.6).

ينبغي التأكد من أن الطرف الخارجي مدرك لالتزاماته ويقبل المسؤوليات والالتزامات المتضمنة في عمليات الوصول إلى المعلومات، معالجتها، الاتصال او إدارة معلومات المنظمة ومرافق معالجة معلوماتها.

معلومات أخـرى

قد تكون المعلومات معرضة للخطر من قبل أطراف خارجية نسبة لعدم كفاءة إدارة أمن المعلومات. يجب تحديد التحكمات وتطبيقها وإدارتها عند إتاحة الفرصة للطرف الخارجي للوصول إلى مرافق معالجة معلومات المنظمة، وعلى سبيل المثال: فإذا كانت ثمة حاجة خاصة في توخي سـرية المعلومات، فأنه يمكن استخدام اتفاقات عدم إفشـاء المعلومات.

قد تواجه المنظمات مخاطر ناجمة عن العمليات المتداخلة في معالجة البيانات والإدارة والاتصال إذا تم بدرجة عالية تطبيق الاستضافة الخارجية. أو عند وجود عدة أطراف خارجية ضالعة في العمليات المختلفة .

تغطي التحكمات (2.2.6 و 3.2.6) الترتيبات المختلفة للأطراف الخارجية الأمثلة تشمل :-

أ) مقدمي الخدمات، مثل مقدمي خدمات الإنترنت، ومزودي الشبكات، وخدمات الهاتف، والصيانة، وخدمات الدعم.

ب) إدارة الخدمات الأمنية.

ج) العمـلاء (الزبائـن) .

د) الاستضافة الخارجية للمرافق و/ أو العمليات، على سبيل المثال: نظم تقنية المعلومات وخدمات جمع البيانات وعمليات مراكز الطلبات .

هـ) مستشاري الإدارة والخبراء الاستشاريين في إدارة الأعمال، ومراجعي الحسابات.

و) مطوري المخترعات والموردين، على سبيل المثال: منتجات البرمجيات ونظم تقنية المعلومات.

ز) خدمات التنظيف، والمطاعم، وغيرها من خدمات الدعم المستضافة خارجياً.

ح) مجموعة الموظفين المؤقتين، ووضع الطلاب في الأمكنة المناسبة وغيرها من التعيينات المؤقتة الموسمية القصيرة الأجل.

ستساعد مثل هذه الاتفاقات على تقليل المخاطر المرتبطة بأطراف خارجية.

2.2.6 المعالجة الأمنية عند التعامل مع الزبائن

التحكـم

ينبغي معالجة المتطلبات الأمنية المحددة قبل منح العملاء فرصة الوصول إلى معلومات أو أصول المنظمة .

توجيهات التطبيق

ينبغي وضع الاعتبار للشروط التالية عند معالجة الأوضاع الأمنية قبل إعطاء الزبائن إذن الوصول إلى أي من أصول المنظمة (اعتماداً على نوع ومدى تفويض إذن الوصول الممنوح واربما قد لا تنطبق فيها جميع الشروط):

أ) حماية الأصول وتشمل الآتي :-

1) إجراءات حماية أصول المنظمة، بما في ذلك المعلومات والبرمجيات وإدارة الثغرات المعروفة.

2) إجراءات لتحديد ما إذا كان اختراق للإصول مثل فقدان او تعديل البيانات قد حدث.

3) سـلامة وتكامل البيانات.

4) القيود المفروضة على نسخ المعلومات والكشف عنها.

ب) وصف المنتج أو الخدمة المراد تقديمها .

ج) الدواعي المختلفة، الاحتياجات، والفوائد المكتسبة من إتاحة إذن الوصول إلى المعلومات للعملاء .

د) سياسة التحكم في الوصول إلى المعلومات تشمل الآتي : -

1) الطرق المسموح بها للوصول إلى المعلومات، وسبل السيطرة عليها واستخدام وثائق التعريف الفريدة مثل استخدام بطاقات الهوية وكلمات الـسر.

2) وصول المستخدم إلى المعلومات، والامتيازات الممنوحة له.

3) الإعلان ان كل الوصول غير المرخص بوضوح سيمنع.

4) عملية إلغاء حقوق الوصول إلى المعلومات، أو مقاطعة الاتصال بين النظم.

هـ) الترتيبات اللازمة لتقديم التقارير، والإخطار، والتحقيق في عدم دقة المعلومات (على سبيل المثال: التفاصيل الشخصية) وحوادث أمن المعلومات والخروقات الأمنية.

ز) وصف كل خدمة يمكن تقديمها حتى تكون متاحة.

ح) الحق في المراقبة، وإلغاء أي نشاط يتعلق بأصول المنظمة.

ط) الالتزامات الخاصة بكل من المنظمة والعملاء.

ي) المسؤوليات ذات الصلة بالمسائل القانونية، وكيفية التأكد من الإيفاء بمتطلباتها، على سبيل المثال: تشريعات حماية البيانات خاصة اذا أخذ في الاعتبار النظم القانونية الوطنية المختلفة إذا كان الاتفاق يشمل التعاون مع عملاء في بلدان أخرى (انظر أيضاً 1.15) .

ك) حقوق الملكية الفكرية وحقوق التأليف و النشر (انظر 2.1.15 وحماية أي عمل مشترك (انظر أيضاً 5.1.15) .

معلومات أخرى

يمكن أن تختلف المتطلبات الأمنية ذات الصلة بالعملاء الذين يُتاح لهم الوصول إلى الأصول التنظيمية اختلافاً كبيراً اعتماداً على طبيعة مرافق معالجة المعلومات والمعلومات التي يتم الوصول إليها، أن هذه المتطلبات الأمنية يمكن معالجتها باستخدام اتفاقات العملاء التي تحتوي على كل المخاطر التي تم تحديدها والاحتياجات الأمنية (انظر أيضاً 1.2.6) .

يمكن أيضاً أن تنطوي الاتفاقات مع أطراف خارجية على أطراف أخرى. الاتفاقات التي تمنح الطرف الخارجي إمكانية الوصول إلى المعلومات ينبغي أن تشتمل على إجازة تعيين الأطراف الأخرى المؤهلة المرغوب فيها، والشروط اللازمة لإتاحة الوصول والمشاركة لهم.

3.2.6 معالجة القضايا الأمنية في الاتفاقات مع طرف ثالث

التحكم

إن الاتفاقات مع أطراف ثالثة، والتي تشتمل على الوصول إلى المعلومات، المعالجة، والتواصل أو إدارة معلومات المنظمة أو مرافق معالجة المعلومات، أو إضافة منتجات أو خدمات إلى مرافق معالجة المعلومات ينبغي أن تشمل جميع المتطلبات الأمنية ذات الصلة.

توجيهات التطبيق

يجب أن يضمن الاتفاق عدم وجود أي سوء تفاهم بين المنظمة والطرف الثالث. يجب أن تُرضى المنظمات نفسها بالتعويض الذي يقدمه الطرف الثالث.

ينبغي النظر في الشروط المرجعية التالية لإدراجها في الاتفاق للإيفاء بالاحتياجات الأمنية المحددة (انظر1.2.6):

أ) سـياسة أمن المعلومات .

ب) التحكمات اللازمة لضمان حماية الأصول وتشمل الآتي : -

1) إجراءات لحماية الأصول التنظيمية بما في ذلك المعلومات والبرمجيات ومجموعة الأجهزة.

2) أي تحكمات وآليات مطلوبة للحماية المادية لها.

3) تحكمات لضمان الحماية ضد البرمجيات الخبيثة (انظر1.4.10) .

4) إجراءات لتحديد ما إذا كان قد وقع تجاوز واختراق للإصول كمثال فقدان او تعديل المعلومات، او البرمجيات و العتاد.

5) تحكمات لضمان إسترجاع او تدمير المعلومات والأصول في نهاية الاتفاق أو في خلال وقت ما متفقاً عليه.

6) السـرية، النزاهة، المتاحية، وأية ممتلكات أخرى ذات صلة بالأصول الموجودة (انظر5.1.2)

7) فرض قيود على النسخ، والإفصاح عن المعلومات واستخدام اتفاقات السرية (انظر 5.1.6) .

ج) تدريب المستخدمين والمديرين على الأساليب ، الإجراءات والأمن .

د) ضمان التأكد من وعي المستخدم لمسؤوليات وقضايا أمن المعلومات .

هـ) نقل الموظفين، حسب الاقتضاء .

و) مسؤوليات تتعلق بتركيب الأجهزة والبرمجيات وصيانتها .

ز) هيكل واضح لتقديم التقارير وأشكال متفق عليها للتقارير.

ح) عملية واضحة ومحددة لإدارة التغيير .

ط) سياسة التحكم في الوصول وتشمل الآتي :-

1) الدواعي المختلفة، والاحتياجات، ومزايا الفوائد المكتسبة التي تجعل وصول الطرف الثالث لازماً

2) الطرق المتاحة للوصول إلى المعلومات، وأساليب التحكم فيها، واستخدام المؤشرات الفريدة لإثبات الهوية مثل بطاقة هوية المستخدم وكلمات السر.

3) عملية ترخيص وصول المستخدم إلى المعلومات، وتحديد امتيازاته.

4) توفير شروط الحفاظ على وجود لائحة بأسماء الأشخاص المرخص لهم باستخدام الخدمات المتاحة لهم، وماهية حقوقهم وامتيازاتهم فيما يتعلق بهذا الاستخدام.

5) الإعلان بان أي وصول غير مصرح له بوضوح سيمنع.

6) عملية إلغاء حقوق متاحية الوصول أو الإعاقة بقطع الاتصال بين النظم.

ي) ترتيبات التبليغ والإخطار والتحقيق في حوادث أمن المعلومات والمخالفات الأمنية، فضلاً عن انتهاكات المتطلبات المنصوصة عليها في الاتفاق.

ك) وصف للمنتج أو الخدمة التي ستُقدم، ووصف للمعلومات التي سوف تُتاح بإرفاق التصنيف الأمني لها (انظر 1.2.7) .

ل) المستوى المستهدف من الخدمة و المستويات غير المقبولة من الخدمات.

م) تعريف معايير الأداء الممكن التحقق منها، ومدى قابليتها للرصد، والإبلاغ عنها.

ن) الحق في مراقبة، وإلغاء أي نشاط يتعلق بأصول المنظمة.

س) الحق في مراجعة المسؤوليات المحددة في الاتفاق، وعلى أن تُنفّذ تلك المراجعات من قبل طرف ثالث، وعلى أن تُحسب تلك الحقوق القانونية لمراجعي الحسابات.

ع) إنشاء آلية تصاعدية لحل المشاكل.

ف) متطلبات استمرارية الخدمات بما في ذلك قياس توفرها، وموثوقيتها وفقاً لأولويات عمل المنظمة .

ص) احترام الأطراف المعنية للاتفاق.

ق) المسؤوليات ذات العلاقة بالمسائل القانونية، وكيف يتم التأكد من تلبية المتطلبات القانونية على سبيل المثال تشريعات حماية البيانات، وبخاصة عند الأخذ في الاعتبار بوجود النظم القانونية الوطنية المختلفة إذا كان الاتفاق يشمل التعاون مع منظمات بلدان أخرى (انظر أيضاً 1.15) .

ر) حقوق الملكية الفكرية وحقوق التأليف والنشر (انظر 2.1.15) وحماية أي عمل تعاوني (انظر أيضاً5.1.6)

ش) إشراك الطرف الثالث لمقاولين من الباطن في تنفيذ التعاقد، وتحديد التحكمات الأمنية التي ينبغي أن يُنفذها
المقاولون من الباطن.

ت) شروط إعادة التفاوض أو إنهاء الاتفاقات وهي تشمل : -

1) يجب وضع خطة الطوارئ في ترتيب الوضع المناسب في حالة أن كلا الطرفين المتعاقدين يرغبان في إنهاء العلاقة قبل نهاية فترة الاتفاقات .

2) إعادة التفاوض حول الاتفاقيات إذا تغيرت المتطلبات الأمنية للمنظمة.
(3) التوثيق الحالي لقوائم الأصول الموجودة، التراخيص، والاتفاقات أو الحقوق المتعلقة بها.

<u>معلومات أخـرى</u>

يمكن أن تختلف الاتفاقات المبرمة مع المنظمات المختلفة وحتى ما بين الأطراف الثالثة بأنواعها المختلفة اختلافاً كبيراً. ولذلك ينبغي توخي الحذر حتى تشمل الاتفاقات جميع المخاطر التي تم

التعرف عليها والمتطلبات الأمنية المحددة (انظر أيضاً 1.2.6). وحيثما كان ذلك ضرورياً يمكن توسيع التحكمات والإجراءات المطلوبة في خطة الإدارة الأمنية .

إذا كانت إدارة أمن المعلومات تعتمد على الاستعانة بمصادر خارجية، فإن الاتفاقات ينبغي أن تتناول كيفية محافظة الطرف الثالث على ضمان توفير الأمن الكافي مثلما حدده فصل تقييم المخاطر، وكذلك كيفية تكييف الأمن للتعرف على تحديد المخاطر والتعامل مع متغيرات المخاطر.

بعض الاختلافات المتضمنة في الاستعانة بمصادر خارجية بتخصيص العائدات لاقتطاع التكاليف وبين غيرها من أشكال توفير خدمات الطرف الثالث تشمل مسألة المسؤولية، وتنظيم الفترة الانتقالية، والعرقلة المحتملة للعمليات خلال هذه الفترة، وترتيبات التخطيط للطوارئ، واستعراض مستحقات النقل بالاجتهاد اللازم بعناية وجمع وإدارة المعلومات عن الحوادث الأمنية. لذا، فمن المهم أن تخطط وتزيد المنظمة مسألة الانتقال إلى ترتيبات الاستعانة بمصادر خارجية، وينبغي أن تمتلك المنظمة العمليات الملائمة في المكان المناسب لإدارة التغييرات، وإعادة التفاوض / إنهاء الاتفاقات.

يتعين النظر في إجراءات مواصلة المعالجة التجهيزية عند عقد الاتفاق لتجنب أي تأخير في ترتيب خدمات الاستبدال في حال أنه قد يصبح الطرف الثالث غير قادر على توفير خدماته.

قد تنطوي الاتفاقات مع أطراف ثالثة أيضاً على أطراف أخرى في التعاقد. الاتفاقات التي تمنح طرفاً ثالثاً متاحية الوصول إلى المعلومات ينبغي أن تشتمل على إجازة تعيين الأطراف الأخرى المؤهلة المرغوبة فيها، والشروط اللازمة لإتاحة الوصول إليها، والمشاركة التداولية لها.

عموماً، توضع الاتفاقات من قبل المنظمة في المقام الأول، وقد تكون هناك مناسبات في بعض الظروف التي يمكن أن يُوضع اتفاق من قبل طرف ثالث ثم يفرضه على المنظمة.تحتاج المنظمة ضماناً لأمنها للتوكيد بأن أمنها لا يتأثر بالضرورة مع متطلبات الطرف الثالث المنصوصة عليها في الاتفاقات المفروضة.

7 إدارة الوصول

1.7 المسئولية عن الأصول

الهدف: تحقيق والحفاظ على حماية مناسبة لأصول المنظمة.

يجب حصر كل الاصول وتسمية مالكين لها. كما يجب تحديد مسئولية صيانة التحكمات المناسبة. ان تطبيق تحكمات محددة ليس بالضرورة ان يتم بواسطة الشخص المالك لهذه التحكمات يمكن ان يتم التطبيق بتفويض مناسب من مالك التحكمات لشخص اخر مناسب ولكن تظل مسئولية المالك قائمة في حماية الاصول بشكل جيد.

1.1.7 جرد الأصول

التحكم

يجب تحديد كل الأصول بوضوح وإنشاء سجل لحفظ كل الأصول الهامة.

توجيهات التطبيق

يجب على المنظمة تحديد كافة الأصول وتوثيق الهام منها. كما يجب ان يحتوي سجل جرد الأصول على كل المعلومات الضرورية والتي تشمل نوع الأصل، شكله، موقعه، معلومات إعادة التشغيل، معلومات الترخيص وقيمته للعمل.

يجب ان لا يكرر سجل الجرد معلومات سجلات أخرى غير ضرورية ولكن يجب ان يضمن السجل صحة محتواه.

بالإضافة لذلك فإن قصايا التملك (انظر 2.1.7) وتصنيف المعلومات (انظر 2.7) يجب ان يتم الاتفاق حولها وتوثيقها لكل أصل من أصول المنظمة.

بناء على أهمية الأصل وقيمته للعمل وتصنيفه الأمني يجب ان يتم تحديد مستوى الحماية المناسب لأهمية الأصل.

معلومات أخرى

هنالك العديد من أنواع الأصول تشمل:

أ) المعلومات: قواعد البيانات وملفات البيانات، العثور، والاتفاقات، وثائق النظام معلومات البحث العلمي، دلائل المستخدمين، مواد التدريب، إجراءات الدعم والتشغيل، خطط استمرارية العمل، الترتيبات الاحتياطية، تقارير المراجعة والفحص والمعلومات المأرشفة.

ب) الأصول البرامجية: البرمجيات التطبيقية، برامجيات النظم، الأدوات المطورة والبرمجيات المساعدة.

ج) الأصول المادية: معدات الحاسوب، معدات الاتصال، الوسائط القابلة للحركة و اي معدات أخرى ذات صلة بنظم وخدمات المعلومات.

د) الخدمات: خدمات الحوسبة والاتصالات، الوسائط المساعدة العامة مثل التدفئة، الإضاءة، الطاقة والتبريد.

هـ) الإفراد ومؤهلاتهم وخبراتهم وتجاربهم.

و) أصول غير محسوسة مثل سمعة وصورة المنظمة.

إن عملية جرد الاصول تساعد في التيقن من ان هنالك حماية للأصول. كما إن عملية الجرد قد تكون مطلوبة لأغراض اخرى تتعلق بالعمل كالصحة والسلامة، التأمين ولأسباب مالية. إن اجراء عملية الجرد هو امر لازم ومطلوب قبل القيام بعملية إدارة المخاطر(انظر البند 4).

2.1.7 ملكية الأصول

التحكم

كل المعلومات والأصول المتصلة بمرافق معالجة المعلومات يجب ان تكون مملوكة لجزء محدد من المنظمة.

توجيهات التطبيق

يجب ان يكون مالك الأصل مسئولاً عن:

أ) التأكد من ان المعلومات والأصول المتعلقة بمرافق معالجة المعلومات قد تم تصنيفها بشكل مناسب وصحيح.

ب) تعريف قيود الوصول للمعلومات للأصول المخصصة المتصلة بمرافق معالجة المعلومات وتصنيفها ومراجعتها بشكل دوري آخذاً في الاعتبار سياسات التحكم في الوصول المطبقة.

إن الملكية يمكن ان تخصص للآتي:

أ) معالجة عمل.

ب) مجموعة معرفة من الأنشطة

ج) تطبيق او.

د) مجموعة معرفة من البيانات.

معلومات اخرى

إن المهام الروتينية يمكن تفويضها، كمثال فإن شخص ما قد يكلف من قبل المالك بالمتابعة ليوم لأحد الاصول ولكن تبقى المسئولية النهاية عن الاصل للمالك.

في نظم المعلومات الكبيرة والمعقدة فقد يكون من المفيد ان يتم تخصيص مجموعة من الأصول التي تعمل معاً لتوفير خدمة او وظيفة محددة. في هذه الحالة فإن مالك هذه الخدمة (الوظيفة) سيكون مسئولاً عن توفير وتوصيل هذه الخدمة بما في ذلك تشغيل الأصول التي توفر هذه الخدمة.

3.1.7 الاستخدام المقبول للاصول

التحكم

يجب ان يتم تحديد وتوثيق وتطبيق قواعد الاستخدام المقبول للمعلومات وللأصول المخصصة بمرافق معالجة المعلومات.

توجيهات التطبيق

يجب على كل الموظفين، المتعاقدين ومستخدمي الطرف الثالث إتباع قواعد الاستخدام المقبول للمعلومات وللأصول المخصصة لمرافق معالجة المعلومات والتي تشمل:

أ) قواعد إستخدام البريد الإلكتروني والإنترنت (انظر 8.10)

ب) إرشادات استخدام اجهزة الموبايل، خاصة الاستخدام خارج أسوار المنظمة (انظر 1.7.11).

على الإدارة المعنية ان توفر قواعد وموجهات محددة. كما يجب ان يكون الموظفين، المتعاقدين ومستخدمي الطرف الثالث الذين لديهم وصول لاصول المنظمة على وعي بحدود استخدامهم لمعلومات المنظمة وللأصول المخصصة لمرفق معالجة المعلومات وللموارد الاخرى. كما يجب ان يكونوا مسئولين عن استخداهم لاي مورد من موارد معالجة المعلومات وعن أي استخدام يقع تحت مسئوليتهم.

2.7 تصنيف المعلومات

الهدف: ضمان ان المعلومات تتلقى مستوى مناسباً من الحماية.
المعلومات يجب ان تكون مصنفة لتشير الى الحوجة والاولويات والدرجة المتوقعة من الحماية عند التعامل مع المعلومات.
المعلومات تختلف في درجات الحساسية والحرجية. قد تتطلب بعض المعلومات درجة اضافية من من الحماية او معاملة خاصة. منهجية لتصنيف المعلومات يجب ان تستخدم لتعريف مجموعة مناسبة من مستويات الحماية وربط الحوجة لقياسات معالجة خاصة.

1.2.7 إرشادات التصنيف

التحكم

المعلومات يجب ان تصنف من حيث قيمتها، المتطلبات القانونية، الحساسية، والحرجية للمنظمة.

توجيهات التطبيق

التصنيفات وما يرتبط بها من تحكمات لحماية المعلومات يجب ان تأخذ في الاعتبار احتياجات العمل للتشارك في المعلومات او تقيدها والتأثيرات على العمل المتعلقة بهذه الاحتياجات.

إرشادات التصنيف يجب ان تشمل إصلاحات التصنيف الأولى وإعادة التصنيف على مر الزمن. وفقاً لبعض سياسات الوصول للتحكم المحددة سلفاً.

يجب ان يكون من مسؤلية مالك الأصل تعريف تصنيفات الأصل (انظر 2.1.7)، ومراجعتها دورياً، والتأكد من تحديثها باستمرار وبالمستوى المناسب، كما يجب ان تأخذ عملية التصنيف في الاعتبار تأثير عملية التجميع الواردة في البند 2.7.10 والنظر الى عدد من طرق التصنيف والفوائد التي تجنى من استخدامها و تجنب الطرق بالغة التعقيد والتي قد تصبح مرهقة وغير اقتصادية. كما يجب توخي الحذر من تفسير مميزات التصنيف الموجودة على وثائق مؤسسات أخرى والتي يمكن ان يكون لها تعاريف مختلفة رغم استخدام نفس الاسم المميز..

معلومات أخرى

مستوى الحماية يمكن ان يقيم بتحليل السرية والتكاملية والتوفر واي متطلبات أمنية أخرى للمعلومات.

المعلومات غالبا ما تفقد حساسيتها او حرجيتها بعد فترة معينة من الزمن، على سبيل المثال عندما تكون المعلومات قد أصبحت عامة. هذه الجوانب يجب ان تؤخذ بعين الاعتبار، كما ان وجود تصنيفات كثيرة قد تؤدي الى تنفيذ تحكمات لا ضرورة لها مما يؤدي الى تكلفة إضافية.

النظر الى مجموعة الوثائق التي تحتاج لنفس المتطلبات الأمنية كوحدة واحدة عند تخصيص مستويات التصنيف قد يساعد في تسهيل عملية التصنيف.

2.2.7 التعامل مع المعلومات وتمييزها

التحكم

يجب تطوير وتطبيق مجموعة مناسبة من إجراءات تمييز وتناول المعلومات وفقاً لطريقة التصنيف المعتمدة من قبل المنظمة.

توجيهات التطبيق

إجراءات تمييز المعلومات يجب ان تغطي أصول المعلومات بأشكالها المادية والالكترونية .

إن مخرجات النظم التي تحتوي على معلومات مصنفة على انها حساسة تاو حرجة يجب ان تحمل مميز تصنيف مناسب (عند المخرجات) المميز يجب ان يعكس التصنيف بناء على القواعد المنشأة في البند 1.2.7.

العناصر التي تؤخذ بعين الاعتبار تشمل التقارير المطبوعة، عرض الشاشة، الوسائط المسجلة (مثل الأشرطة، والأقراص والأقراص المدمجة)، الرسائل الإلكترونية، ونقل الملفات.

لكل مستوى من مستويات التصنيف، يجب ان توجد معرفة للتعامل مع المعلومات تشمل المعالجة الآمنة، التخزين، النقل، إعادة التصنيف، والتدمير. الاتفاقات مع المنظمات الأخرى تشمل تبادل المعلومات ينبغي ان تشمل إجراءات لتحديد تصنيف تلك المعلومات وتفسير مميزات تصنيف المنظمات الأخرى.

معلومات أخرى

التمييز والتداول الآمن للمعلومات المصنفة هو مطلب رئيسي لترتيبات التشارك في المعلومات. المميزات المادية شكل شائع من أشكال التمييز. ومع ذلك، بعض أصول المعلومات، مثل الوثائق الالكترونية، لا يمكن تمييزها ماديا ولذلك يجب استخدام وسائل تمييز الكترونية كمثال يمكن استخدام مميزات تنبيه تظهر على الشاشة.

عندما يكون التمييز غير ذي جدوى يمكن استخدام وسائل أخرى لتخصيص تصنيف للمعلومات، كمثال عن طريق استخدام الإجراءات. على سبيل المثال، وصف الإشعارات التي قد تظهر في الشاشة او العرض عندما يكون غير ممكن وصفها، وغيرها من وسائل تعيين تصنيف المعلومات يمكن تطبيقها، على سبيل المثال عن طريق إجراءات أو البيانات الوصفية.

8 أمن الموارد

1.8 *قبل التوظيف*

الهدف: ضمان أن الموظفين والمتعاقدين ومستخدمي الطرف الثالث قد فهموا مسئولياتهم، وأنهـم مناسبون للأدوار المنوطة بهم، والحد من مخاطر السرقة ، الغش وإساءة استخدام المرافق. كما يجب أن يتم تناول مسئوليات الأمن قبل التوظيف في الوصف الوظيفي وفـي مهـام وشـروط الاستخدام. كل المرشحين للعمل والمتعاقدين ومستخدمي الأطراف الأخرى يجب أن يتم فرزهم بشكل مناسـب وخاصة للأعمال الحساسة. الموظفين والمتعاقدين ومستخدمي الطرف الثالث لمرافق معالجة المعلومات يجب أن يوقعوا علـى اتفاق حول مهامهم ومسئولياتهم الأمنية.

1.1.8 الأدوار والمسئوليات

<u>التحكم</u>

يجب أن يتم تعريف وتوثيق المهام والمسئوليات الأمنية للعاملين والمتعاقدين ومـستخدمي الطـرف الثالث، وفقاً لسياسة أمن المعلومات في المنظمة.

<u>توجيهات التطبيق</u>

يجب أن تشتمل مهام ومسئوليات الأمن المتطلبات اللازمة:

أ) لأن يتم التطبيق والتصرف وفقاً لسياسات أمن معلومات المنظمة (أنظر 5-1).

ب) لحماية الأصول من الوصول غير المصرح ، الكشف، التعديل، التدمير والتشويش.

ج) لتنفيذ معالجات أو أنشطة أمنية محددة.

د) لضمان أن المسئولية الفردية قد حددت للأفعال المتخذة.

و) لرفع تقرير عن الأحداث الأمنية أو الأحداث المؤثرة وغيرها من المخاطر الأمنية على المنظمة.

إن المسئوليات والمهام الأمنية يجب أن تعرف وأن توصل بوضوح للمرشحين للعمل في الفترة مـا قبل الاستخدام.

معلومات أخرى

يمكن استخدام الوصف الوظيفي لتوثيق المهام والمسئوليات الأمنية، إن المهام والمسئوليات الأمنيـة للأفراد خارج إطار توظيف المنظمة (كمثال التابعين لمنظمة طرف ثالث) يجب أن يـتم تحديـدهم بوضوح وإبلاغهم بمهامهم ومسئولياتهم الأمنية.

2.1.8 معاينات وفرز المترشحين

التحكم

يجب أن تتم اختبارات للتحقق من خلفية كافة المترشحين للعمل بالمنظمة، والمتعاقدين ومـستخدمي الطرف الثالث وفقاً للقوانين واللوائح ذات الصلة والأخلاق وبما يتناسـب مـع متطلبـات العمـل وتصنيف المعلومات المراد الوصول إليها والمخاطر المتوقعة.

توجيهات التطبيق

اختبارات التحقق ينبغي أن تأخذ في الاعتبار كل القوانين ذات الصلة بالخصوصية، حماية البيانـات الشخصية والاستخدام، ويجب أن تشمل الآتي:

أ) توفر مرجعيات شخصية كافية

ب) التأكد من اكتمال ودقة السيرة الذاتية للمتقدم.

ج) التوثق والتأكد من المؤهلات الأكاديمية والمهنية.

د) التحقق من الهوية (جواز سفر أو وثيقة)

هـ) التحقق من قضايا أخرى مثل الرصيد المصرفي والسجل الجنائي. إذا كانـت الوظيفـة سواء تعيين لأول مرة أو ترقيه ترتبط باستخدام الشخص لمرافق معالجة المعلومات وبشكل خـاص إذا كانت هذه المرافق تعالج بيانات حساسة، كالمعلومات المالية أو معلومات عالية الـسرية فعلـى المنظمة النظر في اختبارات تحقق إضافية وتفصيلية.

يجب أن تعرف إجراءات المنظمة قواعد وحدود اختبارات التحقق ، كمثـال مـن هـو الـشخص المسئول عن معاينات المترشحين للعمل، وكيف تتم المعاينات ومتى ولماذا تتم اختبارات التحقق.

إن عملية فرز المترشحين يجب أن تتم أيضا للمتعاقدين مع المنظمة ومستخدمي الطـرف الثالـث. عندما يتم تقديم المتعاقدين عبر وكالة فإن الاتفاق (التعاقد) مع الوكالة يجب أن ينص وبوضوح على مسئوليات الوكالة في عملية الفرز وإجراءات التبليغ التي يجب إتباعها إذا لم تتم عملية الفرز أو أن نتائج الفرز كانت سبباً للشك أو مثيرةً للاهتمام. على نفس النسق فإن الاتفاق مع الأطـراف الثالثـة (أنظر أيضا 3.2.6) يجب أن تحدد وبوضوح كافة المسئوليات وإجراءات التبليغ لعملية الفرز.

يجب أن تكون المعلومات المتعلقة بكافة المترشحين لوظائف بالمنظمة قد تم جمعهـا وتـداولها وفقاً للقوانين المناسبة السارية. اعتماداً على اللوائح المعمول بها يجب إخطار المترشحين للعمل في المنظمة مسبقاً بعمليات الفرز والمعاينات.

3.1.8 شروط و مهام الاستخدام

التحكم

كجزء من الالتزام التعاقدي يجب أن يقر ويوقع العاملين والمتعاقـدين ومـستخدمي الطـرف الثالث على عقود استخدام توضح شروط ومهام العمل ومسئولياتهم ومسئولية المنظمة تجاه أمن المعلومات.

توجيهات التطبيق

إن شروط الاستخدام يجب أن تعكس السياسة الأمنية للمنظمة وأن توضح وتنص على:

أ) أن على كافة العاملين ، المتعاقدين ومستخدمي الطرف الثالث الذين أعطوا حق الوصـول لمعلومات حساسة أن يوقعوا على اتفاق يلزمهم بالحفاظ على سـرية المعلومـات وعـدم كشفها وذلك قبل إعطاءهم حق الوصول لمرافق معالجة المعلومات.

ب) الحقوق والمسئوليات القانونية للعاملين ، والمتعاقدين وأي مستخدم آخر، كمثال فيمـا يتعلق بقوانين النسخ وتشريعات حماية البيانات(انظر أيضاً1.1.15 و 2.1.15).

ج) المسئوليات المتعلقة بتصنيف المعلومات وإدارة أصول المنظمة المتعلقة بنظم المعلومـات والخدمات التي يستخدمها العاملين والمتعاقدين والمستخدمين الآخرين (انظر ايضاً1.2.7 و 3.7.10).

د) مسئوليات العاملين والمتعاقدين ومستخدمي الطرف الثالث فيما يختص بتناول المعلومات الواصلة للمنظمة من شركات ومنظمات أخرى وجهات خارجية.

هـ) مسئوليات المنظمة تجاه تناول المعلومات الشخصية ، بما في ذلك المعلومات الشخصية الناشئة كنتيجة للعمل أو أثناء العمل في المنظمة .

و) المسئوليات التي يجب الإضطلاع بها خارج حدود المنظمة وخارج الدوام الرسمي ، كمثال لذلك عند مزاولة العمل بالمنزل(انظر أيضا 5.2.9 ، 1.7.11).

ز) الأفعال التي يجب اتخاذها في حالة تجاهل العامـل أو المتعاقـد أو مـستخدم الأطـراف الأخرى لمتطلبات أمن المنظمة . (انظر أيضا 3.2.8).

يجب على المنظمة التأكد من أن العاملين والمتعاقدين ومستخدمي الطرف الثالث موافقين علـى شروط العمل المتعلقة بأمن المعلومات والمناسب لطبيعة ومدى الوصول الممنوح لهم لأصـول المنظمة ذات الصلة بخدمات ونظم المعلومات.حيثما كان مناسباً، يجب الإبقاء على المسئوليات المضمنة في شروط العمل لفترة محددة بعد انتهاء الاستخدام.(أنظر أيضا 3.8).

معلومات أخرى

من الممكن استخدام مدونة سلوك لتغطى مسئوليات الموظف، المتعاقد، ومستخدم الطرف الثالث فيما يتصل بالسرية ، حماية البيانات، الأخلاق والاستخدام المناسب لمعدات ومرافق المنظمة ، فضلاً عن الممارسات الحسنة التي تتوقعها المنظمة. إن المتعاقد أو مستخدمي الطرف الثالث قد يكون مرتبطاً بمنظمة خارجية والتي بدورها ستكون مطالبة بالدخول في ترتيبات تعاقدية نيابةً عن الفرد المتعاقد.

2.8 خلال التوظيف

الهدف : ضمان أن الموظفين ، والمتعاقدين و مستخدمي الطرف الثالث على علم بقضايا ومهددات أمن المعلومات وبمسؤولياتهم، وإنهم مجهزون لدعم سياسة أمن المنظمة أثناء عملهم وأن المخاطر الناشئة عن الأخطاء البشرية قد تم تقليصها.

يجب أن يتم تعريف المسئوليات الإدارية لضمان أن الأمن قد طبق طوال فترة عمل الفرد في المنظمة.

يجب أن يتم توفير قدر مناسب من الوعي والتعليم والتدريب في إجراءات الأمن وفي الاستخدام السليم لمرافق معالجة المعلومات لكافة العاملين ، المتعاقدين، ومستخدمي الطرف الثالث لتقليل المخاطر الأمنية المحتملة، كما ينبغي إنشاء آلية رسمية للعقاب لمعالجة الخروقات الأمنية.

1.2.8 مسئوليات الإدارة

التحكم

يجب على الإدارة أن تطلب من الموظفين والمتعاقدين ومستخدمي الطرف الثالث تطبيق الأمن وفقاً للسياسات والإجراءات القائمة بالمنظمة.

توجيهات التطبيق

يجب أن تشمل مسئوليات الإدارة التأكد من أن الموظفين والمتعاقدين ومستخدمي الطرف الثالث:

أ) على دراية بمهامهم ومسئولياتهم الأمنية قبل التصريح لهم بالوصول للمعلومات الحساسة ونظم المعلومات.

ب) قد تم مدهم بإرشادات حول مهامهم داخل المنظمة .

ج) قد تم حثهم وتحفيزهم للإيفاء بالسياسة الأمنية للمنظمة.

د) أن لديهم قدر من الوعي بالأمن ذو الصلة بمهامهم ومسئولياتهم في المنظمة. (انظر أيضاً2.2.8)

هـ) أنهم ملتزمون بشروط ومهام العمل التي تشمل سياسة أمن معلومـات المنظمـة وطرق العمل الملائمة.

و) أنهم مستمرون في امتلاك الخبرات والتأهيل المناسب.

معلومات أخرى

إذا لم تتم توعية الموظفين والمتعاقدين ومستخدمي الطرف الثالث بمـسؤولياتهم الأمنيـة فقـد يتسببون في إحداث خسائر فادحة بالمنظمة، في المقابل فإن الأشخاص الواعين يتـسببون فـي حوادث أمن معلومات أقل.

إن الإدارة الضعيفة قد تتسبب في إحساس الأفراد بعدم فائدتهم مما يترتب عليه آثار أمنيـة سالبة على المنظمة كمثال فإن الإدارة الضعيفة قد تؤدي إلى عدم اهتمام العاملين بقضايا الأمن أو الاستخدام السيئ لأصول المنظمة.

2.2.8 أمن المعلومات الوعي ، التعليم، التدريب

التحكم

يجب أن يتلقى كافة العاملين بالمنظمة ، التدريب المناسب للوعي بأمن المعلومـات وأن يلمـوا بالتحديثات التي تدخل على سياسات وإجراءات المنظمة ذات العلاقة بمهامهم الوظيفية.

توجيهات التطبيق

يجب الشروع في تدريب العاملين للوعي بأمن المعلومات وتقديم السياسات الأمنية للمنظمة لهم قبل التصريح للعاملين بالوصول للمعلومات أو الخدمات.

التدريب المستمر يجب أن يشتمل على متطلبات الأمن، المسئوليات القانونية وضوابط العمـل وكذلك التدريب على الاستخدام الأمثل لمرافق معالجة المعلومات.

معلومات أخرى

الوعي بالأمن ، التعلم وأنشطة التدريب يجب أن تكون مناسبة وملائمة لواجبـات ومـسئوليات وخبرات الشخص ، كما يجب أن تشتمل على معلومات عن المهددات الأمنية والجهات التي يتم الاتصال بها للمشورة الأمنية والقنوات التي يجب إتباعها للإبلاغ عن حوادث أمن المعلومات. (انظر أيضاً 1.13).

إن التدريب مهم لرفع الوعي وجعل الأفراد قادرين على التعرف على المـشاكل والحـوادث الأمنية وكيفية الاستجابة لها وفقاً لمتطلبات عملهم.

3.2.8 عملية التأديب والعقاب

التحكم

يجب أن تكون هنالك عملية رسمية لعقاب العاملين الذين يرتكبون خروقات أمنية.

توجيهات التطبيق

يجب أن لا تبدأ عملية العقاب قبل التحقق من أن اختراق أمني قد حدث (انظر أيـضاً 3.2.13 جمع الأدلة)

يجب أن تضمن عملية التأديب الرسمية صحة وعدالة معاملة العاملين المشكوك في ارتكـابهم لتجاوزات أمنية كما ينبغي أن تأخذ عملية العقاب في الاعتبار عوامل مثـل طبيعـة وجـسامة التجاوز أو الخلل الأمني واثر ذلك على العمل ، وما إذا كان التجاوز هو الأول أم مكرر، وما إذا كان الشخص المسبب للخرق مدرب جيدا أم لا، كذلك يجب الأخذ في الاعتبار التـشريعات ذات العلاقة وعقود العمل وغيرها من العوامل ذات الصلة. في حالات سـوء الـسلوك الـشاذ للموظف تجاه الأمن ، يجب أن تسمح عملية العقاب بالإيقاف الفوري للموظف عن أداء عملـه وإيقاف صلاحيات وحقوق وصوله للمعلومات وإخراجه مباشرةً من موقع العمل إذا كان ذلـك ضرورياً.

معلومات أخرى:

ينبغي أن تستخدم عملية العقاب أيضاً كرادع لمنع الموظفين والمتعاقدين ومستخدمي الطـرف الثالث من انتهاك السياسات الأمنية والإجرائية للمنظمة ومن إحداث أي مخالفات أخرى.

3.8 إنهاء أو تغيير العمل

الهدف: ضمان أن إنهاء عمل الموظفين ، والمتعاقدين ومستخدمي الطرف الثالث في المنظمـة أو تغيير العمل يتم بطريقة منتظمة.
يجب أن تكون هنالك جهة مسئولة تضمن أن إنهاء عمل الموظـف أو المتعاقـد أو مـستخدم الطرف الثالث في المنظمة يتم بشكل منظم وأن كل المعدات التي يستخدمها قد تم اسـترجاعها وأن كافة صلاحيات وصوله للمعلومات قد أزيلت.
أن تغيير المسئوليات أو العمل يجب أن يتم إدارته بشكل مماثل لإنهاء العمل أو المسئولية، كما يجب أن تتم إدارة المسئولية أو العمل الجديد كما جاء في البند 1.8.

1.3.8 مسئوليات الإنهاء

التحكم

يجب أن يتم وبوضوح تعريف وتخصيص المسئوليات المتعلقة بإنهاء الخدمة أو تغيير الوظيفة.

توجيهات التطبيق

يجب أن تشتمل مسئوليات الإنهاء المتطلبات الأمنية المستمرة والمسئوليات القانونية والمسئوليات المضمنة في اتفاقات السرية (انظر 5.1.6) وشروط ومهام العمل (انظر 3.1.8) المستمرة لفترة أمنية محددة بعد إنهاء الخدمة.

أن المسئوليات والواجبات المستمرة بعد إنهاء الخدمة يجب أن تضمن قي عقود الموظف ،المتعاقد أو مستخدم الطرف الثالث.

إن التغيير في المسئوليات أو العمل يجب أن يدار بشكل مماثل لإنهاء العمل كما يجب.

معلومات أخرى

إن وظيفة الموارد البشرية بشكل عام هي المسئولية عن إنهاء عملية إنهاء التوظيف وتقوم بذلك بالعمل مع المدير المشرف على الشخص المنهي عمله لإدارة القضايا الأمنية في الإجراءات ذات الصلة.

في حالة الأشخاص المتعاقدين فإن مسئولية إنهاء العمل قد تقع على كاهل الوكالة المسئولة عن التعاقد وفي حالة المستخدمين من الطرف الثالث فإن المسئولية تقع على عاتق المنظمات التي يتبعون لها.

قد يكون من المهم إبلاغ الموظفين والمتعاملين ، المتعاقدين ومستخدمي الطرف الثالث بالتغيرات التي تطرأ على وظائف الأفراد وترتيبات العمل.

2.3.8 إعادة الأصول

التحكم

عند إنهاء العمل أو التعاقد أو الاتفاق فعلى كافة الموظفين ، والمتعاقدين ، ومستخدمي الطرف الثالث إعادة كافة الأصول التي بحوزتهم.

توجيهات التطبيق

إن عملية إنهاء الخدمة يجب أن تشمل إعادة كل البرامجيات، الوثائق والمعدات وممتلكات المنظمة الأخرى كأجهزة الموبايل والحواسيب المحمولة ، بطاقات الائتمان بطاقات الدخول والمعلومات المخزنة في وسائط اليكترونية.

في الحالات التي يكون فيه الموظف أو المتعاقد أو مستخدم الطرف الثالث قد قام بشراء الأجهزة التي يستخدمها من المنظمة أو أنه يستخدم أجهزته الشخصية، فيجب إتباع الإجراءات التي تضمن أن كافة المعلومات ذات الصلة بالمنظمة قد تم نقلها للمنظمة وتمت إزالتها من الأجهزة الشخصية.(أنظر أيضاً 10.7).

في الحالات التي يكون فيها الموظف أو المتعاقد أو مستخدم الطرف الثالث له معرفة بمعلومات مهمة ولازمة للعمليات الجارية داخل المنظمة فإن تلك المعلومات يجب توثيقها وتمليكها للمنظمة.

3.3.8 إزالة حق الوصول

التحكم

يجب إزالة حقوق الوصول للمعلومات ولمرافق معالجة المعلومات لأي عامل أو متعاقد أو مستخدم طرف ثالث عند إنهاء الخدمة أو التعاقد أو الاتفاق أو نتيجة لتغيرات في المنظمة.

توجيهات التطبيق

ويجب إعادة النظر في حقوق الوصول للأصول ذات الصلة بنظم وخدمات المعلومات للفرد عند إنهاء خدمته، وتحديد ما إذا كان من الضروري إزالة هذه الحقوق. تغيير طبيعة العمل يجب أن تنعكس في إزالة كافة صلاحيات الوصول غير المصرح بها للوظيفة الجديدة. إن الصلاحيات التي يجب إزالتها أو تعديلها تشمل الوصول الفيزيائي والمنطقي للمعلومات ولمرافق معالجة المعلومات ، استخدام المفاتيح، كروت تحديد الهوية وغيرها(انظر 4.2.11) أيضا يجب إزالة العاملين المنهي خدماتهم من أي وثائق تشير إلى إنهم أعضاء عاملين بالمنظمة.

إذا كان الموظف أو المتعاقد أو مستخدم الطرف الثالث المغادر للعمل بالمنظمة على علم بكلمات مرور لبعض الحسابات التي ستظل نشطة بعد مغادرته للمنظمة فيجب أن يتم تغيير كلمات المرور.

إن حقوق الوصول لأصول المعلومات ولمرافق معالجة المعلومات يجب أن تقلل أو تزال قبل إنهاء خدمة الموظف أو تغييره ، اعتماداً على عوامل تقييم المخاطر التالية:

أ) هل إنهاء الخدمة أو التغيير جاء نتيجة لمبادرة من الموظف أوالمتعاقد أو مستخدم الطرف الثالث، أم تم بمبادرة من الإدارة وما هي أسباب إنهاء الخدمة.

ب) المسئوليات المنوطة حالياً بالموظف المراد إنهاء خدماته.

ج) قيمة الأصول المتاح حالياً للموظف الوصول إليها.

معلومات أخرى

من الممكن في ظل ظروف خاصة أن يتم تخصيص حقوق الوصول على أساس الإتاحة لعـدد كبير من الأشخاص وليس للموظف المغادر للمنظمة فقط كمثال لذلك وجـود مجموعـة مـن الموظفين في مجموعة واحدة في مثل هذه الحالات فإن الأفراد المغادرين يجب إزالتهم من أي مجموعة ينتمون إليها وإخطار بقية العاملين المعنيين بعدم التشارك في المعلومات مع الشخص المغادر للمنظمة.

في حالة إنهاء الخدمة لشخص جاء من الإدارة فقد يتعمد بعض العاملين الساخطين على إنهـاء الخدمة تخريب المعلومات أو مرافق معالجة المعلومات.

9 الأمن المادي والبيئي

1.9 المناطـق الآمنـة

الهدف: هو منع الوصول المادي غير المرخص به، وتفادي إحداث الأضرار والتخريب لمباني ومعلومات المنظمة.
ينبغي إقامة مرافق معالجة المعلومات الحرجة أو الحساسة في المواقع المأمونة، وحمايتها بمحيط امن معرف، وذلك باستخدام الحواجز الأمنية الملائمة وتحكمات الدخول. ويجب أن تكون المرافق محمية مادياً من الدخول غير المصرح به والتخريب او الاختراق.

كما ينبغي أن تكون الحماية الموفرة متناسبة مع المخاطر المحددة.

1.1.9: الحماية المادية للمحيط

التحكم

يجب استخدام الحدود الأمنية للمحيط (على سبيل المثال استخدام الحواجز مثل: الجدران، وبوابات الدخول المتحكمة فيها ببطاقة الدخول، أو مكاتب الاستقبال المُدارة بالناس) لحماية المناطق التي تحتوي على المعلومات ومرافق معالجة المعلومات.

توجيهات التطبيق

يجب مراعاة تنفيذ المبادئ التوجيهية التالية عندما تكون مناسبة للحدود الأمنية.

أ) يجب تحديد الحدود الأمنية للمحيط بوضوح، علماً أن تموضع وقوة كل واحد من مكونات الحدود الأمنية للمحيط يعتمدان على الاحتياجات الأمنية للأصول في داخل الحد الأمني للمحيط ونتائج تقييم المخاطر.

ب) حدود محيط أي مبنى أو موقع يحتوى على مرافق معالجة المعلومات يجب أن تكون متينة مادياً (على سبيل المثال: لا ينبغي أن توجد ثغرات في المحيط أو مناطق قابلة للكسر للولوج عبرها بسهولة)، ويجب أن تكون الجدران الخارجية متينة البناء، وأن تكون كل الأبواب الخارجية محمية بشكل مناسب ضد الدخول غير المرخص به إستخدام بآليات تحكم مثل القضبان، وأجهزة الإنذار، والأقفال وغيرها، ويجب أن تكون الأبواب والشبابيك مغلقة في حالة عدم ارتياد العاملين للمبنى، ويتحتم وضع اعتبار للحماية الخارجية للشبابيك بخاصة نوافذ على مستوى الدور الأرضي.

ج) يجب أن تكون هنالك وسيلة لضبط الدخول الشخصي للموقع او المبنى كوجود استقبال او غيره من المرافق كما يجب ان يكون الدخول الى الموقع او المبنى قاصراً فقط على الأفراد المرخص لهم بالدخول.

د) يجب تشييد الحواجز العمرانية عند اقتضاء الضرورة لمنع الدخول غير المرخص به لمنع التلوث البيئي.

هـ) كل أبواب النار على المحيط الأمنى يجب أن تكون معدة ومراقبة وتم اختبارها مع الجدران للوصول للمستوى المطلوب من المقاومة وفقاً للمعايير الإقليمية والوطنية والعالمية المناسبة، كما يجب أن تعمل معايير الإطفاء وفقاً للقانون المحلي لإطفاء النار،بطريقة السقوط الآمن.

و) يجب تركيب النظم المناسبة لاكتشاف الدخلاء بتطبيق المعايير الوطنية أو الإقليمية أو الدولية وعلى أن يتم اختبارها بانتظام لكي تغطي مهام فحص كل الأبواب الخارجية، والنوافذ المتيحة للدخول ، ويجب أن تكون الأماكن غير المستخدمة خاضعة دائماً للمراقبه

وللتنبيه بالخطر، وينبغي أيضاً توفير التغطية الأمنية لتشمل المناطق الأخرى مثل غرفة الحواسيب الآلية أو غرف الاتصالات.

ز) مرافق مرافق معالجة المعلومات التي تديرها المنظمة يجب أن تكون منفصلة عمرانياً عن تلك المرافق التي تديرها أطراف ثالثة.

معلومات أخـرى

يمكن تحقيق الحماية المادية الفعلية بإنشاء حاجز عمراني مادي واحد أو عدة حواجز حول مباني وأرض المنظمة، وكذلك حول مرافق معالجة المعلومات. ويمنح استخدام حواجز متعددة حماية إضافية، بحيث لايترتب على إخفاق حاجز واحد تعرض الأمن للخطر.

من الممكن أن تكون المنطقة الأمنية عبارة عن مكتب قابل للإغلاق بإحكام أو عدة غرف محاطة بحاجز أمني عمراني داخلي متصل. ومن المرجح أن توجد حاجة إلي الحواجز الإضافية والحدود الأمنية للمحيط للتحكم في إتاحة الوصول المادي ما بين الأماكن ذات المتطلبات الأمنية المتنوعة في داخل الحد الأمني لمحيط المنطقة الأمنية.

يجب وضع اعتبار خاص تجاه الوصول المادي عبر المباني العمرانية بتوفير الأمن في حالة وجود منظمات عديدة مُقامة في تلك البقعة التي بها مباني المنظمة.

2.1.9 تحكمات الدخول الفيزيائي

التحكم

يجب ان تحمي المناطق الآمنة باستخدام تحكمات دخول مناسبة للتأكد من ان الافراد المرخص لهم فقط هم من سيسمح لهم بالدخول.

توجيهات التطبيق

ينبغي مراعاة التوجيهات التالية:

أ) يجب تسجيل تاريخ ووقت دخول وخروج الزوار، ويجب مراقبة كل الزوار ما لم يكن دخولهم قد تمت الموافقه عليه مسبقاً، على أن يُمنحوا إذن الدخول للأغراض المرخصة والمحددة، وعلى أن يكون الإذن الصادر مرفقاً بالتعليمات الإرشادية للاحتياجات الأمنية وإجراءات الطوارئ للمنطقة المعنية.

ب) يجب التحكم في متاحية الوصول إلي المرافق التي تتم فيها معالجة وتخزين المعلومات الحساسة، وعلى أن يقتصر الوصول إليها فقط على الأفراد المخولين لهم بالدخول، وتشمل تحكمات موثوقية الدخول كمثال: بطاقة ضبط الدخول، بالإضافة إلي رقم التعريف الشخصي الذي يجب استخدامه لترخيص وتفعيل سريان مفعول إذن الدخول بالكامل، وعلى أن يتم الاحتفاظ بأمان بدفتر رصد الدخول.

ج) يُطلب من جميع الموظفين العاملين، والمتعاقدين "المقاولين"، والمستخدمين الذين يعملون مع أطراف ثالثة، وكل الزوار ارتداء نوع معين من الزي للتعرف عليهم، ويجب عليهم إخطار أفراد الأمن إذا ما وجدوا زواراً غير مسجلين، أو أي شخص لا يرتدي علامة مميزة واضحة محددة لهويته.

د) يجب أن يُمنح الأفراد العاملين في مجال تقديم الخدمات التي يوفرها طرف ثالث إذن دخول مقيد إلي المناطق الآمنة أو مرافق معالجة المعلومات الحساسة فقط عند اقتضاء الضرورة، وينبغي أن يكون هذا الوصول مرخصاً به ومراقباً.

هـ) يستوجب الأمر مراجعة وتحديث حقوق الوصول إلي المناطق الآمنة بانتظام، وعلى أن تُلغى تلك الحقوق الممنوحة عند الضرورة. (انظر 8-3-3).

3.1.9 تأمين المكاتب والقاعات والمرافق

التحكم:

ينبغي تصميم وتطبيق الأمن المادي العمراني للمكاتب والغرف والمرافق.

توجيهات التطبيق

يجب مراعاة التوجيهات التالية لتأمين المكاتب والغرف والمرافق:

أ) يجب وضع اعتبار للوائح والمعايير المناسبة للصحة والسلامة.

ب) يجب تفادي وصول الجمهور للمرافق الرئيسية.

ج) متى ما كان ملائماً، يجب أن تكون المباني غير واضحة المعالم، وأن لا تشير إلا للحد الأدنى من مهام أغراضها، ويتحتم أن لا تُوضع أية علامات بارزة في داخل أو خارج المبنى، لتفادي وجود أي دلالة لأنشطة معالجة المعلومات.

د) كتب دليل الهاتف ودفاتر التلفونات الداخلية التي تحدد مواقع مرافق معالجة المعلومات الحساسة يجب ألا تكون متاحة للتداول من قبل الجمهور.

4.1.9 الحماية ضد التهديدات الخارجية والبيئية

التحكـ ـم

ينبغي تصميم وتطبيق الحماية المادية ضد الأضرار الناتجة من حرائق النيران والفيضانات ، والزلازل الأرضية، والانفجارات، وعدم الاستقرار الناتج عن الاضطرابات المدنية "الشغب" ، وغيرها من أشكال الكوارث الطبيعية أو التي تكون من صنع البشر.

توجيهـات التطبيق

يجب الأخذ في الاعتبار التهديدات الأمنية التي يمكن أن تنشأ من وجود منشآت مجاورة مثل اندلاع النيران في مبنى مجاور للمنظمة، أو تسرب المياه من سقوف أو من طوابق المباني تحت الأرض أو انفجار في الشارع.

ينبغي مراعاة التوجيهات التالية حتى يمكن تفادي الأضرار الناتجة عن حرائق النيران، أو الفيضانات، أو الزلازل الأرضية أو الانفجارات، والاضطرابات المدنية (الشغب)، وغيرها من أصناف الكوارث الطبيعية أو التي من صنع البشر

أ) المواد المحفوفة بالمخاطر و القابلة للاشتعال يجب تخزينها في مكان آمن بعيداً عن المنطقة الأمنية. وينبغي عدم تخزين الإمدادات السائبة غير المعبأة مثل القرطاسية والأدوات المكتبية في المنطقة المتاخمة للمنطقة الأمنية.

ب) المعدات الاحتياطية وتجهيزات مرافق الإعلام يجب وضعها على مسافة آمنة ومناسبة حتى يتسنى تجنب الأضرار الناجمة عن أي كارثة تؤثر على الموقع الرئيسي.

ج) ينبغي توفير المعدات المناسبة لإطفاء الحرائق، وعلى أن تُوضع في المكان الملائم.

5.1.9 العمل في المناطق الآمنـة

التحكم

يجب تصميم وتطبيق الحماية المادية والتوجيهات اللازمة لأداء العمل في المناطق الآمنة.

توجيهـات التطبيق

يجب مراعاة التوجيهات الآتية:

أ) ينبغي أن يكون الأفراد العاملين فقط على معرفة بوجود منطقة مأمونة أو أنشطة جارية في نطاق المنطقة الآمنة وان تكون معرفة كل منهم على قدر حاجة العمل.

ب) يجب تجنب أداء العمل غير الخاضع للإشراف في الأماكن الآمنة وذلك من اجل السلامة ومنع إتاحة الفرص للأنشطة الخبيثة.

ج) الأماكن غير المستخدمة في المناطق الآمنة ينبغي أن تكون مغلقة فعلياً بمتانة ملموسة، ويتحتم أن تخضع للفحص دورياً.

د) ينبغي ألا يُسمح بإدخال معدات التصوير الفوتوغرافي والفيديو، ومعدات بث واستقبال الصوت، وغيرها من معدات التسجيل مثل الكاميرات على أجهزة الموبايل إلي الموقع ما لم يكن هنالك تصريح بذلك.

تشتمل ترتيبات تنظيم العمل في مناطق آمنة على تحكمات للتحكم على العاملين، والمقاولين، ومستخدمي الطرف الثالث العاملين في المنطقة الآمنة بالإضافة إلي التحكم في الأنشطة المدارة في الموقع من قبل الأطراف الثالثة الأخرى.

6.1.9 الوصول المتاح للجمهور، وتسليم المواد ومناطق شحنها

التحكم

ينبغي التحكم في نقاط الدخول مثل أماكن التسليم والشحن وغيرها من النقاط التي يمكن أن يصل إليها الأشخاص غير المخول لهم الدخول إلي المباني والأراضي التابعة للمنظمة، كما يجب بقدر الإمكان أن تكون تلك النقاط معزولة عن مرافق معالجة المعلومات لتجنب الوصول غير المرخص به.

توجيهات التطبيق

يجب مراعاة التوجيهات التالية:

أ) ينبغي أن تكون متاحية الوصول إلي مناطق التسليم والشحن من خارج المبنى قاصرة فقط على لأفراد العاملين المحددين والمرخص لهم بالدخول إلي الموقع المعنى.

ب) يجب أن تكون منطقة التسليم والشحن مصممة بحيث يتم تفريغ الإمدادات دون إن يتمكن عمال الشحن من الوصول لأجزاء أخرى من المبنى.

ج) يجب أن تكون الأبواب الخارجية لمكان تسليم وتحميل الإمدادات مأمنة عندما تكون الأبواب الداخلية مفتوحة.

د) يجب فحص المواد الواردة ضد المهددات المحتملة (انظر 1.2.9.د) قبل نقلها من مكان التسليم والتحميل إلى مكان الاستلام.

هـ) يجب تسجيل المواد الواردة وفقاً لإجراءات إدارة الأصول الموجودة (أنظر أيضاً 1.1.7) عند إدخالها إلي الموقع.

و) يجب فصل شحنات المواد الواردة والصادرة الطبيعية كلما كان ذلك ممكناً.

2.9 *سلامة المعدات*

الهـدف: هو منع ضياع أو تلف أو سرقة أو تعرض الأصول للخطر وإعاقة أنشطة المنظمة. يجب حماية المعدات من المهددات الطبيعية المادية والبيئية. تكون حماية المعلومات ضرورية (خاصة المعدات المستخدمة خارج المقر الرئيسي، بالإضافة إلي حماية الممتلكات عند نقلها) لتقليص مخاطر الوصول غير المرخص به إلي المعلومات، وحمايتها كذلك ضد الضياع أو الإتلاف. كذلك يجب وضع اعتبار لمسألة وضع وإزالة المعدات، قد تكون هنالك حاجة إلي تحكمات خاصة ضد التهديدات المادية لحماية المرافق الداعمة مثل الإمداد الكهربائي والبنية التحتية للكوابل.

1.2.9 تحديد مواقع نصب المعدات وحمايتها

التحـكـم

يجب تحديد مواقع نصب المعدات وإحاطتها أو حمايتها لتقليص المخاطر الناجمة عن التهديدات البيئية والتعرض للأخطار وتقليل فرص إتاحة التوصل غير المرخص به.

توجيهات التطبيق

ينبغي مراعاة التوجيهات الآتية لحماية المعدات:

أ) يجب تحديد مواقع المعدات وإحاطتها لتقليص الدخول غير الضروري إلي أماكن العمل.

ب) يجب أن تكون مرافق معالجة المعلومات التي تتناول البيانات الحساسة فى مواقع تقيد زاوية النظر، وذلك للحد من مخاطر النظر للمعلومات من قبل أفراد غير مرخص لهم أثناء تكون إستخدامها، وتأمين مرافق التخزين ضد الوصول غير المصرح به.

ج) أصناف المواد التي تحتاج إلي حماية خاصة يجب عزلها لتخفيض المستوى العام من الحماية المطلوبة.

د) يجب تطبيق التحكمات لتقليل مخاطر التهديدات المادية المؤثرة (على سبيل المثال: السرقة، الحرائق، التفجيرات، الدخان، المياه (أو الفشل في توفير إمدادات المياه) ، الغبار، الارتجاج، التأثيرات الكيماوية، التداخل التعارضي لإمدادات الكهرباء، والتشويش التداخلي للاتصالات، والإشعاع الكهرومغناطيسي، وتخريب المرافق.

هـ) يجب إصدار التوجيهات الإرشادية في النواحي المتعلقة بالأكل والشرب والتدخين بالقرب من منشآت مرافق معالجة المعلومات.

و) يجب رصد الأحوال البيئية مثل درجة الحرارة والرطوبة، والتي يمكن أن تؤثرا سلباً على عملية تشغيل مرافق معالجة المعلومات.

ز) يستوجب تطبيق نظام حماية لكل المباني من صواعق البرق، وأن تُركب مرشحات الوقاية (موانع الصواعق) والحماية من صواعق البرق على كل أجهزة نقل الطاقة الداخلة إلي المباني وخطوط الاتصالات.

ح) يجب الاهتمام باستعمال أساليب الحماية الخاصة (مثل أغشية لوحة المفاتيح) للمعدات المستخدمة في البيئات الصناعية.

ط) يجب حماية المعدات المستخدمة في معالجة المعلومات الحساسة لتقليل مخاطر تسرب المعلومات نتيجة لانبعاثها من مصدرها.

2.2.9 المرافق الداعمة

التحكم

يجب حماية المعدات من انقطاع الطاقة ومن المشاكل الأخرى الناتجة عن فشل الأدوات والمرافق الداعمة.

توجيهات التطبيق

يجب أن تكون كل المرافق الداعمة مثل الكهرباء، وإمدادات المياه، والصرف الصحي، والتدفئة/ التهوية، وتكييف الهواء كافية ومناسبة لتشغيل النظم التي تدعمها. كما ينبغي فحص الرسائل الداعمة بانتظام، وأن يتم اختبارها بشكل مناسب لضمان أدائها لعملها بالصورة المناسبة، وحتى يتسنى تقليل حدوث أي مخاطر ناجمة عن سوء التشغيل أو القصور في الأداء. كما ينبغي توفير الإمداد الكهربائي الملائم الذي يتسق مع المواصفات التشغيلية التي يضعها صانع المعدات.

يُوصى بوجود جهاز إمداد غير متقطع للطاقة (UPS) للمعدات الداعمة لعمليات العمل الحرجة. يجب أن تغطي خطط توفير الطاقة للطوارئ ما يجب اتخاذه من أفعال في حالة حدوث خلل في جهاز الإمداد غير المتقطع للطاقة(UPS). يجب وضع اعتبار لتوفير مولد كهربائي احتياطي إذا كانت المعالجة العملية تتطلب الاستمرار في حالة حدوث انقطاع للكهرباء لفترة طويلة.كما ينبغي توفير الإمداد الكافئ من الوقود لضمان أن المولد الكهربائي يمكن أن يؤدي عمله لفترة ليست بقصيرة. أيضاً يجب فحص جهاز معدات الإمداد غير المتقطع للطاقة والمولدات الكهربائية بانتظام للتأكد من أنها تمتلك القدرة الكافية، وعلى أن تكون المعدات مفحوصة طبقاً لتوصيات الصانع.

بالإضافة لما ذكر يجب وضع اعتبار لاستعمال مصادر متعددة للطاقة أو في حالة اتساع الموقع يجب استخدام محطة فرعية منفصلة لتوفير الطاقة المطلوبة.

يجب تركيب محولات قطع الطاقة في حالة الطوارئ بالقرب من مخارج الطوارئ في غرف المعدات حتى يسهل إيقاف الطاقة بسرعة في حالة الطوارئ.كما يجب توفير إضاءة طواري في حالة حدوث عطل للمصدر الرئيسي للطاقة.

ايضاً يجب أن تكون إمدادات المياه مستقرة ومناسبة لتزويد معدات تكييف الهواء، والترطيب وأجهزة إطفاء الحرائق (إذا كانت مستخدمة).

حالات سوء تشغيل نظام التزويد بالمياه يمكن أن تسبب في إتلاف المعدات، أو منع إخماد الحرائق بفاعلية. يجب وضع تقدير لأهمية نظام الإنذار وتركيبه في منظومة المرافق المساندة لفحص واكتشاف أعطال حالات سوء أداء وظائف تشغيل المرافق إذا دعت الضرورة. ينبغي ايضاً ربط معدات الاتصالات السلكية واللاسلكية بمذود الخدمة على الاقل لتجاوز المشاكل الناتجة عن حدوث عطل في احد المسارين. يجب أن تكون خدمات الصوت مناسبة لتفي بالاحتياجات القانونية المحلية المتعلقة بالاتصالات الطوارئ.

معلومـات أخـرى

تشمل خيارات تحقيق استمرارية إمدادات الطاقة وجود مصادر متعددة للتغذية بالطاقة حتى يتسنى تجنب العجز الذي يمكن أن ينشأ عن توقف مصدر واحد للإمداد بالطاقة.

3.2.9 سلامة شبكة الكابلات

التحكم

يجب حماية الشبكة الناقلة للطاقة وشبكة الاتصالات الناقلة للبيانات أو الداعمة لخدمات المعلومات من الإيقاف أو التلف.

توجيهـات التطبيق

ينبغي مراعاة التوجيهات التالية لتأمين شبكة الكابلات:

أ. يجب أن تكون خطوط نقل الطاقة والاتصالات الموصلة إلي مرافـق معالجـة المعلومـات موضوعة تحت سطح الأرض إذا ما أمكن ذلك، أو تكون خاضعة لخيارات حماية بديلـة وافية.

ب. يجب حماية خطوط شبكة الكابلات من الاعتراض المعوق غير المرخص به أو الإتلاف، ويمكن أن تتم الحماية على سبيل المثال: باستعمال أنبوب وقائي للأسلاك أو تجنب مرور خطوط النقل عبر الأماكن العامة.

ج. كابلات الطاقة يجب أن تكون مفصولة عن كابلات الاتـصالات حتـى يتـسنى تجنـب التشويش.

د. يجب استخدام الكابلات المحددة المفروزة ووضع علامات مميزة على المعدات بوضـوح لتقليل أخطاء تداولها مثل الاستخدام الفجائي الخاطئ لكوابل الشبكة.

ه. يجب استخدام قائمة موثقة من المعالجات.

و. عند التعامل مع النظم الحساسة أو الحرجة يجب مراعاة إضافة تحكمات أخرى تشمل.

1- تركيب أنابيب واقية، أو إنشاء غرف محددة أو صناديق معينة قابلة للإغلاق عند مواقع التفتيش أو نقاط انتهاء التوصيلات.

2- استخدام مسارات توصيلات بديلة أو وسائط نقل لتوفير السلامة الأمنية الملائمة.

3- استعمال شبكة كابلات مصنوعة من الألياف المرئية بالعين.

4- استخدام هيكل حجاب كهرومغناطيسي واقي لحماية الكابلات.

5- تركيب أجهزة المسح للبحث عن أجهزة التصنت وإزالتها، واعتماد تطبيق نظام التفتيشات الطبيعية على العمران للتحقق من عدم وجود أجهزة تصنت غير مرخصة بها موصلة على الكابلات.

6- الدخول المتَحكم فيه بالنسبة للوصول إلي لوحات التوصيلات وغرف التحكم في الكابلات.

4.2.9 صيانة المعدات

<u>التحكم</u>

يجب حفظ وصيانة المعدات بشكل صحيح لضمان استمرارية التوفر والسلامة.

<u>توجيهات التطبيق</u>

يجب مراعاة التوجيهات الموجزة التالية عند صيانة المعدات:

أ. يجب صيانة المعدات وفقاً لمواصفات وفترات الخدمة الموصى بها من قبل المورد.

ب. يجب أن يُسمح فقط للطاقم المرخص له بإجراء الإصلاحات وتشغيل المعدات بـصيانة المعدات.

ج. ينبغي الاحتفاظ بسجلات لكل الأعطال المشكوك فيها، أو الأعطال الفعلية، وكل أعمال الصيانة الوقائية والتصليحية.

د. يجب تطبيق التحكمات الملائمة عند جدولة المعدات لإجراء الصيانة عليهـا، علـى أن يُراعى ما إذا كانت الصيانة ينجزها أفراد طاقم في داخل موقع المنظمة أو في خارجها، وعند اقتضاء الضرورة ينبغي إزالة المعلومات الحساسة من متن المعدات، أو أن يكون أفراد طاقم صيانة المعدات موثوق بهم بصورة كافية.

ه. ينبغي الإذعان لجميع المتطلبات التي تفرضها سياسات التأمين باتساق تام.

5.2.9 أمن سلامة المعدات خارج المباني

التحكـم:

يجب تطبيق أمن المعدات خارج المنظمة بالأخذ في الاعتبار المخاطر المختلفة الناتجة عن العمل خارج مقر مباني المنظمة.

توجيهـات التطبيق

بغض النظر عن الملكية، فإن استخدام معدات معالجة المعلومات في خارج مواقع المنظمـة يجب الترخيص له من قبل إدارة المنظمة. وينبغي مراعاة التوجيهات التالية لحماية المعـدات التـي تُستعمل في خارج مقر المنظمة:

أ. يستوجب الأمر بألاّ تُترك المعدات ومرافق العمل التي يتم نقلها خارج مقر المنظمـة فـي الأماكن العامة بدون مراقبة، وينبغي حمل الحواسيب المحمولة وكأنها متـاع محمولـة باليد، ويفضل أن تكون مغطّاة عند نقلها أثناء السفر إذا ما أمكن ذلك.

ب. ينبغي مراعاة تعليمات الصانعين لحماية المعدات في كل الأوقات خاصة الحماية ضـد التعرض للمجالات الكهرومغناطيسية القوية.

ج. يجب تحديد تحكمات التحكم المنزلي عبر تقييم المخاطر والتطبيق الملائـم للتحكمـات المناسبة على سبيل المثال: استعمال الخزائن المغلقة للملفات، والسياسة الواضحة لإدارة المكاتب وتحكمات للتحكم في الوصول إلي الحاسبات الآلية، وتوفير الاتصالات الآمنـة مع المكتب الرئيسي (انظر أيضاً أمن الشبكة ISO/IEC18028)

د. توفير التغطية التأمينية الكافية لحماية المعدات الموجودة خارج مقر المنظمة، وينبغـي مراعاة المخاطر الأمنية، مثلاً: أضرار الإتلاف، والسرقة أو التصنت، التي يمكـن أن تختلف في المقدار ما بين المواقع المختلفة، ويتحتم أن تُتخذ أهم التحكمـات الملائمـة لتحديدها.

معلومـات أخـ ـرى:

تشمل عملية تخزين المعلومات ومعدات معالجتها على جميع أنواع الحواسيب الشخـصية، والآلات الدقيقة المنظمة والهواتف النقّالة، والبطاقات الذكية والأوراق، وغيرها من أشكال الوسائط التي يمكن استخدامها في أداء عمل الواجب المنزلي أو التي يمكن نقلها بعيداً عـن موقـع العمـل العادي.

ويمكن الحصول على مزيد من المعلومات في النواحي الأخرى المتعلقة بحمايـة المعـدات القابلة للنقل في الفقرة (11-7-1).

6.2.9 التخلص المأمون من المعدات أو إعادة استخدامها

التحكم:

ينبغي فحص جميع المعدات التي تحتوي على وسائط التخزين لضمان أن أيـة البيانـات الحـساسة والبرمجيات المرخص بها قد تمت إزالتها، تمت تغطيتها بامان قبل التخلص منها.

توجيهـات التطبيق

يجب تدمير الأجهزة المحتوية على معلومات حساسة، أو أن يتم توفير المعلومات الموجودة بها بمحوها، أو إعادة كتابتها باستخدام تقنيات تجعل استرجاع المعلومـات الأصـلية غيـر قابلـة للاسترجاع ويجب ان لا تستخدم الطرق العادية في المسح وتهيئة الاقراص.

معلـومـات أخـرى:

يمكن أن تحتاج الأجهزة المتعطلة المحتوية على بيانات حساسة إلي عملية تقييم للمخـاطر لتحديد، ما إذا كانت أصناف تلك المعدات يجب تدميرها فعلياً بدلاً عن أن تُرسل إلي ورشة التصليح لإعادة إصلاحها أو التخلص منها. ويمكن ان تتعرض المعلومات للخطـر مـن خـلال الـتخلص المحفوف بالإهمال أو عبر إتاحة فرصة لإعادة استخدامها (انظر أيضاً10-7-2).

7.2.9 نقل الممتلكـات

التحكم

يجب أن لا تُؤخذ المعدات والوسائط الحاوية للمعلومات أو البرمجيات خارج موقع المنظمة إلا بإذن صادر مسبقاً.

توجيهـ ـات التطبيق

يجب مراعاة التوجيهات التالية:

أ. يجب ان لا يتم أخذ المعدات والوسائط المحتوية للمعلومات أو البرمجيـات خـارج موقـع المنظمة إلاّ بترخيص صادر مسبقاً.

ب. العاملون والمقاولون، ومستخدمو الطرف الثالث الذين يُمنحون إذن تفويض نقل الممتلكـات من مقر المنظمة يجب تحديدهم بوضوح.

ج. ينبغي وضع حدود زمنية لنقل المعدات خارج المقر والتدقيق في الفترة الزمنية لإرجاعها لتتوافق مع اللوائح التنظيمية.

د. عندما يكون ضرورياً ومناسباً، يجب تسجيل المعدات عند نقلها خارج مقر المنظمة، وكذلك تسجيلها عند إعادتها إلي.

معلومات أخرى:

يجب إنشاء نقاط تفتيش للتحقق من النقل غير المرخص به للممتلكات، ويمكن أن تشمل نقاط التفتيش البحث عن أجهزة التسجيل غير المرخص بها، والأسلحة وغيرها، ومنع إدخالها إلي الموقع، على أن تنشأ مثل هذه النقاط التفتيشية وفقاً للتشريعات واللوائح التنظيمية ذات العلاقة، يجب إخطار الأفراد العاملين بوجود نقاط التفتيش، وأن عملية التفتيش ستتم بناء على تخويل يتناسب مع المتطلبات القانونية والتنظيمية.

10 إدارة العمليات والاتصالات

1.10 الإجراءات التشغيلية والمسؤوليات

الهدف: ضمان التنفيذ الصحيح وتأمين مرافق معالجة المعلومات.
المسؤوليات والإجراءات اللازمة لإدارة وتشغيل جميع تجهيز المعلومات وينبغي أن تكون مرافق المنشأة. وهذا يشمل وضع إجراءات التشغيل المناسبة. ينبغي الفصل بين واجبات يتم تنفيذها، حسب الاقتضاء، للحد من مخاطر إهمال أو تعمد إساءة استخدام النظام.

1.1.10 إجراءات التشغيل الموثقة

التحكم

ينبغي أن تكون إجراءات التشغيل موثقة، وإتاحتها لجميع المستخدمين الذين يحتاجون إليها.

توجيهات التطبيق

وينبغي أن الإجراءات الموثقة تكون مستعدة للأنشطة المرتبطة بنظام المعلومات تجهيـز ومرافـق الاتصالات، مثل تشغيل الحاسب الآلي وثيق بانخفاض الإجراءات، والنسخ الاحتيـاطي، وصـيانة المعدات، والتعامل مع وسائل الإعلام، وقاعة حاسوب والبريد التعامل مع الإدارة، والسلامة.
وإجراءات التشغيل وينبغي أن تحدد تعليمات مفصلة لتنفيذ كل مهمة بما في ذلك:

ا) تجهيز ومعالجة المعلومات؛

ب) احتياطية (انظر 10.5)؛

ج) جدولة الاحتياجات ، بما في ذلك الترابط مع النظم الأخرى ،بدء العمل في أقرب وقت وآخر مرة إنجاز المهمة؛

د) تعليمات لمعالجة الأخطاء أو غيرها من الظروف الاستثنائية التي قد تنشأ أثناء وظيفة التنفيذ ، بما في ذلك القيود المفروضـة على استخـدام الأدوات المساعـدة للنظـام (انظر 11.5.4)؛

هـ) دعم الاتصالات في حالة حدوث صعوبات غير متوقعة التشغيلية أو التقنية ؛

و) إنتاج وسائل الإعلام الخاصة والتعامل مع تعليمات ، مثل استخدام قرطاسية خاصـة أو إدارة الإنتاج سرية بما في ذلك الإجراءات اللازمة لضمان التخلص من الناتج مـن فـشل وظيفـة (انظر 10.7.2 و10.7.3) ؛

ز) إعادة تشغيل نظام وإجراءات الاسترداد للاستخدام في حال فشل النظام ؛إدارة مراجعـة الحسابات،ودرب نظام تسجيل المعلومات (انظر 10.10).

وينبغي أن إجراءات التشغيل ،وإجراءات موثقة لأنشطة النظام، أن تعامل على أنها وثائق رسمية والتغييرات التي أذن بها الإدارة. حيث ممكنة من الناحية التقنية ، ينبغي أن تدار نظم المعلومات باستمرار ، وذلك باستخدام نفس الإجراءات ، والأدوات ، والمرافق العامة.

2.1.10 إدارة التغيير

التحكم

تغييرات في مرافق المعالجة ونظم المعلومات يجب السيطرة عليه.

توجيهات التطبيق

نظم التشغيل وبرامج التطبيقات ينبغي أن تخضع لرقابة صارمة لإدارة التغيير.

أ) تحديد وتسجيل التغييرات الهامة ؛

ب) التخطيط واختبار التغييرات ؛

ج) تقييم الآثار المحتملة ، بما في ذلك الآثار الأمنية ، من مثل هذه التغييرات ؛

د) موافقة رسمية لإجراء التغييرات المقترحة ؛

هـ) الاتصال عن تفاصيل التغيير لجميع الأشخاص ذوي الصلة؛

و) إجراءات احتياطية ، بما في ذلك الإجراءات والمسؤوليات للإجهاض ويتعافى من التغييرات غير ناجحة، والأحداث غير المتوقعة.

المسؤوليات الإدارية والإجراءات الرسمية ينبغي أن يكون في مكان لضمان السيطرة مرضية لجميع التغييرات في المعدات والبرمجيات أو الإجراءات. عند إجراء تغييرات، ومراجعة سجل يحتوي على جميع المعلومات ذات الصلة ينبغي الاحتفاظ بها.

معلومات أخرى

يخضع لمراقبة كافية من التغييرات على تجهيز المرافق ونظم المعلومات هو من الأسباب الـشائعة لفشل النظام أو الأمن. التغييرات في البيئة التشغيلية ، وخاصة عند نقل نظام من التنمية إلى المرحلة التشغيلية ، يمكن أن تؤثر على موثوقية للتطبيقات (انظر أيضا 12.5.1).

وينبغي أن التغييرات في النظم التشغيلية يتم فقط عندما يكون هناك سبب والأعمال صالحة للقيـام بذلك ، مثل زيادة في المخاطر التي يتعرض لها النظام. تحديث نظم مع أحدث الإصدارات من نظام التشغيل أو التطبيق ليست دائما في مصلحة العمل لأن هذا لا يمكن تقديم المزيد من الضعف وعـدم الاستقرار من الإصدار الحالي. وقد تكون هناك أيضا حاجـة إلـى تـدريب إضـافي ، وتكـاليف الترخيص ، ودعم وصيانة وإدارة النفقات العامة ، والأجهزة الجديدة لا سيما خلال الهجرة.

3.1.10 فصل الواجبات

التحكم

واجبات ومجالات المسؤولية ينبغي أن تكون منفصلة للحد من فرص التعديل غير المصرح بـه أو غير مقصود أو إساءة استخدام أصول المنظمة.

توجيهات التطبيق

الفصل بين الواجبات هو وسيلة للحد من خطر عرضي أو متعمد إساءة اسـتخدام النظـام. ينبغـي الحرص على عدم تعرض أي شخص واحد يمكن الوصول إليها أو تعديلها أو استخدام الموجـودات دون إذن أو الكشف عنها. وينبغي الشروع في هذا الحدث يمكن فصلها عن التصريح بها. احتمـال وجود تواطؤ وينبغي النظر في وضع الضوابط.

المنظمات الصغيرة قد تجد من الصعب الفصل بين الواجبات لتحقيق ، ولكن المبدأ ينبغي أن يطبـق بقدر ما هو ممكن وعملي. كلما كان من الصعب عزل ، ينبغي النظر في عناصر أخرى مثل رصد الأنشطة ، فإن سجلات التدقيق والرقابة الإدارية أن تكون. فمن المهم أن المراجعة الأمنية لا تـزال مستقلة.

4.1.10 الفصل بين التنمية، والاختبار، والتسهيلات التنفيذية

التحكم

التنمية، والاختبار، ومرافق التشغيل وينبغي فصل للحد من مخاطر الدخول غير المـصرح بـه أو إجراء تغييرات على نظام التشغيل.

توجيهات التطبيق

على مستوى الفصل بين الاختبار العملي، وبيئات تطوير ما هو ضروري لمنع المشاكل التـشغيلية ينبغي تحديد الضوابط المناسبة وتنفيذها.

على وجه الخصوص، ينبغي النظر في البنود الآتية:

أ) ينبغي على القواعد لنقل البرامج من التنمية إلى الوضع التشغيلي يمكن تعريفها وتوثيقها؛

ب) وضع البرامج التنفيذية وينبغي أن تعمل على أنظمة مختلفة أو الكمبيوتر والمعالجـات في مختلف المجالات أو الدلائل؛

ج) المجمعين، والمحررين، وتطوير الأدوات أو غيرها من المرافق ينبغي ألا يكون النظـام يمكن الوصول إليها من النظم التشغيلية عندما لا تكون مطلوبة؛

د) لاختبار نظام البيئة ينبغي أن تحاكي بيئة نظام التشغيل وإلى أقصى حد ممكن؛

هـ) يجب أن المستخدمين استخدام التشكيلات الجانبية للمستخدم مختلفة لنظم التشغيل والاختبار، وينبغي أن القوائم عرض الرسائل الهوية المناسبة للحد من احتمالات الخطأ؛

و) البيانات الحساسة لا ينبغي أن يتم نسخها في نظام اختبار البيئة (انظر 12.4.2).

معلومات أخرى

تطوير واختبار أنشطة يمكن أن يسبب مشاكل خطيرة، على سبيل المثال التعديل غير مرغوب فيها من ملفات النظام أو البيئة، أو تعطل النظام. في هذه الحالة، هناك حاجة للحفاظ على بيئة مستقرة والمعروفة التي لأداء الاختبار مجدية وغير ملائمة لمنع وصول المطور.

حيث تطوير واختبار الموظفين من الوصول إلى نظام التشغيل والمعلومات، وأنها قد تكون قادرة على إدخال رمز غير المصرح بها والتي لم تختبر أو تغيير البيانات التشغيلية. على بعض أنظمة هذه القدرة يمكن استغلالها لارتكاب الغش، أو إدخال الرمز لم تختبر أو الخبيثة، التي يمكن أن تسبب مشاكل خطيرة في العملية.

والمطورين واختبار أيضا تشكل خطرا على سرية المعلومات التشغيلية.
تطوير واختبار الأنشطة قد يسبب تغييرات غير مقصودة لبرامج أو معلومات إذا كانت تشترك في نفس بيئة الحوسبة. فصل التنمية، والاختبار، ومرافق التشغيل وبالتالي مرغوب فيه للحد من مخاطر تغير العرضي أو الدخول غير المصرح به إلى البرامج التشغيلية والبيانات التجارية (انظر أيضا 12.4.2 لحماية بيانات الاختبار).

2.10 *الطرف الثالث تقديم الخدمات الإدارية*

الهدف : من أجل تنفيذ والحفاظ على مستوى مناسب من أمن المعلومات والخدمات التسليم وفقا للاتفاقات خدمة لطرف ثالث التسليم.
ينبغي للمنظمة أن تحقق من تنفيذ الاتفاقات، ورصد الامتثال لاتفاقات التغييرات وإدارتها لضمان أن الخدمات التي تستوفي جميع الشروط المتفق عليها مع طرف ثالث.

1.2.10 تقديم الخدمة

التحكم

وينبغي التأكد من أن الضوابط الأمنية وتعريفات الخدمات ومستويات الأداء المدرجة في خدمة لاطرف ثالث تسليم اتفاق يتم تنفيذها وتشغيلها، وصيانتها من قبل طرف ثالث.

توجيهات التطبيق

تقديم الخدمات من قبل طرف ثالث وينبغي أن تشمل الترتيبات الأمنية المتفق عليهـا، والتعـاريف الخدمة، والجوانب المتعلقة بإدارة الخدمات. في حالة ترتيبات الاستعانة بمصادر خارجيـة، ينبغـي للمنظمة خطة التحولات الضرورية (للمعلومات، ومرافق معالجة المعلومات، وأي شيء آخر لا بـد من تحرك)، وينبغي أن تكفل الحفاظ على الأمن طوال الفترة الانتقالية.

المنظمة ينبغي أن تكفل طرف ثالث يحتفظ بقدرة كافية الخدمة معامع خطط عملية تهدف إلى ضمان مستوى الخدمة المتفق عليها هي المحافظة على استمرارية الخدمـة الرئيـسية التاليـة الفـشل أو الكوارث (انظر 14.1).

2.2.10 رصد واستعراض خدمات طرف ثالث

التحكم

وينبغي للخدمات ، والتقارير والمحاضر المقدمة من طرف ثالث يتم رصدها بانتظام و ينبغي إعادة النظر والمراجعة تتم بصورة منتظمة.

توجيهات التطبيق

رصد واستعراض خدمات طرف ثالث يجب التأكد من أن المعلومات حيث الظروف الأمنية والاتفاقات التي يجري التمسك بها، وهذه المعلومات والحوادث الأمنية
المشاكل التي تدار بشكل صحيح. هذا ينبغي أن ينطوي على خدمة إدارة العلاقة وعملية بين المنظمة والطرف الثالث بما يلي :

أ) خدمة مراقبة مستويات الأداء للتحقق من الامتثال للاتفاقات ؛

ب) استعراض التقارير الخدمات التي ينتجها طرف ثالث وترتيب اجتماعات منتظمة للتقدم المحرز على النحو المنصوص عليه في اتفاقات ؛

ج) تقديم معلومات عن وقوع حوادث أمنية المعلومات واستعراض هذه المعلومات من جانب طرف ثالث والمنظمة على النحو المنصوص عليه في اتفاقات وأي دعم المبادئ التوجيهية والإجراءات ؛

د) استعراض طرف ثالث مسارات مراجعة الحسابات والسجلات من الأحداث الأمنية والمشاكل التشغيل الفشل والبحث عن المفقودين من العيوب والاختلالات المتصلة الخدمة المقدمة؛

هـ) وإدارة أي حل المشاكل التي تم تحديدها.

وينبغي أن مسؤولية إدارة العلاقة مع طرف ثالث يكون تعيينه لفرد معين أو خدمة إدارة الفريق. بالإضافة إلى ذلك ، ينبغي على المنظمة أن تضمن للطرف الثالث يسند مسؤوليات للتدقيق وإنفاذ الامتثال لمتطلبات هذه الاتفاقات. ينبغي كافية المهارات التقنية والموارد المتاحة لرصد تلك الاحتياجات للاتفاق (انظر 6.2.3)،وبخاصة متطلبات أمن المعلومات ، ويجري الحد. وينبغي أن يتخذ إجراء عندما أوجه القصور في تقديم الخدمات ويلاحظ وجود.

ينبغي للمنظمة الحفاظ على ما يكفي من السيطرة الشاملة والوضوح في جميع الجوانب الأمنية للحصول على معلومات حساسة أو حرجة أو الوصول إلى مرافق معالجة المعلومات ، وتجهيزها ، أو تدار من قبل طرف ثالث. المنظمة ينبغي أن تضمن أنها تحتفظ الرؤية في الأنشطة الأمنية مثل إدارة التغيير ، وتحديد مواطن الضعف ، والمعلومات الإبلاغ عن الحوادث الأمنية / استجابة محددة بوضوح من خلال عملية تقديم التقارير وشكلها وبنيتها.

معلومات أخرى

في حالة الاستعانة بمصادر خارجية، يجب على المنظمة أن تدرك أن المسؤولية النهائية عن المعلومات التي تتم معالجتها من قبل طرف الاستعانة بمصادر خارجية لا تزال مع المنظمة.

3.2.10 إدارة التغييرات في خدمات طرف ثالث

التحكم

تغييرات على توفير الخدمات، بما في ذلك صيانة وتحسين المعلومات المتاحة السياسات الأمنية والإجراءات والضوابط ، وينبغي أن تدار، آخذة في الاعتبار حساسية نظم الأعمال والعمليات التي تنطوي عليها، وإعادة تقييم المخاطر.

توجيهات التطبيق

عملية إدارة التغييرات في خدمة طرف ثالث يجب أن يأخذ في الاعتبار:

أ) التغييرات التي أجرتها المنظمة على تنفيذ ما يلي :

1) إدخال تحسينات على الخدمات الحالية المقدمة ؛

2) تطوير أي تطبيقات ونظم جديدة ؛

3) تعديلات أو تحديثات لسياسات المنظمة وإجراءاتها ؛

4) ضوابط جديدة لتسوية الحوادث الأمنية والمعلومات لتحسين الوضع الأمني ؛

ب) حدوث تغييرات في خدمات طرف ثالث لتنفيذ :

1) التغيرات وتعزيز الشبكات ؛

2) استخدام التكنولوجيات الجديدة ؛

3) اعتماد منتجات جديدة أو أحدث إصدارات / النشرات ؛

4) أدوات جديدة للتنمية والبيئة ؛

5) إدخال تغييرات على الموقع الجغرافي للمرافق الخدمات ؛

6) تغير من الباعة.

3.10 نظام التخطيط والقبول

الهدف: للتقليل من مخاطر فشل النظم.
التخطيط المسبق والإعداد المطلوبة لضمان توافر القدرة الكافية والموارد المطلوبة لتقديم أداء النظام. وينبغي أن التوقعات المستقبلية للاحتياجات القدرة التي يمكن، للحد من مخاطر النظام الزائد.
وينبغي أن الاحتياجات التشغيلية لنظم جديدة ستنشأ، موثقة، واختبارها قبل قبولها واستخدامها.

1.3.10 إدارة بناء القدرات

<u>التحكم</u>

وينبغي استخدام الموارد سيتم رصدها، وضبطها، والإسقاطات التي وضعت من القدرات في المستقبل

المتطلبات اللازمة لضمان أداء النظام.

توجيهات التطبيق

لكل نشاط من الأنشطة الجديدة والجارية، ينبغي تحديد الاحتياجات من القدرات. نظام ضبط ومراقبة ينبغي تطبيقها لضمان، وعند الاقتضاء، تحسين توافر وكفاءة النظم. وينبغي أن يكون المخبر الضوابط التي وضعت لتشير إلى مشاكل في الوقت المناسب. إسقاطات الاحتياجات من القدرات في المستقبل ينبغي أن تأخذ في الاعتبار الأعمال الجديدة، ومتطلبات النظام والاتجاهات الحالية والمتوقعة في قدرات المنظمة على معالجة المعلومات.

وأولي اهتمام خاص يحتاج إلى أن يدفع إلى أية موارد لأوقات طويلة، أو أن يؤدي ارتفاع تكاليف عمليات الشراء، وبالتالي ينبغي لمديري مراقبة استخدام الموارد الرئيسية للنظام. وينبغي تحديد الاتجاهات في الاستخدام، وخاصة فيما يتعلق تطبيقات الأعمال أو أدوات نظام إدارة المعلومات.

وينبغي لمديري استخدام هذه المعلومات لتحديد وتجنب الاختناقات المحتملة والاعتماد على الموظفين الرئيسيين يمكن أن يشكل تهديدا لنظام الضمان أو الخدمات ، وخطة العمل المناسبة.

2.3.10 نظام القبول

التحكم

قبول معايير لنظم المعلومات الجديدة ، والترقيات ، والإصدارات الجديدة ينبغي أن تنشأ والاختبارات المناسبة لنظام (ق) التي نفذت خلال التنمية ، وقبل قبولهم.

توجيهات التطبيق

المديرين ينبغي أن تكفل شروط ومعايير لقبول نظم جديـدة واضـحة المعـالم، وافقـت، موثقـة، واختبارها. نظم المعلومات الجديدة، والترقيات، وإصدارات جديدة فقط يجب ترحيلها إلى الإنتاج بعد الحصول على القبول الرسمي. في البنود التالية ينبغي النظر فيها قبل القبول الرسمي التي يجـري تقديمها:

أ) أداء ومتطلبات القدرة الحاسوبية؛

ب) خطأ الانتعاش وإعادة الإجراءات وخطط الطوارئ؛

ج) إعداد واختبار إجراءات التشغيل الروتينية لمعايير محددة؛

د) الاتفاق على مجموعة من الضوابط الأمنية في المكان؛

هـ) وضع إجراءات فعالة للدليل؛

و) الترتيبات استمرارية الأعمال (انظر 14.1)؛

ز) دليل على أن تركيب النظام الجديد لن يؤثر سلبا على النظم القائمة، لا سيما في أوقات الذروة تجهيز مثل نهاية الشهر؛

ح) أدلة على أن تم النظر في تأثير النظام الجديد على مجمل الأمن التابع للمنظمة ؛

ط) التدريب في تشغيل أو استخدام النظم الجديدة ؛

ي) وسهولة الاستخدام ، وهذا يؤثر على الأداء المستخدم ويتجنب الخطأ البشري. لتطورات رئيسية جديدة، ينبغي الرجوع إلى وظيفة العمليات والمستخدمين في جميع مراحل في عملية التنمية من أجل ضمان الكفاءة التشغيلية للتصميم النظام المقترح. وينبغي أن الاختبارات المناسبة ستنفذ للتأكد من أن جميع معايير القبول كانت راضية تماما.

معلومات أخرى

ويمكن أن تشمل قبول شهادة رسمية وعملية الاعتماد للتحقق من أن الأمن الشروط قد عولجت على نحو ملائم.

4.10 الحماية من الشيفرات الخبيثة والمحمول

الهدف: حماية سلامة البرمجيات والمعلومات.

الاحتياطات اللازمة لمنع وكشف إدخال شيفرة خبيثة وغير مصرح به رمز المحمول. برامج وتسهيلات معالجة المعلومات عرضة لإدخال شيفرة خبيثة ، مثل فيروسات الكمبيوتر ، شبكة الديدان وأحصنة طروادة ، ومنطق القنابل. شاهد ينبغي توعية من مخاطر الشيفرات الخبيثة. مديرو ينبغي ، عند الاقتضاء ، وضع ضوابط لمنع وكشف وإزالة الشفرة الخبيثة والتحكم رمز المحمول.

1.4.10 عناصر من الشيفرات الخبيثة

التحكم

كشف والوقاية والإنعاش والضوابط للحماية من الشيفرات الخبيثة والإجراءات المناسبة للمستخدم الوعي ينبغي تنفيذها.

توجيهات التطبيق

وينبغي أن الحماية من الشيفرات الخبيثة أن يقوم على أساس الكشف عن الشيفرات الخبيثة وبرامج الإصلاح، والوعي الأمني، ومناسبة وصول نظام وضوابط لإدارة التغيير. وينبغي أن التوجيهات التالية في الاعتبار:

أ) وضع سياسة رسمية تحظر استخدام البرامج غير المصرح بها (انظر 15.1.2)؛

ب) وضع سياسة رسمية للحماية من المخاطر المصاحبة للحصول على الملفات وإما من البرمجيات أو عن طريق الشبكات الخارجية، أو على أي وسيلة أخرى، تشير إلى ما وينبغي أن تتخذ تدابير وقائية؛

ج) إجراء استعراضات دورية للبرمجيات ومحتوى البيانات من نظم دعم حرجة العمليات التجارية؛ وجود أية ملفات غير معتمدة أو غير مصرح بها التعديلات ينبغي التحقيـق رسميا؛

د) تثبيت وتحديث منتظم للكشف عن الشيفـرات الخبيثة وبرامج لاصلاح لمسـح أجهـزة الكمبيوتر وسائل الإعلام كوسيلة لمراقبة وقائي، أو على أساس روتيني؛ عمليات التفتيش التي تقوم من ينبغي أن تشمل ما يلي:

1) التحقـق من أية ملفات على وسائـط إلكترونية أو بصرية، والملفـات التي يتم استلامها عبر الشبكات لالشيفرات الخبيثة قبل الاستعمال؛

2) التحقق من مرفقات البريـد الإلكترونـي والتنزيـلات لالشيفرات الخبيثـة قبـل الاستعمال؛هذا الاختيار ينبغي أن تتم في أماكن مختلفة، على سبيل المثال في خدمة البريد الكتروني ،أجهزة الكمبيوتر المكتبي ، وعند دخول الشبكة للمنظمة ؛

3) التحقق من صفحات الويب لالشيفرات الخبيثة ؛

هـ) تحديد المسؤوليات والإجراءات الإدارية للتعامل مع الشيفرات الخبيثة الحماية على النظم ، والتدريب على استخدامها والإبلاغ عنها والتي تتعافى من الشيفرات الخبيثـة هجمـات (انظر 13.1 و 13.2) ؛

و) إعداد خطط العمل المناسبة لاستمرار تعافيه من الشيفرات الخبيثة الهجمات ، بما في ذلك جميع البيانات والبرمجيات اللازمة احتياطية وترتيبات استرداد التكاليف (انظر بند 14)؛

ز) تنفيذ الإجراءات اللازمة لجمع المعلومات بصورة منتظمة ، مثل الاشتراك في البريدية قوائم و / أوالتحقق من المواقع على شبكة الإنترنت التي تعطي معلومات عن الشيفرات الخبيثة الجديدة ؛

ح) تنفيذ إجراءات للتحقق من المعلومات المتعلقة الشيفرات الخبيثة ، وضمان أن النشرات التحذيرية هي دقيقة وإعلامية ؛ المديرين ينبغي أن تكفل المؤهلين وقالت مصادر ، على سبيل المثال الصحف ذات السمعة الطيبة ، ومواقع إنترنت أو موردين موثوق انتاج البرمجيات حماية ضد الشيفرات الخبيثة ، والتي تستخدم للتمييز بين الحقيقي والخدع الشيفرات الخبيثة ؛ كافة المستخدمين ينبغي أن تكون على علم بهذه المشكلة من الخدع وماذا تفعل على استلام لهم.

معلومات أخرى

استخدام اثنين أو أكثر من منتجات البرامج التي تحمي من الشيفرات الخبيثة عبر تجهيز المعلومات في مجال البيئة من مختلف البائعين يمكن تحسين فعالية الحماية من الشيفرات الخبيثة.

برامج للحماية من الشيفرات الخبيثة التي يمكن تركيبها على توفير التحديثات التلقائية لملفات تعريف ومحركات المسح الضوئي لضمان حماية هو حتى الآن. بالإضافة إلى ذلك، يمكن تثبيت هذا البرنامج يكون على كل سطح المكتب بالقيام بعمليات تفتيش التلقائي.

وينبغي الحرص على حماية ضد إدخال شيفرة خبيثة أثناء الصيانة وإجراءات الطوارئ، والتي قد تجاوز العادي الشيفرات الخبيثة وضوابط الحماية.

2.4.10 تحكم ضد رمز المحمول

التحكم

حيث استخدام رمز المحمول هو أذن، وينبغي أن التكوين ضمان المصرح رمز المحمول تعمل وفقا لسياسة أمنية واضحة المعالم، وغير مصرح به رمز الجوال ينبغي أن تمنع من التنفيذ.

توجيهات التطبيق

وينبغي أن يكون النظر في الإجراءات التالية لحماية ضد رمز المحمول القيام بأعمال غير مصرح بها:

أ) مدونة المنفذة النقالة في بيئة معزولة منطقيا؛

ب) منع أي استخدام للرمز المتنقلة ؛

ج) حظر تلقي رمز المتنقلة ؛

د) تفعيل التدابير التقنية كما هي متوفرة على نظام محدد لضمان رمز المحمول نجح ؛

هـ) السيطرة على الموارد المتاحة للوصول المحمول رمز ؛

و) الضوابط التشفير لفريد مصادقة رمز المحمول.

معلومات أخرى

المحمول هو رمز البرنامج الذي نقل من جهاز كمبيوتر إلى آخر ومن ثم تنفيذ تلقائيا ، ويؤدي وظيفة محددة مع قليل أو بدون تفاعل المستخدم. المحمول رمز يرتبط مع عدد من الخدمات الوسيطة.

بالإضافة إلى ضمان أن رمز المحمول لا يحتوي على شيفرة خبيثة ، والسيطرة على رمز الجوال أمر ضروري لتجنب الاستخدام غير المصرح به أو تعطل النظام أو الشبكة أو تطبيق الموارد وغيرها من انتهاكات أمن المعلومات.

5.10 *نسخ احتياطية*

الهدف : الحفاظ على سلامة وتوافر المعلومات ومعالجة المعلومات المرافق.
وينبغي أن تكون الإجراءات الروتينية التي أنشئت لتنفيذ الاتفاق احتياطية السياسة والاستراتيجية (انظر كما 14.1) لأخذ نسخ احتياطية للبيانات والتدرب عليها وترميمها في الوقت المناسب.

1.5.10 المعلومات احتياطية

التحكم

نسخ احتياطية من المعلومات والبرامج التي ينبغي اتخاذها واختبارها بانتظام ، وفقا للسياسة المتفق عليها احتياطية.

توجيهات التطبيق

احتياطي كاف وينبغي توفير التسهيلات لضمان أن تكون جميع المعلومات الضرورية وبرامج يمكن استردادها بعد وقوع كارثة أو وسائل الإعلام الفشل.

وينبغي أن البنود التالية للحصول على معلومات احتياطية يمكن النظر فيها :

أ) على المستوى اللازم من احتياطي المعلومات يمكن تعريفها ؛

ب) بسجلات دقيقة وكاملة للنسخ احتياطية واستعادة موثقة وينبغي أن تكون إجراءات المنتجة

ج) مدى (على سبيل المثال الكامل أو فرق احتياطية) ، وتواتر عمليات النسخ الاحتياطي يجب أن تعكس متطلبات العمل في المنظمة ، والاحتياجات الأمنية للمعلومـات المعنية ومدى أهمية هذه المعلومات إلى استمرار تشغيل المنظمة ؛

د) والنسخ الاحتياطية وينبغي أن تكون مخزنة في مكان بعيد ، على مسافة كافية للتخلص من أي الأضرار الناجمة عن كارثة في الموقع الرئيسي ؛

هـ) احتياطية من المعلومات ينبغي أن تعطى على مستوى مناسب من الصحة الجسدية والبيئية حماية (انظر البند 9) بما يتفق مع المعايير المطبقـة في الموقـع الرئيسي ، والضوابط المطبقة على وسائل الاعلام في الموقع الرئيسي ينبغي أن يمتد ليشمـل موقع احتياطي ؛

و) احتياطية وسائل الإعلام ينبغي اختبارها بانتظام للتأكد من أنها يمكن الاعتماد عليها استخدام في حالات الطوارئ عند الضرورة ؛

ز) ينبغي أن تكون إجراءات إعادة فحصها بانتظام واختبارها للتأكد من أنهـا فعالـة وأنها يمكن أن تكتمل في غضون الوقت المخصص له في العملية إجراءات لتحقيق الانتعاش ؛

ح) في الحالات التي يكون فيها السرية ذات أهمية ، احتياطية ينبغي أن تكون محمية من قبل وسائل التشفير.

ترتيبات احتياطية لأنظمة ينبغي أن يكون الفرد اختبارها بانتظام للتأكد من أنها تلبي متطلبات خطط استمرارية الأعمال (انظر البند 14). لنظم الحرجة ، والنسخ الاحتياطي الترتيبات يجـب أن تشمل جميع نظم المعلومات والتطبيقات والبيانات اللازمة لاستعادة النظام الكامل في حال وقوع كارثة.

فترة الاحتفاظ بالمعلومات الضرورية لرجال الأعمال ، وأيضا أي شرط للحصول على نسخ الأرشيف إلى الإبقاء بشكل دائم ينبغي أن تحدد (انظر 15.1.3).

معلومات أخرى

ترتيبات احتياطية يمكن أن تكون آلية للتخفيف من حدة احتياطية وعملية الاستعادة. هذه الآلية ينبغي أن تكون الحلول بما فيه الكفاية اختباره قبل التنفيذ وعلى فترات منتظمة.

6.10 *إدارة أمن الشبكة*

الهدف : ضمان حماية المعلومات في الشبكات وحماية البنية التحتية الداعمة. الإدارة الآمنة للشبكات، والتي قد تمتد الحدود التنظيمية، ويتطلب الحذرالنظر إلى تدفق البيانات، والآثار القانونية، والرصد، والحماية. ضوابط إضافية قد تكون هناك حاجة أيضا لحماية المعلومات الحساسة التي تمر فوق الجمهور الشبكات.

1.6.10 شبكة ضوابط

التحكم

الشبكات يجب أن يكون كافيا إدارتها والسيطرة عليها ، من أجل حمايته مـن التهديـدات ، وإلـى الحفاظ على أمن النظم والتطبيقات التي تستخدم الشبكة ، بما في ذلك المعلومات في العبور.

توجيهات التطبيق

شبكة مديري ينبغي تنفيذ الضوابط اللازمة لضمان أمن المعلومات في الشبكات، وحماية الخـدمات متصلة من الوصول غير المصرح به. على وجه الخصوص، ينبغي النظر في البنود الآتية:

أ) ينبغي أن تتحمل مسؤولية التشغيلي للشبكات يمكن فصلها عن عمليات الكمبيوترحيثما كان ذلك مناسبا (انظر 10.1.3) ؛

ب) والمسؤوليات والإجراءات اللازمة لإدارة المعدات النائية ، بما في ذلك وينبغي أن المعدات في المناطق المستخدم ، سيتم تحديدها ؛

ج) ينبغي أن تكون الضوابط الخاصة التي أنشئت لحماية سرية وسلامة البيانات يمر عبر الشبكات العامة أو عبر الشبكات اللاسلكية ، وحماية متصل لنظم والتطبيقات (انظر 11.4 و 12.3) ؛ ضوابط خاصة قد تكون هناك حاجة أيضا إلى الحفاظ على توافر خدمات الشبكة وأجهزة الكمبيوتر المتصلة ؛

د) تسجيل المناسبة ورصد يجب تطبيقها للتمكن من تسجيل الأمن الإجراءات ذات الصلة ؛

هـ) ينبغي أن تكون إدارة أنشطة منسقة بشكل وثيق على حد سواء لتحسين الخدمة للتنظيم وضوابط لضمان أن تطبق باستمرار عبر المعلومات تجهيز البنية التحتية.

معلومات أخرى

يمكن الحصول على معلومات إضافية بشأن أمن الشبكات يمكن العثور عليها في الايزو / اللجنة الانتخابية المستقلة 18028 ، تكنولوجيا المعلومات

2.6.10 الأمن من خدمات الشبكة

التحكم

ميزات الأمان، ومستويات الخدمة، ومتطلبات إدارة جميع خدمات الشبكة ينبغي أن يكون حددت وإدراجها في أي اتفاق خدمات الشبكة، سواء كانت هذه الخدمات المقدمة داخل الشركات أو الاستعانة بمصادر خارجية.

توجيهات التطبيق

قدرة مزود خدمة الشبكة لإدارة الخدمات المتفق عليها في وسيلة آمنة يجب أن يكون تحدد وتراقب بانتظام، والحق في المراجعة يجب أن يكون متفق عليها.

الترتيبات الأمنية اللازمة لخدمات معينة، مثل المزايا الأمنية، ومستويات الخدمة، والمتطلبات الإدارية، ينبغي تحديدها. المنظمة ينبغي أن تكفل مزودي خدمات الشبكات في تنفيذ هذه التدابير.

معلومات أخرى

شبكة الخدمات تشمل توفير الاتصالات وخدمات الشبكات الخاصة، والقيمة المضافة الشبكات وحلول أمن الشبكات المدارة مثل الجدران النارية وأنظمة كشف التسلل.

هذه الخدمات يمكن أن تتراوح من بسيطة غير المدارة عرض النطاق التـرددي للقيمـة المـضافة العروض المعقدة.

ميزات الأمان للخدمات الشبكة يمكن أن يكون:

أ) طلب للحصول على خدمات أمن الشبكة، مثل التوثيق، والتشفير، وشبكة ضوابط الصدد ؛

ب) المعايير التقنية اللازمة لتأمين الاتصال مع شبكة الخدمات في وفقا لقواعد الأمن واتصال الشبكة ؛

ج) الإجراءات اللازمة لخدمة الشبكة استخدام لتقييد الوصـول إلـى خـدمات الـشبكة أو التطبيقات ، حيثما كان ذلك ضروريا.

7.10 التعامل مع وسائل الإعلام

الهدف: منع الكشف غير المصرح به أو التعديل أو إزالة أو تدمير الممتلكات، وانقطاع للأنشطة التجارية. ينبغي أن تكون وسائل الاعلام الخاضعة للرقابة وجسديا المحمية.

وينبغي أن تكون إجراءات التشغيل الملائمة التي أنشئت لحماية الوثائق وسائل الاعلام الكمبيوتر (مثل الأشرطة ، والأقراص) ، إدخال / إخراج البيانات والوثائق من نظام الإفصاح غير المصرح به أو التعديل أو الإزالة ، والدمار.

1.7.10 إدارة الوسائط القابلة للإزالة

التحكم

ينبغي أن تكون هناك اجراءات مناسبة لإدارة الوسائط القابلة للإزالة.

توجيهات التطبيق

وينبغي أن المبادئ التوجيهية التالية لإدارة الوسائط القابلة للإزالة في الاعتبار :

أ) إذا لم تعد مطلوبة ، محتويات أي إعادة صالحة للاستعمال وسائل الاعلام التي سيتم إزالتها من ينبغي أن تكون منظمة غير قابل للاسترداد ؛ تقنيات الأمن -- تكنولوجيا المعلومات وأمن الشبكات.

ب) حيثما كان ذلك ضروريا وعمليا ، ينبغي أن يطلب الإذن لإزالتها من وسائل الاعلام وينبغي للمنظمة وسجل لعمليات الإزالة من هذا القبيل أن تبقى من أجل الحفاظ على لمراجعة الحسابات ؛

ج) جميع وسائل الإعلام يجب أن تكون مخزنة في بيئة آمنة ومأمونة ، وفقا الصانعين المواصفات ؛

د) المعلومات المخزنة على وسائل الاعلام التي يجب أن تتوفر لفترة أطول من العمر وسائل الاعلام (في ينبغي أن يتفق مع الصانعين المواصفات) يكون أيضا مخزنة في مكان آخر لتفادي معلومات الخسارة الناجمة عن تدهور وسائل الإعلام ؛

هـ) ينبغي تسجيل الوسائط القابلة للإزالة اعتبار للحد من فرصة للبيانات خسارة ؛

و) محركات أقراص الوسائط القابلة للنقل لا ينبغي تمكين إذا كان هناك سبب للقيام بذلك العمل. وينبغي لجميع الإجراءات ومستويات إذن أن تكون موثقة بوضوح.

معلومات أخرى

الوسائط القابلة للإزالة تشمل الأشرطة ، والأقراص ، وأقراص فلاش ، والقابلة للإزالة محركات الأقراص الصلبة والأقراص المدمجة وأقراص الفيديو الرقمية ، ووسائل الإعلام المطبوعة.

2.7.10 التخلص من وسائل الاعلام

التحكم

وسائل الإعلام يجب أن يتم التخلص منها بشكل آمن وبسلام عندما لم تعد مطلوبة ، وذلك باستخدام إجراءات رسمية.

توجيهات التطبيق

الإجراءات الرسمية لضمان التخلص من وسائل الاعلام وينبغي تقليل خطر المعلومات الحساسة

تسرب للأشخاص غير المصرح بها. إجراءات لضمان التخلص من وسائل الاعلام التي تتضمن حساسة ينبغي أن تكون المعلومات التي تتناسب مع حساسية لتلك المعلومات. في البنود التالية ينبغي النظر في :

أ) ينبغي على وسائل الإعلام التي تحتوي على معلومات حساسة يمكن تخزينها والتخلص منها بأمان ، وعلى سبيل المثال عن طريق الحرق أو التقطيع أو محوها من البيانات لاستخدامها من قبل تطبيق آخر داخل المنظمة ؛

ب) الإجراءات التي ينبغي أن تكون في المكان لتحديد البنود التي قد تتطلب التخلص من آمن

ج) أنه قد يكون من الأسهل أن يرتب لجميع البنود وسائل الإعلام التي ينبغي جمعها والتخلص منها بأمان ، بدلا من محاولة لفصل المواد الحساسة ؛

د) والعديد من المنظمات وجمع وتقديم الخدمات للتخلص من الأوراق ، والمعدات وسـائل الإعلام ؛ ينبغي توخي الحذر في اختيار المقاول المناسب مع وجود ضوابط كافية والتجربة ؛

هـ) التخلص من المواد الحساسة وينبغي أن يكون تسجيل حيثما أمكن ذلك من أجل الحفاظ على مراجعة الحسابات درب.

عندما تتراكم وسائل الإعلام من أجل التخلص منها ، وينبغي النظر إلى أثر التجميـع ، ممـا قـد يتسبب في كمية كبيرة من المعلومات غير الحساسة لتصبح حساسة.

غيرها من المعلومات الحساسة من المعلومات يمكن الكشف عنه من خلال التخلص من الإهمال في وسائل الإعلام (انظر أيضا 9.2.6 للحصول على معلومـات حـول الـتخلص مـن المعـدات).

3.7.10 إجراءات التعامل مع المعلومات

التحكم

وينبغي أن إجراءات لمناولة وتخزين المعلومات التي أنشئت لحماية هذا المعلومات من الإفصاح غير المصرح به أو إساءة استخدامها.

توجيهات التطبيق

ينبغي أن تكون إجراءات وضعت لمناولة ومعالجة وتخزين ، ونقل المعلومات بمـا يتماشـى مـع تصنيف (انظر 7.2). وينبغي أن يكون النظر في البنود التالية:

أ) المناولة ووضع العلامات على جميع وسائل الإعلام إلى المستوى المـشار إليـه فـي التصنيف ؛

ب) القيود المفروضة على الوصول لمنع الوصول غير المصرح به من الموظفين ؛

ج) الحفاظ على سجل رسمي للمستلمين المخولين من البيانات ؛

د) ضمان إدخال البيانات كاملة ، والتي يتم تجهيزها بشكل صحيح وأنه أنجز الإخراج التحقق من صحة تطبيق ؛

هـ) حماية البيانات المخزنة مؤقتا في انتظار الإخراج إلى مستوى يتفق مع حساسيتها ؛

و) تخزين وسائل الاعلام وفقا الصانعين المواصفات ؛

ز) الحفاظ على توزيع البيانات إلى أدنى حد ممكن ؛

ح) وضع علامات واضحة للجميع نسخ من وسائل الإعلام لانتباه المتلقي أذن ؛

ط) استعراض قوائم التوزيع وقوائم المستفيدين من أذن في فترات زمنية منتظمة.

معلومات أخرى

هذه الاجراءات تطبق على المعلومات الواردة في الوثائق ، نظم الحوسبة والشبكات والمحمول الحوسبة والاتصالات المتنقلة ، والبريد ، والبريد الصوتي ، والاتصالات الصوتية بصفة عامة ، والوسائط المتعددة ، والخدمات البريدية / المرافق ، واستعمال آلات الفاكس وأية بنود أخرى حساسة ، على سبيل المثال شيكات على بياض، والفواتير.

4.7.10 الأمن من وثائق النظام

التحكم

وينبغي أن تكون وثائق نظام حماية ضد الوصول غير المصرح به.

توجيهات التطبيق

لتأمين وثائق النظام، ينبغي النظر في البنود الآتية:

أ) ينبغي أن يكون نظام وثائق مخزنة بشكل آمن؛

ب) قائمة من أجل الوصول إلى وثائق نظام يكون في أضيق الحدود ، والتي أذن بها صاحب الطلب ؛

ج) نظام التوثيق الذي عقد على الشبكة العامة، أو توريدها عبر الشبكة العامة ، وينبغي أن تكون الحماية الملائمة.

معلومات أخرى

نظام الوثائق قد تحتوي على مجموعة من المعلومات الحساسة، على سبيل المثال وصفا للتطبيقات العمليات والإجراءات وهياكل البيانات ، وعمليات الترخيص.

8.10 *تبادل المعلومات*

الهدف: المحافظة على أمن المعلومات وبرامج تبادل داخل المنظمة ومع أي جهة خارجية. وينبغي أن يكون تبادل المعلومات والبرمجيات بين المنظمات أن يستند إلى سياسة رسمية الصرف ، ونفذت وفقا للاتفاقات التبادل ، وينبغي أن تكون متوافقة مع أي من التشريعات ذات الصلة (انظر البند 15). وينبغي أن تكون الإجراءات والمعايير المحددة لحماية المعلومات والوسائط المادية التي تحتوي على معلومات في العبور.

1.8.10 تبادل المعلومات السياسات والإجراءات

التحكم

سياسات سعر الصرف الرسمي والإجراءات والضوابط ينبغي أن يكون في مكان لحماية تبادل المعلومات من خلال استخدام كافة أنواع مرافق الاتصالات.

توجيهات التطبيق

والإجراءات والضوابط التي ينبغي اتباعها عند استخدام مرافق الاتصالات الالكترونية لتبادل المعلومات ينبغي أن ينظر في البنود التالية :

أ) إجراءات تهدف إلى حماية تبادل المعلومات من الاعتراض ، والنسخ ، تعديل وسوء التوجيه والدمار ؛

ب) إجراءات للكشف عن والحماية من الشيفرات الخبيثة التي قد تكون تنتقل عن طريق استخدام الاتصالات الالكترونية (انظر الفقرة 10.4.1) ؛

ج) الإجراءات اللازمة لحماية إبلاغ المعلومات الالكترونية الحساسة التي هي في شكل ملحق؛

د) سياسة أو مبادئ توجيهية لتحديد الاستخدام المقبول للمرافق الاتصالات الالكترونية (انظـر 7.1.3)؛

هـ) الإجراءات اللازمة لاستخدام الاتصالات اللاسلكية ، مع الأخذ في الاعتبار مخاطر معينـة المعنية ؛

و) الموظف والمقاول ويمكن لأي مستخدم آخر مسؤوليات على عدم تقديم تنازلات ال المنظمة ، على بيل المثال عن طريق تشويه صورتها ، والمضايقات ، وانتحال الشخصية ، وتحويل سلسلة من رسائل ، وشراء غير مصرح بها ، وما إلى ذلك ؛

ز) استخدام تقنيات التشفير على سبيل المثال لحماية سرية وسلامة و صحة للمعلومـات (انظـر الفقرة 12.3) ؛

ح) والاحتفاظ بهم والمبادئ التوجيهية للتخلص من كافة المراسلات التجارية ، بما في ذلك رسائل ، في وفقا للتشريعات الوطنية والمحلية ذات الصلة واللوائح ؛

ط) لا يترك الحرجة الحساسة أو معلومات عن مرافق الطباعة ، على سـبيل المثـال الناسـخات والطابعات ، وآلات الفاكس ، وهذه يمكن الوصول إليها من قبل أفراد غير مرخص بها ؛

ي) الضوابط والقيود المرتبطة شحن مرافق الاتصالات ، على سبيل المثال التوجيه التلقائي للبريد الالكتروني لعناوين البريد الخارجي ؛

ك) لتذكير الموظفين بضرورة أن تتخذ الاحتياطات المناسبة ، على سبيل المثال عدم الكشف عن المعلومات الحساسة حتى لا يسترق أو اعتراضها عند إجراء مكالمة هاتفية من قبل :

1) الناس في المناطق المجاورة لها وخاصة عند استخدام الهواتف النقالة ؛

2) التنصت على المكالمات الهاتفية ، وغيرها من أشكال الوصول المادي من خلال التنصت على الهاتف أو خط الهاتف ، أو باستخدام المسح الاستقبال ؛

3) أشخاص في المستلم الغاية ؛

ل) عدم ترك رسائل تحتوي على معلومات حساسة عن الإجابة لأن هذه الآلات قد يكون ردها من قبل أشخاص غير مأذون لهم ، المخزنة على أنظمة طائفية أو تخزينها غير صحيح نتيجة لمكالمة خاطئة

م) لتذكير الموظفين عن مشاكل باستخدام آلات الفاكس ، وهما :

1) الوصول غير المصرح به إلى المدمج في مخازن رسالة لاسترداد الرسائل ؛

2) متعمدة أو عرضية من آلات البرمجة لإرسال رسائل إلى محددة أرقام ؛

3) إرسال وثائق ورسائل إلى عدد إما عن طريق الخطأ أو باستخدام مكالمة خاطئة وتخزين رقم خاطئ ؛

ن) تذكير الموظفين ليس لتسجيل البيانات الديموغرافية ، مثل عنوان البريد الإلكتروني أو غيره المعلومات الشخصية ، في أي برامج لتجنب الاستخدام غير المصرح به للجمع ؛

س) مذكرا بأن أفراد الحديثة آلات الفاكس وآلات النسخ ومخابئ الصفحة وصفحات مخزن في حالة وجود ورقة أو نقل خطأ ، والتي سيتم طبع مرة واحدة الخطأ هو تطهيرها.

بالإضافة إلى ذلك، ينبغي أن نتذكر أن الأفراد لا ينبغي أن يكون في محادثات سرية الأماكن العامة أو فتح مكاتب وأماكن الاجتماع مع المنظمات غير سليمة - الجدران العازلة. تسهيلات لتبادل المعلومات ينبغي أن تمتثل لأي المتطلبات القانونية ذات الصلة (انظر البند 15).

<u>معلومات أخرى</u>

تبادل المعلومات قد تحدث عن طريق استخدام عدد من أنواع مختلفة من مرافق الاتصالات، بما في ذلك البريد الإلكتروني والصوتي، والفاكس، والفيديو.

برامج تبادل قد تحدث من خلال عدد من وسائل مختلفة ، بما في ذلك تحميله من شبكة الانترنت والحصول عليها من شركات بيع المنتجات ، والجرف.

وينبغي أن الأعمال التجارية ، والقانونية ، والآثار الأمنية المرتبطة تبادل البيانات الالكترونية والتجارة الالكترونية ، والاتصالات الالكترونية والاحتياجات اللازمة لضوابط ينبغي النظر فيها.

المعلومات التي يمكن أن يتعرض للخطر بسبب نقص الوعي أو سياسة أو إجراءات بشأن اسـتخدام تسهيلات لتبادل المعلومات ، على سبيل المثال أن سمع على الهاتف المحمول في الأماكن العامـة ، التوجيه الخاطئ للرسالة بريد الكتروني ، الإجابة على الآلات التي سمع ، والوصول غير المصرح به إلى الاتصال الهاتفي في أنظمة البريد الصوتي أو غير قصد إرسال الفاكسات إلى أجهزة الفاكس خاطئة.

العمليات التجارية يمكن أن تتعطل ، والمعلومات التـي يمكـن أن يتعـرض للخطـر إذا مرافـق الاتصالات تفشل ، مثقلة أو انقطاع (انظر البند 10.3 و14). معلومات يمكن أن يتعرض للخطر إذا كـان الوصـول إليهـا مـن قبـل المـستخدمين غيـر المخـولين (انظـر البنـد 11).

2.8.10 اتفاقات التبادل

التحكم

ينبغي وضع اتفاقات لتبادل المعلومات والبرمجيات بين لمنظمة وأطراف خارجية.

توجيهات التطبيق

تبادل الاتفاقات ينبغي أن تنظر في الأوضاع الأمنية التالية :

أ) مسؤوليات الإدارة وإخطار لمراقبة انتقال العدوى ، وإيفاد ، وتسلم ؛

ب) الإجراءات اللازمة لإخطار المرسل من نقل وارسال وتلقي ؛

ج) إجراءات لضمان التتبع وعدم التنصل ؛

د) الحد الأدنى من المعايير التقنية من أجل التعبئة والتغليف والنقل ؛

هـ) اتفاقات الضمان ؛

و) ساعي معايير تحديد الهوية ؛

ز) والمسؤوليات في حال وقوع حوادث أمنية من المعلومات ، مثل ضياع البيانات ؛

ح) استخدام نظام وضع العلامات المتفق عليها للحصول على معلومات حساسة أو الحرجة ، وضمان أن معنى التسميات على الفور ، ويفهم أن المعلومات بشكل مناسب المحمية ؛

ط) الملكية والمسؤوليات لحماية البيانات وحقوق التأليف والنشر وتراخيص البرامج واعتبارات مماثلة (انظر 15.1.2 و15.1.4) ؛

ي) المعايير التقنية لتسجيل وقراءة المعلومات والبرمجيات ؛

ك) أي ضوابط خاصة قد تكون ضرورية لحماية المواد الحساسة ، مثل التشفير مفاتيح (انظر 12.3).

السياسات والإجراءات ، وينبغي وضع معايير والحفاظ عليها لحماية المعلومات وسائط مادية في العبور (انظر أيضا 10.8.3) ، وينبغي الإشارة إليها في اتفاقات للتبادل من هذا القبيل.

محتوى الأمنية في أي اتفاق ينبغي أن يعبر عن حساسية المعلومات التجارية المعنية.

معلومات أخرى

الاتفاقات التي قد تكون الكترونية أو استعماله ، وقد تتخذ شكل عقود رسمية أو ظروف العمل. للحصول على معلومات حساسة وتستخدم آليات محددة لتبادل المعلومات من هذا القبيل ينبغي أن تكون متسقة لجميع المنظمات وأنواع الاتفاقات.

3.8.10 البدنية في وسائل الاعلام العابر

التحكم

وينبغي أن تحتوي على معلومات وسائل الإعلام أن تكون محمية ضد الوصول غير المصرح به أو إساءة الاستخدام أو الفساد أثناء النقل خارج المنظمة في الحدود الطبيعية.

توجيهات التطبيق

المبادئ التوجيهية التالية ينبغي النظر في وسائل الإعلام لحماية المعلومات التي يجري نقلها بين المواقع:

أ) ينبغي على وسائل النقل موثوق بها أو سعاة استخدامها ؛

ب) قائمة ناقلي أذن ينبغي الاتفاق مع الإدارة ؛

ج) إجراءات للتأكد من تحديد حاملي ينبغي تطويرها ؛

د) التعبئة والتغليف وينبغي أن يكون كافيا لحماية المحتويات من أي ضـرر مـادي ، مـن المرجح أن تنشأ أثناء العبور وفقا لأي الصانعين المواصفات (مثلا البرمجيات)، وعلى سـبيل المثال حماية ضد أي العوامل البيئية التي قد تقلل من وسائل الاعلام لاستعادة فعاليـة مثـل التعرض للحرارة ، رطوبة أوالكهرومغناطيسي الميادين ؛

هـ) الضوابط التي ينبغي اعتمادها ، عند الاقتضاء ، لحماية المعلومات الحساسة من الكشف غير المصرح به أو التعديل ؛ وتشمل الأمثلة :

1) استخدام الحاويات مؤمن ؛
2) التسليم باليد ؛
3) التعبئة والتغليف للعبث واضح (وهو ما يكشف أية محاولة للوصول) ؛

4) في حالات استثنائية ، تقسيم للشحنة في أكثر من واحد والتسليم ارسال عبر طرق مختلفة.

معلومات أخرى

المعلومات يمكن أن تكون عرضة للوصول غير المصرح به أو إساءة الاستخدام أو الفـساد أثنـاء النقل المادي ، على سبيل المثال عند إرسال وسائل الاعلام عن طريق البريد أو عن طريق البريـد السريع.

4.8.10 الرسائل الالكترونية

التحكم

وينبغي أن تشارك في المعلومات الرسائل الإلكترونية بشكل مناسب المحمية.

توجيهات التطبيق

الاعتبارات الأمنية لتبادل الرسائل الالكترونية وينبغي أن تشمل ما يلي :

أ) حماية الرسائل من الوصول غير المصرح به أو التعديل أو الحرمان من الخدمة ؛

ب) وضمان معالجة صحيحة ونقل الرسالة ؛

ج) الموثوقية عامة وتوافر الخدمة ؛

د) الاعتبارات القانونية ، على سبيل المثال لمتطلبات التوقيعات الالكترونية ؛

هـ) الحصول على موافقة مسبقة لاستخدام الخارجي الخدمات العامة مثل الرسائل الفورية أو ملف تقاسم ؛

و) أقوى مستويات مصادقة التحكم في الوصول للجمهور من الشبكات يمكن الوصول إليها.

معلومات أخرى

الرسائل الإلكترونية كالبريد الإلكتروني وتبادل البيانات الإلكترونية (التبادل الالكتروني للبيانـات) ، والرسائل الفورية وتلعب دورا متزايد الأهمية فـي الاتـصالات والأعمـال التجاريـة. المراسـلة الالكترونيـة مخـاطر مختلفـة مـن الاتـصالات القائمـة علـى الـورق.

5.8.10 الأعمال ونظم المعلومات

التحكم

السياسات والإجراءات التي ينبغي وضعها وتنفيذها لحماية المعلومات المرتبطة الربط بين أنظمة المعلومات التجارية.

توجيهات التطبيق

إيلاء الاعتبار لأمن والآثار المترتبة على الأعمال التشابك والتداخل بين هذه التـسهيلات يجـب أن تشمل ما يلي:

أ) معرفة نقاط الضعف في النظم الإدارية والمحاسبية التي تكون فيها المعلومات المـشتركة بين الأجزاء المختلفة للمنظمة ؛

ب) معلومات من مواطن الضعف في نظم الاتصالات التجارية ، على سبيل المثال الهـاتف تسجيل المكالمات أو المكالمات الجماعية وسرية المكالمات، وتخزين أجهزة الفاكس ، وفتح البريـد، توزيع البريد ؛

ج) السياسات والضوابط المناسبة لإدارة تبادل المعلومات ؛

د) باستثناء فئات المعلومات التجارية الحساسة ، وإذا كانت وثائق سرية نظام لا توفر مستوى مناسب من الحماية (انظر 7.2) ؛

هـ) تقييد الوصول إلى مذكرات المعلومات المتعلقة بالأفراد المختارة ، على سـبيل المثـال الموظفين يعملون في مشاريع حساسة ؛

و) من فئات الموظفين والمتعاقدين ، أو شركاء الأعمال يسمح لاستخدام نظام ومن المواقـع التي يمكن الوصول إليها (انظر 6.2 و 6.3) ؛

ز) تقييد مختارة مرافق لفئات محددة من المستخدمين ؛

ح) تحديد حالة من المستخدمين ، على سبيل المثال العاملين في المنظمة أو المقـاولين فـي الدلائل لفائدة المستخدمين الآخرين ؛

ط) والاحتفاظ بهم واحتياطية للمعلومات التي عقدت على النظام (انظر 10.5.1) ؛
ي) الاحتياجات والترتيبات الاحتياطية (انظر 14).

معلومات أخرى

مكتب نظم المعلومات والفرص المتاحة لزيادة سرعة نشر وتقاسم الأعمال المعلومات باستخدام مزيج من : وثائق وأجهزة الكمبيوتر والحوسبة النقالة والمحمولة الاتصالات والبريد ، والبريد الصوتي ، الاتصالات الصوتية بصفة عامة ، والوسائط المتعددة والبريد خدمات / مرافق وأجهزة الفاكس.

9.10 خدمات التجارة الالكترونية

الهدف: ضمان الأمن لخدمات التجارة الإلكترونية واستخدامها آمن.

الآثار الأمنية المرتبطة باستخدام خدمات التجارة الإلكترونية ، بما في ذلك على الخط وينبغي أن المعاملات ، والاحتياجات اللازمة للضوابط ، يمكن النظر فيها. سلامة وتوافر المعلومات وتنشر إلكترونيا من خلال النظم المتاحة للجمهور كما ينبغي النظر.

1.9.10 التجارة الالكترونية

التحكم

وينبغي أن تشارك المعلومات في مجال التجارة الإلكترونية المارة عبر الشبكات العامة تكون محمية من النشاط الاحتيالي ، المنازعات الناشئة عن العقود ، والإفصاح غير المرخص به والتعديل.

توجيهات التطبيق

الاعتبارات الأمنية للتجارة الالكترونية وينبغي أن تشمل ما يلي:

أ) مستوى الثقة يتطلب كل طرف في كل المطالب هوية الآخرين، على سبيل المثـال مـن خلال التوثيق؛

ب) الإذن العمليات المرتبطة الذين قد ضـبط الأسـعار، ومـسألة التوقيـع أو التجـاريين الرئيسيين وثائق ؛

ج) ضمان أن الشركاء التجاريين هم على علم تام توكيلاتهم ؛

د) تحديد وتلبية لمتطلبات السرية والسلامة ، ودليلا على إيفاداستلام الوثـائق الرئيـسية ، وعدم التنصل من العقود ، على سبيل المثال المقترنة العطاءات وعمليات العقد ؛

هـ) على المستوى المطلوب من الثقة في نزاهة قوائم الأسعار المعلن عنها ؛

و) سرية أي معلومات أو بيانات حساسة ؛

ز) سرية وسلامة أية معاملات النظام ، ومعلومات الدفع ، والتسليم تفاصيل العنوان ، وتأكيدا لهذه الإيصالات ؛

ح) درجة التحقق المناسب للتأكد من دفع المعلومات المقدمة من قبل العملاء ؛

ط) اختيار الشكل الأنسب لتسوية المدفوعات للوقاية من الاحتيال ؛

ي) مستوى الحماية المطلوبة للحفاظ على سرية وسلامة النظام المعلومات ؛

ك) تجنب الخسارة أو ازدواجية في المعلومات المعاملات ؛

ل) المسؤولية القانونية المرتبطة مع أية عمليات احتيالية ؛

م) متطلبات التأمين.

كثير من الاعتبارات المذكورة أعلاه يمكن مواجهتها من خلال تطبيق الـضوابط التـشفير (انظـر 12.3) ، مع الأخذ في الاعتبار الامتثال للمتطلبات القانونية (انظر 15.1 ، وخـصوصا ل15.1.6 الترميز التشريع).

وينبغي أن ترتيبات التجارة الالكترونية بين الشركاء التجاريين تكون مدعومة اتفاق الموثقـة التـي تلزم كلا الطرفين للشروط المتفق عليها للتجارة ، بما في ذلك تفاصيل الترخيص (انظر ب) أعلاه). اتفاقات أخرى مع المعلومات والخدمات ذات القيمة المضافة مزودي الشبكة قد تكون ضرورية.

ينبغـي أن تعلـن علـى الجمهـور أنظمـة التـداول عـن شـروط التجاريـة للعمـلاء. وينبغي النظر إلى القدرة على مواجهة هجوم من الدولة المـضيفة (ق) المـستخدمة فـي التجـارة الإلكترونية ، والآثار الأمنية المترتبة على أي شبكة الربط الكهربائي المطلوبة لتنفيذ خدمات للتجارة الإلكترونية (انظر 6.4.11).

معلومات أخرى

التجارة الإلكترونية هي عرضة لعدد من التهديدات الشبكة التي قد تسفر عن الاحتيال النشاط ، عقد النزاع ، والكشف عن المعلومات أو تعديلها.

التجارة الإلكترونية ويمكنها الاستفادة من أساليب المصادقة الآمنة ، على سبيل المثـال باسـتخدام المفتاح العمومي، التشفير والتوقيعات الرقمية (انظر أيضا 12.3) للحد من المخاطر. أيضا ، طرف ثالث موثوق به يمكن استخدامها ، حيث هناك حاجة إلى مثل هذه الخدمات.

2.9.10 على الخط الصفقات

التحكم

معلومات تشارك في المعاملات على شبكة الإنترنت يجب أن تكون محمية لمنع انتقال العدوى غير مكتملة ، والخطأ في التوجيه ، وغير مصرح بها رسالة التغيير ، والكشف غير المصرح به أو غير المأذون بها رسالة ازدواجية أو تكرار.

توجيهات التطبيق

الاعتبارات الأمنية المعاملات على شبكة الإنترنت وينبغي أن تتضمن ما يلي:

أ) استخدام التوقيعات الالكترونية ، من قبل كل طرف من الأطراف المشاركة في المعاملة ؛

ب) جميع جوانب هذه الصفقة ، أي كفالة ما يلي:

1) اعتماد المستخدم لصالح جميع الأطراف والتحقق منها ؛

2) هذه الصفقة لا تزال سرية ، و

3) خصوصية مرتبطة مع جميع الأطراف المعنية هو الإبقاء ؛

ج) مسار الاتصالات بين جميع الأطراف المعنية هو مشفرة ؛

د) والبروتوكولات المستخدمة للاتصال بين جميع الاطراف المعنية هو المضمون ؛

هـ) التأكد من أن تخزين تفاصيل الصفقة تقع خارج أي الجمهور بيئة يسهل الوصول إليها ، على سبيل المثال على منصة التخزين الموجودة على الشبكة الداخلية التنظيمية ، وعدم الاحتفاظ بها وكشفها على وسيلة تخزين للوصول مباشرة من شبكة الإنترنت ؛

و) حيث يتم استخدام سلطة موثوق بها (على سبيل المثال لأغراض إصدار والحفاظ الرقمية تواقيع و / أوالشهادات الرقمية) هو أمنية متكاملة وجزءا لا يتجزأ من جميع أنحاء نهاية بأكمله إلى نهاية الشهادة / إدارة عملية التوقيع.

معلومات أخرى

مدى الضوابط التي سوف تحتاج إلى أن تكون متناسبة مع مستوى المخاطر المرتبطة بكل شكل من أشكال المعاملات على الخط.

المعاملات قد تحتاج إلى الامتثال للقوانين والقواعد والأنظمة المعمول بها في الولاية التي يتولد من المعاملات ، عن طريق تجهيزها ، أنجزت في ، و / أو تخزينها.

وتوجد العديد من أشكال الصفقات التي يمكن القيام بها في على الخط بطريقة مثلا التعاقدية والمالية وما إلى ذلك.

سلامة المعلومات التي يتم إتاحتها على نظام متاحة للجمهور ينبغي حمايتها لمنـع التعـديل غيـر المصرح به.

3.9.10 المعلومات المتاحة للجمهور

التحكم

إن تكاملية المعلومات يجب أن تكون متاحة على نظم عامة ويجب أن تحمى مـن التعـديل غيـر المصرح به.

توجيهات التطبيق

البرمجيات والبيانات والمعلومات الأخرى التي تتطلب مستوى عال من النزاهة، والتي تتـاح علـى نظام متاحة للجمهور، وينبغي أن تكون محمية بواسطة آليات مناسبة، على سبيل المثال التوقيعـات الرقمية (انظر 12.3).

وينبغي أن تكون متاحة للجمهور نظام اختبار مقابل نقاط الـضعف والفـشل المـسبق للمعلومـات المتاحة.
يجب أن يكون هناك موافقة رسمية قبل عملية المعلومات في متناول الجمهور. بالإضافة إلى ذلـك، جميع المدخلات المقدمة من الخارج لهذا النظام يجب أن يـتم التحقـق منهـا والموافقـة عليهـا. نظم النشر الالكتروني، وخاصة تلك التي تسمح للدخول المباشر والتغذية المرتدة من المعلومـات، وينبغي مراقبتها بعناية بحيث :

أ) معلومات تم الحصول عليها في الامتثال لأي تشريع حماية البيانات (انظر 15.1.4) ؛

ب) لإدخال المعلومات ومعالجتها من قبل ، فإن نشر نظام تتم معالجتها بالكامل وبدقة في الوقت المناسب ؛ وسوف ج) معلومات حساسة تكون محمية خلال جمع البيانات وتجهيزها ، وتخزينها ؛

د) الوصول إلى نظام النشر لا تسمح بالوصول إلى الشبكات غير المقصودة التي نظام متصل.
معلومات أخرى
على نظام المعلومات المتاحة للجمهور، على سبيل المثال معلومات عن خادم ويب يمكن الوصول إليها عبر الإنترنت، قد تحتاج إلى الامتثال للقوانين والقواعد والأنظمة المعمول بها في الولاية التي تقع في النظام، حيث تنعقد التجارة أو إذا كان للمالك (ليالي الإقامة. التعديل غير المصرح به للمعلومات المنشورة قد يسيء الى سمعة المنظمة النشر.

10.10 الرصد

الهدف: الكشف عن معلومات غير مصرح بها أنشطة التجهيز.

وينبغي أن تكون أنظمة رصد الأحداث وأمن المعلومات يجب أن يتم تسجيلها. وينبغي أن يسجل خطأ تسجيل الشركة المشغلة ويمكن استخدامها لضمان نظام للمعلومات هي المشاكل التي تم تحديدها.

وينبغي للمنظمة أن يمتثل لجميع المتطلبات القانونية ذات الصلة التي تنطبق على أنشطة الرصد وقطع الأشجار.
وينبغي أن تستخدم نظام مراقبة للتحقق من فعالية الرقابة والتي اعتمدت للتحقق طبقا لهذه السياسة وصول النموذج.

1.10.10 تسجيل التدوين

التحكم

مراجعة سجلات تسجيل أنشطة المستخدم والاستثناءات والاحداث الامنية والمعلومات التي يجب أن يتم إنتاجها والاحتفاظ بها لفترة زمنية متفق عليها للمساعدة في التحقيقات في المستقبل ، والتحكم في الوصول للرصد.

توجيهات التطبيق

مراجعة سجلات وينبغي أن تشمل، عند الاقتضاء:

أ) هوية المستخدم؛

ب) التواريخ والأوقات، وتفاصيل الأحداث الرئيسية، على سبيل المثال الـدخول علـى الـسجل وخالا؛

ج) هوية محطة أو موقع إذا كان ذلك ممكنا ؛

د) سجلات المحاولات الناجحة ورفض الوصول إلى النظام ؛

هـ) سجلات البيانات الناجحة وغيرها من الموارد ، ورفض محاولات الوصول ؛

و) إدخال تغييرات على نظام التكوين ؛

ز) استخدام الامتيازات ؛

ح) استخدام المرافق النظام والتطبيقات ؛

ط) الملفات والوصول إلى هذا النوع من الوصول إليها ؛

ي) عناوين الشبكة والبروتوكولات ؛

ك) الإنذارات التي أثارها نظام مراقبة الدخول؛

ل) تفعيل وإلغاء تفعيل أنظمة الحماية مثل برامج مكافحة الفيروسات وأنظمة أنظمة كشف التسلل.

معلومات أخرى

ومراجعة السجلات قد تحتوي على البيانات السرية والشخصية تطفلا. تدابير لحماية خصوصية المناسبة التي ينبغي اتخاذها (انظر أيضا 15.1.4). حيثما كان ذلك ممكنا ، ينبغي أن مسؤولي النظام لا تملك صلاحية لمحو أو دي تفعيل سجلات أنشطتها الخاصة (انظر 10.1.3).

2.10.10 استخدام نظام الرصد

التحكم

وينبغي أن إجراءات لرصد استخدام مرافق معالجة المعلومات المزمع إنشاؤه ونتائج أنشطة الرصد مراجعتها بانتظام.

توجيهات التطبيق

مستوى الرصد المطلوبة للمرافق الفردية يجب أن يحددها تقييم المخاطر.

وينبغي للمنظمة أن يمتثل لجميع المتطلبات القانونية ذات الصلة التي تنطبق على رصده الأنشطة.

المجالات التي ينبغي النظر فيها ما يلي:

أ) ولوج) أذن ، بما في ذلك تفاصيل مثل :

1) من هوية المستخدم.

2) التاريخ والوقت من الأحداث الرئيسية ؛

3) أنواع الأحداث ؛

4) الملفات الوصول إليها ؛

5) برنامج / المرافق المستخدمة جميع العمليات المتميزة ، مثل :

1) استخدام الحسابات المميز ، على سبيل المثال المشرف ، والجذرية ، والمسؤول

2) نظام البدء والتوقف ؛

3) إدخال / إخراج الجهاز مرفق / مفرزة ؛

ج) محاولات الوصول غير المصرح به ، مثل :

1) فشل او رفض إجراءات المستخدم ؛

2) فشل أو رفض الإجراءات التي تشمل البيانات وغيرها من الموارد ؛

3) الوصول انتهاكات سياسة والإشعارات لشبكة البوابات والجدران النارية ؛
4) التنبيهات من أنظمة الملكية كشف التسلل ؛
1) وحدة التحكم أو تنبيهات الرسائل ؛
2) سجل نظام الاستثناءات ؛
3) شبكة أجهزة الإنذار والإدارة ؛
4) الإنذارات التي أثارها نظام مراقبة الدخول ؛

هـ ـ) التغييـرات ، أو محـاولات لتغييـر ، إعـدادات أمـان النظـام والـضوابط. كيف كثيرا ما تكون نتائج أنشطة الرصد ويتم استعراض ينبغي أن يعتمد على المخاطر التي تنطوي عليها. خطر العوامل التي ينبغي النظر فيها وتشمل :

والحرجية) من عمليات التطبيق ؛

ب) قيمة ، والحساسية ، وحساسية المعلومات المعنية ؛

ج) التجربة الماضية من عمليات التسلل وإساءة استخدام النظام ، وتواتر نقاط الضعف يجري استغلالها ؛

د) مدى الترابط نظام (شبكات عامة وخاصة) ؛

هـ) تسجيل مرفق دي يجري تفعيلها.

معلومات أخرى

استخدام إجراءات الرصد ضرورية لضمان أن المستخدمين إلا أن أداء الأنشطة وقد تم بإذن صريح.

استعراض سجل ينطوي على فهم التهديدات التي يواجهها النظام وهذه الطريقة التي قد تنشأ. أمثلة من الأحداث التي قد تتطلب مزيدا من التحقيق في حالة وقوع حوادث أمن المعلومات ، وترد في 13.1.1.

3.10.10 سجل حماية المعلومات

التحكم

قطع الأشجار والمرافق ومعلومات السجل ينبغي حمايتها من التلاعب والوصول غير المصرح به.

توجيهات التطبيق

الضوابط وينبغي أن تهدف إلى حماية ضد تغييرات غير مصرح بها والمشاكل التشغيلية مع تسجيل المنشأة بما في ذلك :

أ) تغيرات في أنواع الرسائل التي يتم تسجيلها ؛

ب) سجل الملفات التي يتم تعديلها أو حذفها ؛

ج) القدرة على التخزين وسائل الإعلام في ملف السجل يتم تجاوز ، مما يترتب عليه إما الفشل في سجل الأحداث أو الإفراط في كتابة الأحداث المسجلة في الماضي.

قد تكون بعض مراجعة السجلات المطلوب حفظها كجزء من سياسة سجل الاحتفاظ بها أو بسبب المتطلبات اللازمة لجمع الأدلة والاحتفاظ بها (انظر أيضا 13.2.3).

معلومات أخرى

سجلات النظام غالبا ما تحتوي على كمية كبيرة من المعلومات والكثير منها هي دخيلة على الأمن الرصد. للمساعدة في تحديد الأحداث الهامة لأغراض رصد الأمن، فإن نسخ أنواع الرسالة المناسبة تلقائيا إلى سجل الثانية، و/ أو استخدام الأدوات المساعدة لنظام أو أدوات مناسبة لإجراء مراجعة ملف الاستجواب والترشيد ينبغي النظر فيها.

سجلات النظام في حاجة إلى الحماية، لأنه إذا كانت البيانات يمكن تعديل أو حذف البيانات في نفوسهم، قد وجودها خلق شعور زائف بالأمان.

د) نظام التنبيهات أو الفشل.

4.10.10 مدير ومشغل الجذوع

التحكم

مسؤول النظام وأنشطة المشغل يجب أن يكون نظام تسجيل.

توجيهات التطبيق

سجلات ينبغي أن تشمل ما يلي:

أ) في الوقت الذي حدث (النجاح أو الفشل) وقعت؛

ب) معلومات عن هذا الحدث (مثل التعامل مع الملفات) أو فشل (خطأ وعلى سبيل المثال وقعت اتخاذ الإجراءات التصحيحية) ؛

ج) التي تمثل والمسؤول أو المشغل الذي كان ضالعا ؛

د) العمليات التي كانوا متورطين.

المسؤول عن النظام وسجلات المشغل ينبغي أن يعاد النظر على أساس منتظم.

معلومات أخرى

ونظام كشف التسلل خارج تمكنت من السيطرة على النظام ومسؤولي الشبكات يمكن استخدامها لرصد أنشطة ونظام إدارة الشبكة من أجل الامتثال.

5.10.10 خطأ تسجيل

التحكم

وينبغي أن يكون للتسجيل أخطاء والمطلوب تحليلها واتخاذ الإجراءات الملائمة.

توجيهات التطبيق

أخطاء ذكرت من قبل المستخدمين أو عن طريق نظام برامج تتعلق بمشكلات مع معالجة المعلومات أو نظم الاتصالات وينبغي أن يتم تسجيل. ينبغي أن تكون هناك قواعد واضحة للتعامل مع تقارير الاعطال بما في ذلك :

أ) استعراض للخطأ سجلات لضمان أن أخطاء قد تم حلها بصورة مرضية ؛

ب) إعادة النظر في اتخاذ تدابير تصحيحية لضمان أن الضوابط لم الشبهة ، وأن الإجراءات التي اتخذت لديه تفويض كامل.

وينبغي التأكد من أن يتم تمكين تسجيل الخطأ ، إذا كان هذا النظام هو وظيفة متاحة.

معلومات أخرى

قطع الأشجار من الأخطاء والعيوب يمكن أن تؤثر على أداء النظام. وينبغي لمثل قطع الأشجار يتم تمكين من الموظفين الأكفاء ، وعلى المستوى المطلوب للتسجيل من النظم الفردية وينبغي أن يـتم تحديدها بواسطة لتقييم المخاطر ، مع الأخذ في الاعتبار تدهور الأداء.

6.10.10 ساعة التزامن

التحكم

الساعات في جميع النظم ذات الصلة، معالجة المعلومات داخل المؤسسة أو المجال الأمني ينبغي أن يتزامن مع مصدر دقيقة متفق عليها الزمن.

توجيهات التطبيق

حيث كمبيوتر أو جهاز الاتصالات لديها القدرة على العمل في الوقت الحقيقي على مدار الـساعة ، يجب تعيين هذه الساعة يكون لمعيار متفق عليه ، على سبيل المثال التوقيـت العـالمي (تعـم) أو بالتوقيت المحلي القياسية. حيث ان بعض الساعات ومن المعروف أن الانجراف مع الوقت ، ينبغي أن يكون هناك إجراء من شأنه أن يتحقق من ويصحح أي تفاوت كبير.

التفسير الصحيح للتاريخ / تنسيق الوقت من المهم ضمان أن يعكـس الطـابع الزمنـي للتـاريخ الحقيقي/ الساعة. خصوصيات المحلية (مثل الادخار الصيفي) ينبغي أن تؤخذ بعين الاعتبار.

معلومات أخرى

الإعداد الصحيح من الساعات الكمبيوتر المهم لضمان دقة ومراجعة السجلات ، والتي قـد تكـون هناك حاجة لإجراء تحقيقات أو كدليل في حالات قانونية أو تأديبية. مراجعة السجلات غير دقيقة قد تعوق مثل هذه التحقيقات ويلحق الضرر بمصداقية هذه الأدلة. ويمكن ربط عقارب الساعة الى زمن البث الإذاعي من ساعة ذرية وطنية يمكن استخدامها على مدار الساعة كما رئيـسية لـنظم قطـع الأشجار. ويمكن لشبكة بروتوكول الوقت أن تستخدم للحفاظ على كافة الملقمات فـي تـزامن مـع الساعة الرئيسية.

11 التحكم في الوصول

1.11 احتياج العمل للتحكم في الوصول

الهدف: التحكم في الوصول للمعلومات
إن الوصول للمعلومات ولأدوات معالجة المعلومات ولمعالجات العمل يجب أن يتم التحكم فيه بناء على مطلوبات العمل والأمن.
إن قواعد التحكم في الوصول للمعلومات يجب أن تأخذ في الاعتبار سياسات التصريح وتوزيع ونشر البيانات.

1.1.11 سياسة التحكم فى الوصول

التحكم

يجب أن يتم وضع سياسة لضبط الوصول للمعلومات قائمة على مطلوبات العمل والأمن. إن هذه السياسة يجب أن توثق وأن تراجع وتقيم.

موجهات التطبيق

يجب أن يتم وبوضوح تام وضع القواعد المتحكمة والمحددة لحقوق الوصول للمعلومات لكل مستخدم أو مجموعة من المستخدمين في سياسة التحكم في الوصول. إن قواعد التحكم في الوصول تشتمل كلاً من القواعد المنطقية والمادية.

عند وضع السياسة يجب اخذ الآتي في الإعتبار:

أ) الاحتياجات الأمنية الخاصة بكل تطبيق من تطبيقات العمل.

ب) تحديد كل المعلومات المرتبطة بتطبيقات العمل والمخاطر التي تواجهها.

ج) سياسات التصريح ونشر توزيع المعلومات (أنظر 2.7).

د) الاتساق بين سياسات التحكم في الوصول وتصنيف المعلومات للنظم والشبكات المختلفة.

هـ) الضوابط القانونية والالتزامات التعاقدية المتعلقة بحماية الوصول للبيانات والخدمات (أنظر 1.15).

و) الوصول للمعلومات اللازمة لأعمال المستخدمين داخل المنظمة.

ز) إدارة حقوق الوصول في بيئة شبكية وموزعة.

ح) تقسيم ضوابط الوصول كمثال إلى طلبات الوصول, تصريح وصول وإدارة وصول.

ط) متطلبات التصريح الرسمي لطلبات الوصول(أنظر 1.2.11) .

ي) متطلبات المراجعة الدورية لضوابط التحكم في الوصول (أنظر 4.2.11).

ك) إزالة حق الوصول (أنظر 3.3.8).

معلومات أخري

عند تحديد قواعد التحكم في الوصول يجب الأخذ في الاعتبار الآتي:

أ) التفريق بين القواعد الملزمة والموجهات الاختيارية أو الشرطية.

ب) وضع قواعد مبنية على مبدأ " بشكل عام أي شئ ممنوع ما لم يسمح به صراحة " وليس المبدأ الأضعف بشكل عام أي شئ مسموح به ما لم يمنع صراحة".

ج) تغيير مميزات المعلومات (أنظر 2.7) التي تنشأ آلياً بواسطة أدوات معالجة المعلومات.

د) تغيير صلاحيات المستخدم التي تم تخصيصها آلياً بواسطة نظام المعلومات أو تلك التي تم تحديدها بواسطة مدير النظام.

و) القواعد التي تحتاج لإجازة خاصة قبل تطبيقها وتلك التي لا تحتاج لذلك.

إن قواعد التحكم في الوصول يجب أن تدعم بواسطة إجراءات رسمية ومسئوليات محددة وواضحة (أنظر 3.1.6 ، 3.11 ، 1.4.10 ، 6.11).

2.11 إدارة وصول المستخدم

الهدف: ضمان وصول المستخدم المصرح له لنظم المعلومات ومنع غير المصرح لهم من الوصول.
يجب أن تكون هنالك إجراءات رسمية لضبط عملية الحصول على حقوق الوصول لنظم المعلومات والخدمات. إن هذه الإجراءات يجب أن تغطي كل مراحل دورة حياة وصول المستخدم، إبتداء من التسجيل الأولي للمستخدمين الجدد ونهايةً بإلغاء تسجيل المستخدمين الذين لم يعودوا في حاجة للوصول لنظم المعلومات والخدمات.
يجب إعطاء اهتمام خاص لمسألة ضبط عملية تخصيص صلاحيات وحقوق الوصول والتي من الممكن أن تسمح للمستخدمين بتجاوز ضوابط النظام.

1.2.11 تسجيل المستخدم

التحكم

يجب أن تكون هنالك إجراءات رسمية موضوعة لتسجيل المستخدم ولإلغاء التسجيل ويسمح بمقتضاها للمستخدم بالوصول لنظم المعلومات والخدمات أو لمنع المستخدم من الوصول.

موجهات التطبيق

إن إجراءات تسجيل وإلغاء تسجيل المستخدم يجب أن تشمل الآتي:

أ) استخدام محدد هوية مفرد مميز للمستخدم حتى يتثنى للمستخدمين التواصل فيما بينهم وتحمل مسئوليات أفعالهم. ان استخدام محددات هوية للمجموعات يجب أن يسمح به فقط في حالة ضرورة ذلك العمل.

ب) التحقق من أن المستخدم مصرح له من قبل مدير النظام لإستخدام نظم المعلومات أو الخدمات، كما إن وجود موافقة من الإدارة بحق الوصول للمعلومات قد تكون مطلوبة.

ج) التحقق من ان الصلاحيات الممنوحة للوصول للمعلومات تناسب إغراض العمل الذي يؤديه المستخدم ومتسقة مع السياسة الأمنية للمنظمة (أنظر 1.11 و3.1.10) .

د) إعطاء المستخدمين وثيقة مكتوبة تبين حقوقهم وصلاحياتهم في الوصول للمعلومات.

هـ) توقيع المستخدمين على إقرار بفهمهم لشروط الوصول للمعلومات.

و) ضمان أن لا يقوم مزودي الخدمة بالسماح للمستخدمين بالوصول حتى تكتمل إجراءات التصريح وتحديد الصلاحيات.

ز) إنشاء سجل رسمي للمستخدمين المسجلين لإستخدام خدمة معينة.

ح) الإزالة الفورية لحق الوصول أو إغلاق حسابات المستخدمين الذين تغيرت أعمالهم ومهامهم او تركوا العمل في المنظمة (أنظر 4.2.11).

ط) التحقق الدوري من عدم وجود حسابات للمستخدمين بلا فائدة وإغلاق او إزالة تلك الحسابات إن وجدت.

معلومات أخرى

يجب أن يؤخذ في الاعتبار أن الصلاحيات الممنوحة للمستخدمين للوصول للمعلومات مبنية على متطلبات العمل. كما يجب تضمين نصوص في التعاقدات الشخصية وتعاقدات الخدمات تحدد العقوبات التي تطال الأشخاص أو وكالات الخدمات في حالة محاولة الوصول لمعلومات أو خدمات غير مصرح بها.

2.2.11 إدارة الامتيازات

التحكم

إن تخصيص واستخدام الامتيازات يجب أن يكون مقيد ومتحكم فيه.

موجهات التطبيق

إن النظم متعددة المستخدمين والتي تحتاج لحماية من الوصول غير المصرح به يجب أن تخضع فيها عملية تخصيص الامتيازات للتحكم عبر عملية إصدار تصاريح رسمية. إن النقاط التالية يجب أخذها في الاعتبار:

أ) ن امتيازات الوصول لأى نظام (كمثال: نظام التشغيل، نظام إدارة قواعد البيانات....الخ) يجب ان تحدد، وكذلك المستخدمين الذين يحتاجون ان تخصص لهم هذه النظم.

ب) يجب أن تخصص الامتيازات للمستخدمين على أساس الحاجة للإستخدام بما يتسق مع سياسة التحكم في الوصول (أنظر 1.1.11). (أي الحد الأدنى للوصول الذي يفي بحاجة العمل).

ج) يجب ان يتم حفظ سجلات لكافة الامتيازات المخصصة ولعملية التصريح. ان الامتيازات يجب ان لا يتم الموافقة عليها حتى تنتهي عملية التصريح.

د) تطوير واستخدام برامج النظام يجب ان يشجع لتجنب الاحتياج للموافقة على امتيازات للمستخدمين.

هـ) تطوير واستخدام البرامج التى تتجنب الإحتياج لإمتيازات عند التنفيذ يجب ان تشجع.

و) الامتيازات يجب ان تخصص للمستخدم بمحدد هوية مختلف عن تلك المحددات التي تستخدم في العمل العادي.

معلومات اخرى

ان الاستخدام غير المناسب لامتيازات مدير النظام قد يكون عاملاً رئيسياً لفشل او خرق النظم.

3.2.11 إدارة كلمات مرور المستخدمين

التحكم

أن تخصيص كلمات المرور لمستخدمي النظام يجب أن يتم التحكم فيه عبر إجراءات إدارية رسمية.

موجهات التطبيق

إن عمليـة إدارة كلمـات المـرور يجـب أن تشـمـل المتطلبـات التاليـة:

أ) يجب أن يوقع مستخدمي النظام على وثيقة ملزمة بعدم إفشاء كلمات المرور الخاصة بهم وعلى الاحتفاظ بكلمات مرور المجموعة داخل أفرادها فقط. أن مثل هذه الوثيقة يمكن أن تكون جزء من شروط الاستخدام.

ب) عندما يطلب المستخدمين الاحتفاظ بكلمات المرور الخاصة بهم يجب ان يوفر لهم في البداية كلمة مرور آمنة مؤقتة وإرغامهم على تغييرها مباشرةً.

ج) وضع إجراءات للتحقق من هوية المستخدم قبل أن يمنح كلمة مرور جديدة أو مؤقتة أو يسمح له بإبدال كلمة المرور.

د) كلمات المرور المؤقتة يجب أن تعطي للمستخدمين بطريقة آمنة، ويجب تجنب استخدام وسيط ثالث أو رسائل الكترونية غير مشفرة.

هـ) كلمات المرور المؤقتة يجب إن تكون مفردة وغير قابلة للتنبؤ.

و) على المستخدمين تأكيد استلامهم لكلمات المرور.

ز) يجب عدم الاحتفاظ بكلمات المرور داخل الحاسوب بشكل غير محمي.

ح) كلمات المرور الأولية من مصنعي النظم يجب تبديلها أثناء عملية تنصيب النظم أو البرمجيات.

معلومات أخرى

ان كلمات المرور هي احد الوسائل العامة المستخدمة في تحديد هوية المستخدم قبل منحه إمكانية الوصول لنظم المعلومات أو الخدمات وفقاً للتخويل الممنوح له. التقنيات الأخرى المستخدمة في تحديد هوية وتوثيق المستخدم مثل الخواص البيولوجية كالتحقق بالبصمة، والتوقيع الرقمى أو استخدام الكروت الذكية يجب أخذها في الاعتبار إذا كانت مناسبة.

4.2.11 مراجعة صلاحيات وصول المستخدمين

التحكم

يجب على إدارة المنظمة مراجعة صلاحيات الوصول الممنوحة للمستخدمين بشكل دوري بإستخدام عملية رسمية.

موجهات التطبيق

عند مراجعة صلاحيات الوصول يجب اخذ النقاط التالية في الاعتبار:

(أ) يجب مراجعة صلاحيات الوصول للمستخدمين بشكل دوري منتظم، كمثال بعد كل 6 أشهر وبعد كل تغيير إداري يطرأ على مواقع العاملين بالمنظمة سواء أكان ذلك ترفيع أو تخفيض أو إعفاء من العمل (أنظر1.2.11).

ب) يجب مراجعة صلاحيات الوصول للمستخدمين وإعادة تخصيصها عندم تتم عملية نقل من وظيفة لأخرى داخل المنظمة.

ج) الترخيص بامتيازات حقوق وصول خاصة (انظر 2.2.11) يجب ان يراجع على فترات اقصر كمثال بعد كل 3 أشهر .

د) يجب التحقق من تخصيص الصلاحيات بشكل دوري للتأكد من عدم تجاوز المستخدمين لصلاحياتهم.

هـ) التغيير الذي يطرأ على الحسابات المميزة يجب ان يرصد لأغراض المراجعة الدورية.

معلومات أخرى

من الضروري ان تتم بشكل دوري مراجعة صلاحيات الوصول للمستخدمين للحفاظ على تحكم فاعل للوصول للبيانات وخدمات المعلومات.

3.11 مسئوليات المستخدم:

الهدف: منع وصول المستخدمين غير المصرح به واختراق او سرقة المعلومات ومرافق معالجة المعلومات.
يجب أن يكون المستخدمين ملمين بمسئولياتهم للحفاظ على فاعلية تحكمات الوصول للمعلومات, وعلى وجه الخصوص استخدام كلمات المرور وتأمين أجهزة المستخدم. يجب تطبيق سياسة نظافة المكتب والشاشة لتقليل مخاطر الوصول غير المصرح به او تخريب الأوراق والوسائط ومرافق معالجة المعلومات.

1.3.11 استخدام كلمات المرور:

التحكم

يجب على المستخدمين إتباع طرق آمنة للإختيار وإستخدام كلمات المرور.

موجهات التطبيق

يجب توجيه النصائح التالية للمستخدمين

أ) الحفاظ على سرية كلمات المرور.

ب) تجنب الكتابة أو الاحتفاظ بكلمة المرور على ورقة أو ملف برامجي أو جهاز محـمول باليد، ما لم تكن الطريقة المستخدمة آمنة وموافق عليها.

ج) التغيير الفوري لكمة المرور عند وجود أي مؤشرات لإحتمال إختراق النظام أو كلمة المرور.

د) اختيار كلمات مرور عالية الجودة بطول أدنى قياسى بحيث تكون:

1) سهلة التذكر.

2) غير معتمدة على أي شئ يمكن التنبؤ به بسهولة أو على معلومات لها علاقة بالمستخدم كالأسماء، أرقام الهاتف، تاريخ الميلاد....الخ

3) غير قابلة لهجمات القواميس (أي أنها لا تشتمل على كلمات قاموسية).

4) غير متماثلة، أي ليست كلها أرقام أو كلها حروف أبجدية.

هـ) تغير كلمات المرور بشكل منتظم، وتجنب إعادة استخدام كلمات مرور قديمة.

و) التغيير الفوري مع الدخول الأول لكلمة المرور المؤقتة.

ز) عدم استخدام كلمات المرور في أي عملية دخول آلي.

ح) عدم مشاركة الآخرين لكلمة المرور.

ط) عدم استخدام كلمة المرور نفسها لأغرض العمل ولأغرض لا علاقة لها بالعمل.

إذا احتاج المستخدم لإستخدام أكثر من نظام أو خدمة مما يتطلب استخدام أكثر من كلمة مرور واحدة، فيجب نصحه باستخدام كلمة مرور واحدة عالية الجودة لكافة النظم والخدمات.

معلومات اخرى

على إدارة مكتب المساعدة الذى يتعامل مع كلمات المرور المفقودة او المنسية من قبل المستخدمين إيلاء اهتمام خاص لهذه العملية، لانه من الممكن ان يكون طلب المساعدة وسيلة للهجوم على نظام كلمات مرور النظام.

2.3.11 أجهزة المستخدمين في غيابهم

التحكم

يجب على المستخدمين التحقق من ان الأجهزة التي يستخدمونها ستكون في غيابهم محمية بشكل مناسب.

موجهات التطبيق

يجب أن يكون كافة المستخدمين مدركين لمطلوبات وإجراءات تأمين وحماية الأجهزة التي يستخدمونها في غيابهم ومسئولياتهم في تطبيق هذه الحماية. يجب أن ينصح المستخدمين بالآتي:

أ) إنهاء البرامج والتطبيقات المستخدمة عند الانتهاء من استخدامها ما لم تكن هنالك طرق مناسبة للإغلاق الآلي كحافظات الشاشة المحمية بكلمة مرور.

ب) الخروج من المخدمات والحواسيب الشخصية عند الانتهاء من الاستخدام وليس فقط قفل الحاسوب أو الشاشة.

ج) تأمين الحواسيب الشخصية والطرفيات ضد الاستخدام غير المخول في فترة عدم الاستخدام.

معلومات أخرى

الأجهزة المركبة في أماكن العمل مثل مخدمات الملفات ومحطات العمل قد تحتاج لحماية خاصة من الاستخدام غير المصرح به عند تركها دون رقابة لفترة زمنية.

3.3.11 سياسة نظافة المكتب والشاشة

التحكم

يجب وضع سياسة لنظافة المكتب من الاوراق ووسائط التخزين المتحركة وسياسة لنظافة الشاشة لمرافق معالجة المعالجات.

توجيهات التطبيق

ان سياسة نظافة المكتب ونظافة الشاشة يجب ان تأخذ في الاعتبار تصنيف المعلومات (انظر 2.7)، المتطلبات القانونية والتعاقدية (انظر 1.15) والمخاطر المقابلة والتوجيهات الثقافية للمنظمة.
يجب الاخذ في الاعتبار الموجهات التالية:

أ) معلومات العمل الحساسة او الحرجة سواء اكانت على الورق او وسيط تخزين اليكتروني يجب حفظها بعيداً عدم الحوجة لها وخاصة عند خلو المكتب.

ب) الحواسيب والطرفيات يجب ان تكون مغلقة او محمية بوسائل اغلاق الشاشة ولوحة المفاتيح المتحكم فيها بكلمة مرور او أي وسيلة توثيق اخرى في غياب المستخدم، ويجب ان تحمي باقفال او كلمات مرور او غيرها من التحكمات عندما لا تكون في الاستخدام.

ج) نقاط البريد القادم والصادر واجهزة الفاكس يجب حمايتها.

د) الاستخدام غير المصرح به في النسخ وغيره من تكنولوجيا اعادة الانتاج (كمثال الماسحات، والكاميرات الرقمية) يجب ان تمنع.

هـ) الوثائق التي تحتوي على معلومات حساسة او مصنفة يجب ازالتها من الطابعات فوراً

معلومات اخرى

ان سياسة نظافة المكتب ونظافة الشاشة تقلل من مخاطر الوصول غير المصرح به وفقدان وتخزين المعلومات اثناء دوام العمل الرسمي أو بعده. إن وسائل الحفظ الامن يمكن ان تحفظ المعلومات الموجودة بداخلها من الكوارث مثل النيران، الهزات الارضية، الفيضانات او الانفجارات، أيضا يجب النظر الى استخدام الطابعات بطريقة تسمح فقط لطالبي الطباعة بالحصول على المطبوعات وفقط عندما يكونون بجانب الطابعة.

4.11 التحكم في الوصول للشبكة

الهدف: منع وصول غير المصرح لهم لخدمات الشبكة .

يجب التحكم في وصول المستخدمين لخدمات الشبكة الداخلية والخارجية، و يجب ان لا يكون في وصول المستخدمين للشبكات وخدماتها تجاوزاً للتأمين اللازم لهذه الشبكات وخدماتها، كذلك يجب التحقق من الاتي:

أ) وجود واجهات مناسبة بين شبكة المنظمة وشبكات المنظمات الاخرى والشبكات العامة.

ب) تطبيق طرق مناسبة لتوثيق المستخدمين والاجهزة.

ج) وجود ضوابط تحكم وصول المستخدمين لخدمات المعلومات.

1.4.11 سياسة استخدام خدمات الشبكة

التحكم

يجب منح المستخدمين صلاحيات الوصول للخدمات المصرح لهم استخدامها فقط.

موجهات التطبيق

يجب وضع سياسة لاستخدام الشبكة وخدماتها، هذه السياسة يجب ان تغطي الاتي:

أ) الشبكات والخدمات الشبكية المسموح بالوصول اليها.

ب) اجراءات توثيق لتحديد من يسمح له بالوصول للشبكات والخدمات الشبكية.

ج) الضوابط الادارية والاجراءات اللازمة لحماية الوصول للإرتباطات والخدمات الشبكية.

د) الوسائل والطرق المستخدمة للوصول للشبكات والخدمات الشبكية (كمثال الشروط اللازمة للسماح باستخدام التلفون في الوصول لمزود خدمات انترنت او نظام بعيد).

ان سياسة استخدام خدمات الشبكة يجب ان تكون متسقة مع سياسة التحكم في الوصول لمصادر العمل (انظر 1.11).

معلومات أخرى

ان الارتباطات غير الآمنة وغير المصرح بها لخدمات الشبكة يمكن ان تؤثر على كل المنظمة لهذا إن وجود ضوابط متشددة للإرتباطات امر هام خاصة للتطبيقات الهامة والحساسة بالنسبة للعمل.

2.4.11 توثيق المستخدمين للإرتباطات الخارجية

التحكم

يجب استخدام طرق توثيق مناسبة للتحكم في وصول المستخدمين عن بعد.

موجهات التطبيق

توثيق المستخدمين عن بعد يمكن ان يتم، كمثال باستخدام طرق معتمدة عن علم التشفير، وسائل مادية، او بروتوكول تحدي واستجابة. من الممكن العثور على تطبيقات لهذه الطرق في العديد من حلول الشبكات الإفتراضية الخاصة.
خطوط الاتصال المخصصة يمكن ان تستخدم ايضاً لضمان مصدر الارتباطات.

إن إجراءات وتحكمات الاستدعاء الراجع يمكن ان توفر حماية من الارتباطات غير المصرح بها او غير المرغوب فيها لمرافق معالجة معلومات المنظمة. إن هذا النوع من التحكم يوثق المستخدمين الذين يحاولون انشاء ارتباط مع شبكة المنظمة من على البعد. عند استخدام هذا التحكم يجب على

المنظمة عدم استخدام خدمات الشبكة التي تضم تمرير المكالمة وإلا فيجب عليهم ايقاف استخدام مثل هذه المزايا لتجنب الضعف الملازم لتمرير المكالمة.

يجب ان تضمن عملية الاستدعاء الراجع ان عملية قطع اتصال فعلي على جانب المنظمة قد حدثت، وإلا فان المستخدم عن بعد يستطيع جعل الخط فاتحاً متظاهراً بان تأكيد الاستدعاء الراجع قد حدث، لهذا يجب ان يتم اختبار كلي لإجراءات وتحكمات الاستدعاء الراجع تحسباً لهذا الاحتمال.

ان طريقة توثيق العقدة يمكن استخدامها كطريقة بديلة لتوثيق مجموعات المستخدمين عن بعد حينما يكونوا مرتبطين بمرفق حاسوب امن ومتشارك. إن طرق علم التشفير، كمثال الطرق المعتمدة على شهادات الالة يمكن ان تسخدم في توثيق العقدة، وهي واحدة من حلول متعددة تعتمد عليها الشبكات الافتراضية الخاصة.

يجب ان تطبق تحكمات توثيق إضافية للتحكم في الوصول للشبكات اللاسلكية، وبشكل محدد فإن اهتماماً خاصاً يجب ان يعطى لعملية اختيار تحكمات (ضوابط) الشبكات اللاسلكية نتيجة للفرص الواسعة للوصول غير المكتشف والادخال في حركة الشبكة.

معلومات أخرى

ان الارتباطات الخارجية توفر إمكانية للوصول غير المرخص لمعلومات العمل. إن هنالك العديد من انواع طرق التوثيق بعضها يوفر مستوى أعلى من الحماية من بعضها الآخر، كمثال فإن الطرق المبنية على استخدام علم التشفير توفر توثيقاً أقوى. لهذا فمن المهم ان يتم تحديد مستوى الحماية المطلوب عبر عملية تقييم المخاطر كما إن تحديد مستوى الحماية مطلوب أيضاً من اجل اختيار طريقة التوثيق المناسبة.

ان وجود وسيلة للإرتباط الآلي بحاسوب بعيد من الممكن ان توفر طريقة للحصول على وصول غير مرخص لتطبيقات العمل ان هذا الأمر مهم بشكل خاص اذا كان الارتباط يستخدم شبكة خارج تحكم ادارة امن المنظمة.

3.4.11 تحديد المعدات في الشبكات

التحكم

يجب ان ينظر الى عملية التحديد الآلي للمعدات كوسيلة لتوثيق الارتباطات من مواقع ومعدات معينة.

توجيهات التطبيق

إن عملية تحديد المعدات يمكن ان تستخدم اذا كان مهماً أن تتم مبادرة الاتصال من موقع او من معدات معينة. ان المحدد او المميز الموجود داخل المعدة او الملتصق بها يمكن استخدامه تبيان ما اذا كانت هذه المعدة مسموح لها بالارتباط بالشبكة. يجب ان تبين هذه المحددات او المميزات وبوضوح الشبكة المسموح للمعدة الارتباط بها في حالة وجود اكثر من شبكة واحدة وخاصة اذا كانت هذه الشبكات مختلفة الأهمية والحساسية.

قد يكون من الضروري الأخذ في الاعتبار توفير الحماية المادية للمعدة في سبيل الحفاظ على أمن محدد او مميز المعدة.

معلومات أخرى

ان هذا التحكم يمكن ان يكمل بطرق توثيق أخرى لمستخدم المعدة (انظر 2.4.11). توثيق المعدة يمكن تطبيقه كإضافة لتوثيق المستخدم.

4.4.11 حماية مرافئ التحليل والتهيئة عن بعد

التحكم

يجب ان يتم التحكم في الوصول المادي والفيزيائي لمرافئ التحليل والتهيئة.

توجيهات التطبيق

ان التحكمات الفاعلة للوصول لمرافئ التحليل والتهيئة تشمل استخدام الأقفال والإجراءات الداعمة لضبط الوصول المادى للمرفأ. كمثال لهذه الإجراءات الداعمة هو ضمان ان الوصول لمرافئ التحليل والتهيئة يتم بترتيبات بين مدير خدمة الحاسوب والأفراد الداعمين للعتاد/ البرمجيات الذين يرغبون في الوصول.

المرافئ والخدمات وغيرها من الوسائل المنصبة على حاسوب او مرفق شبكي والتي ليست مطلوبة تحديداً لأداء إحدى مهام العمل يجب عدم تنشيطها او إزالتها.

معلومات أخرى

العديد من أنظمة الحاسوب ونظم الشبكات والاتصال تنصب مع مرافق للتحليل والتهيئة عن بعد لاستخدامها بواسطة مهندس الصيانة، وبالتالي إذا لم تتوفر الحماية فإن هذه المرافئ ستصبح وسيلة للوصول غير المشروع.

5.4.11 تقسيم الشبكات

التحكم

يجب ان يتم تقسيم مجموعات خدمات المعلومات، المستخدمين ونظم المعلومات على الشبكات.

توجيهات التطبيق

واحدة من طرق التحكم في امن الشبكات الكبيرة هي ان تقسم الشبكات الى نطاقات شبكات منطقية منفصلة، كمثال ان تقسم شبكة منظمة الى نطاقات شبكة داخلية ونطاقات شبكة خارجية وتحمي كل منهما بمحيط امني.

يمكن تطبيق مجموعة من التحكمات على نطاقات شبكات منطقية مختلفة من اجل تقسيم إضافي لبيئة امن الشبكة، كمثال ان تقسم الشبكة الى نظم الوصول العام، الشبكات الداخلية والأصول الحرجة.

ان تعريف النطاقات يجب ان يتم بناء على تقييم المخاطر والمتطلبات الأمنية المختلفة اللازمة لكل نطاق.

يمكن إنشاء محيط شبكة بتنصيب بوابة بين الشبكتين المراد ربطهما للتحكم في الوصول وفي تدفق المعلومات بين النطاقين (الشبكتين). هذه البوابة يجب ان تهيأ لتصفية حركة البيانات بين النطاقين (انظر 6.4.11 و 7.4.11) وان تمنع الوصول غير المصرح به وفقاً لسياسة المنظمة للتحكم في الوصول (انظر 1.11). كمثال لهذا النوع من البوابة هو التقنية المسماة بجدار النار. من الطرق الأخرى التي يمكن استخدامها في تقسيم النطاقات المنطقية المنفصلة هي تقييد الوصول للشبكة باستخدام الشبكات الافتراضية الخاصة لمجموعات المستخدمين داخل المنظمة.

يمكن تقسيم الشبكات ايضاً باستخدام اجهزة وظائف الشبكات كمثال محول عناوين بروتوكول الإنترنت، في هذه الحالة فإن النطاقات المنفصلة يمكن ان تجسد بالتحكم في تدفق البيانات باستخدام قدرات التوجيه/ التحويل لهذه الأجهزة مثل قوائم التحكم في الوصول.

إن المنهج الذي يستخدم في تقسيم الشبكات الى نطاقات يجب ان يعتمد على سياسة التحكم في الوصول ومتطلبات الوصول (انظر 1.10)، ويجب ايضاً ان يأخذ في الاعتبار التكلفة المقابلة والاثر على الاداء عند استخدام تقنية بوابة او توجيه شبكة مناسبة (انظر 6.4.11 و 7.4.11).

بالاضافة لذلك، فإن تقسيم الشبكات يجب ان يتم بناءا على قيمة و تصنيف المعلومات المخزنة او المعالجة فى الشبكة، مستويات الثقة أو خطوط العمل من أجل إنقاص الأثر الكلى لتوقف الخدمة.

يجب الوضع فى الإعتبار تقسيم الشبكات اللاسلكية من الشبكات الداخلية والخاصة، ولأن محيط الشبكات اللاسلكية غير معرف جيدا يجب القيام بعملية تقييم للمخاطر ليتثنى تحديد التحكمات اللازمة للحفاظ على تقسيم الشبكة.

معلومات اخرى

لقد اصبحت الشبكات عادة ما تمتد خارج الحدود التقليدية للمنظمة، اذ ان شركاء العمل قد يرغبون في الارتباط مع المنظمة او التشارك في معالجة المعلومات والمرافق الشبكية. ان هذا التمدد قد يترتب عليه زيادة مخاطر الوصول غير المصرح به لانظمة المعلومات الموجودة التي تستخدم الشبكة والتي قد يحتاج بعضها للحماية من مستخدمي الشبكات الاخرى نتيجة لحساسيتها او حرجيتها.

6.4.11 التحكم في إرتباط الشبكة

التحكم

يجب تقييد قدرات المستخدمين في الارتباط بالشبكات المتشاركة وخاصة تلك التي تجاوز محيط المنظمة وفقاً لسياسة التحكم في الوصول ومتطلبات تطبيقات العمل (انظر 1.11).

توجيهات التطبيق

ان حقوق المستخدمين في الوصول للشبكة يجب الحفاظ عليها وتحديثها وفقاً لسياسة التحكم في الوصول (انظر 1.1.11).

إن قدرات المستخدمين في الارتباط يمكن قصرها عبر بوابات الشبكة التي تقوم بتصفية حركة الشبكة باستخدام جداول أو قواعد معرفة مسبقاً. من أمثلة التطبيقات التي يجب أن يطبق فيها القصر:

أ) التراسل كمثال البريد الالكتروني.
ب) نقل الملفات
ج) الوصول المتفاعل
د) الوصول للتطبيق

ربط حقوق الوصول للشبكة بزمن معين من اليوم او بتاريخ معين يجب ان يؤخذ في الاعتبار.

معلومات أخرى

إن إدراج التحكمات في تقييد قدرات المستخدمين في الارتباط قد يكون مطلوباً في سياسة التحكم في الوصول للشبكات المتشاركة وخاصة تلك التي تتجاوز حدود المنظمة.

7.4.11 التحكم في توجيه الشبكة.

التحكم

يجب تطبيق تحكمات التوجيه في الشبكات لضمان ان الارتباط وتدفق المعلومات لا يخرق سياسة التحكم في الوصول لتطبيقات العمل.

توجيهات التطبيق

يجب ان تعتمد تحكمات التوجيه على طرق اختبار لعناوين مصدر ومستقبل موجبه .

يمكن استخدام البوابات الآمنة للتحقق من عناوين المصدر والمستقبل في نقاط تحكم شبكية داخلية وخارجية اذا تم استخدام تقنية بروكسى أو تقنية مترجم عناوين شبكة.

الذين يقومون بالتطبيق يجب عليهم ان يكونوا على وعي بقوة وضعف أي من الآليات والطرق المطبقة. إن متطلبات التحكم في توجيه ألشبكه يجب ان يبنى على سياسة التحكم في الوصول (انظر 1.11).

معلومات أخرى

الشبكات المتشاركة وخاصةً تلك التي تتجاوز حدود المنظمة قد تحتاج لتحكمات توجيه إضافية. إن هذا ينطبق تحديداً عندما تكون الشبكات متشاركة مع مستخدمي طرف ثالث.

5.11 التحكم في الوصول لنظم التشغيل

الهدف: منع الوصول غير المصرح به لنظم التشغيل.

يجب استخدام تقنيات الأمن لقصر الوصول لنظم التشغيل على المستخدمين المصرح لهم فقط. ان التقنيات الأمنية يجب ان تكون قادرة على إدارة الآتي:

أ) توثيق المستخدمين المصرح لهم مع وجود سياسة لضوابط الوصول.

ب) تسجيل محاولات التوثيق الناجحة والفاشلة.

ج) تسجيل استخدام صلاحيات النظام الخاصة.

د) إصدار تنبيهات عند حدوث تجاوز لسياسة امن النظام.

هـ) توفير وسائل مناسبة لتوثيق المستخدمين.

و) تقييد ارتباط المستخدمين بالنظام عندما يكون ذلك مناسباً.

1.5.11 إجراءات الدخول الآمن

التحكم

يجب التحكم في الوصول لنظم التشغيل بواسطة إجراءات دخول آمن.

توجيهات التطبيق

إن إجراءات الدخول لنظام التشغيل يجب أن تصمم بحيث تقلل من فرص الوصول غير المصرح به للنظام. لهذا فإن إجراءات الدخول يجب ان تكشف عن اقل قدر ممكن من المعلومات المتعلقة بنظام التشغيل حتى لا تتوفر معلومات عن النظام تساعد المستخدمين غير المصرح لهم. ان الإجراءات الجيدة للدخول يجب ان تتصف بالاتي:

أ) لا تظهر معرفات عن النظام او التطبيق لحين الانتهاء بنجاح من عملية الدخول للنظام.

ب) إظهار مذكرة تنبيه عامة بان النظام يجب ان يستخدم فقط بواسطة المستخدمين المصرح لهم.

ج) عدم إظهار أي رسائل مساعدة أثناء عملية الدخول للنظام يمكن ان تساعد المستخدمين غير المصرح لهم .

د) التحقق من معلومات الدخول للنظام يجب ان تتم بعد الانتهاء تماماً من إدخال كافة البيانات المطلوبة، وفي حالة وجود خطأ ما في بيانات الدخول يجب ان لا يوضح النظام أي جزء من البيانات هو الصحيح او أي جزء هو الخطأ.

هـ) تحديد عدد محاولات الدخول للنظام, كمثال ثلاثة محاولات مع اخذ الآتي في الاعتبار:

1) تسجيل محاولات الدخول الناجحة و الفاشلة

2) فرض انتظار زمني قبل السماح بأي محاولات دخول تالية او رفض أي محاولات تالية بدون عملية توثيق محددة.

3) فصل ارتباطات وصل البيانات.

4) إرسال رسالة تحذير على شاشة النظام عند الوصول للحد الأقصى لمحاولات الدخول.

5) ربط تحديد عدد محاولات إدخال كلمة المرور بالحد الأدنى لطول كلمة المرور وبقيمة النظام الذي نود حمايته.

و) تحديد الزمن الأدنى والأقصى المسموح به لإجراءات عملية الدخول, وإذا تم تجاوز الزمن يجب على النظام إنهاء عملية الدخول.

ز) إظهار المعلومات التالية عند اكتمال عملية الدخول للنظام بنجاح:

1) تاريخ وزمن الدخول الناجح السابق.

2) تفاصيل محاولات الدخول الفاشلة منذ آخر دخول ناجح.

ح) عدم إظهار كلمة المرور المدخلة أو إخفاء حروف كلمة المرور بإستخدام رموز.

ط) عدم نقل كلمات المرور كنص صريح عبر الشبكة.

معلومات أخرى

إذا تم نقل كلمات المرور صريحة عبر الشبكة إثناء جلسة الدخول فإنها تكون عرضة للإلتقاط بواسطة برامج التجسس على الشبكة.

2.5.11 تحديد هوية المستخدم وتوثيقه

التحكم

يجب أن يكون لكل مستخدم محدد هوية للإستخدام الشخصي، كما يجب أن يكون هنالك أسلوب توثيق تم اختياره للتحقق من هوية المستخدم المدعي.

توجيهات التطبيق

إن هذا التحكم يجب أن يطبق على جميع المستخدمين بما في ذلك الأشخاص المسئولين عن الدعم الفني، المشغلين، مديري الشبكة، مبرمجي النظم ومديري قواعد البيانات.

يجب استخدام محدد الهوية لتعقب أفعال مستخدمي النظام, كما يجب ان لا تتم الأفعال والأنشطة العادية للمستخدمين من حسابات خاصة ذات صلاحيات.

في الظروف الاستثنائية التي تكون فيها منفعة للعمل يمكن ان يتشارك مجموعة من المستخدمين في استخدام محدد هوية واحد، وفي هذه الحالة يجب توثيق موافقة الإدارة وإضافة ضوابط للمحاسبة.

ان استخدام محددات الهوية العامة يجب الا يسمح به إلا عندما تكون الأفعال أو وظائف الوصول التي يتيحها محدد الهوية لا تحتاج للتعقب والرصد (كمثال الوصول للقراءة فقط).

عندما تكون هنالك حاجة لوسائل توثيق او تحقق متينة لمحددات الهوية، فإن وسائل توثيق بديلة لكلمات المرور مثل الوسائل البيولوجية، التشفير، الكروت الذكية وغيرها يجب ان يتم استخدامها.

<u>معلومات أخرى</u>

ان كلمات المرور (انظر 1.3.11 و 3.5.11) تمثل طريقة شائعة لتوفير التوثيق والتحقق إعتماداً على سر يعرفه المستخدم فقط. نفس النتائج يمكن الوصول إليها بإستخدام طرق التشفير وبروتوكولات التوثيق. إن قوة الوسيلة المستخدمة في التوثيق يجب ان تتناسب مع أهمية وقيمة المعلومات المراد الوصول إليها.

3.5.11 نظام إدارة كلمات المرور

التحكم

يجب ان يكون نظام إدارة كلمات المرور نظاماً متفاعلاً ومحققاً لجودة كلمات المرور.

توجيهات التطبيق

يجب ان يحقق نظام إدارة كلمات المرور الآتي:

أ) فرض استخدام محددات الهوية وكلمات المرور لتحقيق المحاسبية.

ب) يسمح للمستخدمين باختيار وتغيير كلمات المرور الخاصة بهم وتضمين إجراءات تأكيد لتسمح بإعادة الإدخال عند الخطأ.

ج) فرض اختيار كلمات مرور جيدة (انظر 1.3.11).

د) فرض تغيير كلمات المرور (انظر 1.3.11).

هـ) إجبار المستخدمين على تغيير كلمة المرور عقب الدخول الأول (انظر 3.2.11).

و) إنشاء سجل كلمات المرور المستخدمة سابقاً وفرض عدم إعادة استخدامها.

ز) عدم إظهار كلمات المرور على الشاشة عند إدخالها.

ح) تخزين ملفات كلمات المرور منفصلة عن بيانات نظام التطبيق.

ط) تخزين ونقل كلمات المرور في شكل محمي.

معلومات أخرى

إن كلمات المرور تمثل احد الطرق الرئيسية في التحقق من أحقية المستخدم في الوصول لخدمات النظام.

إن بعض التطبيقات تتطلب إن يتم تخصيص كلمات المرور بواسطة جهة مستقلة مخولة، في هذه الحالة فإن النقاط (ب)، (د) و (هـ) أعلاه لا يمكن تطبيقها. في معظم الحالات فإن كلمات المرور يتم اختيارها بواسطة المستخدمين (أنظر 1.3.11 دليل استخدام كلمات المرور).

4.5.11 استخدام أدوات النظام المساعدة

التحكم

إن استخدام برامج النظام المساعدة التي تمكن من تجاوز ضوابط النظام والتطبيق يجب ان يقيد استخدامها ويتحكم فيها جيداً.

توجيهات التطبيق

عند استخدام أدوات النظام المساعدة يجب اخذ الآتي في الاعتبار:

أ) استخدام إجراءات التحقق والتوثيق والتخويل لأدوات النظام.

ب) فصل أدوات النظام المساعدة عن برمجيات التطبيق.

ج) قصر استخدام أدوات النظام على الحد الأدنى من المستخدمين الموثوق بهم والمصرح لهم.

د) توثيق الاستخدام غير المخطط لأدوات النظام.

هـ) قصر فترة توفر أدوات النظام.

و) رصد كافة استخدامات أدوات النظام.

ز) تعريف وتدوين مستويات تخويل أدوات النظام.

ح) إزالة كافة أدوات النظام والبرامجيات التي لا حاجة لها.

ط) عدم إتاحة أدوات النظام للمستخدمين المصرح لهم الوصول للتطبيقات الموجودة على النظم التي تتطلب فصل بين الواجبات.

معلومات أخرى

معظم نظم التشغيل لها برامج أدوات نظام قد تسمح بتجاوز ضوابط النظام والتطبيق.

5.5.11 إنتهاء زمن الجلسة

التحكم

ان الجلسات غير النشطة يجب إنهائها بعد فترة زمنية محددة.

توجيهات التطبيق

يجب ان تكون هنالك وسيلة لنظافة شاشة الجلسة ومن ثم إغلاق التطبيق والارتباط بالشبكة بعد فترة زمنية محددة غير نشطة. إن طول أو قصر هذه الفترة الزمنية يجب ان يعكس حجم المخاطر في مجال التطبيق وأهمية المعلومات المعالجة والمخاطر المرتبطة بأجهزة المستخدمين.

يمكن ان تكون هنالك بعض النظم المزودة بوسائل إنهاء جلسة تنظف شاشة المستخدم فقط وتمنع الوصول او الاستخدام غير المصرح به ولكنها لا تنهي وتغلق التطبيق او الارتباط بالشبكة.

معلومات أخرى

ان هذا التحكم ذو أهمية خاصة في أماكن المخاطر العالية التي تشمل الأماكن العامة او المناطق خارج نطاق إدارة امن المنظمة. ان جلسات المستخدمين يجب إغلاقها لمنع وصول الأشخاص غير المصرح لهم للتطبيقات والنظم لمنع هجمات تعطيل الخدمة.

6.5.11 تحديد زمن الارتباط

التحكم

يجب وضع قيود على الزمن الذي يمكن فيه للمستخدمين الارتباط لتوفير مزيد من الأمن للتطبيقات عالية المخاطر.

توجيهات التطبيق

يجب ان يؤخذ في الاعتبار وضع ضوابط وقيود على زمن الارتباط بتطبيقات الحاسوب الحساسة, خاصة من الأماكن عالية المخاطر. من أمثلة هذه الضوابط والقيود:

أ) استخدام فترات زمنية معرفة مسبقاً.

ب) تغيير زمن الارتباط بساعات العمل المكتبية فقط اذا لم تكن هنالك حاجة لساعات عمل إضافية.

ج) إعادة توثيق المستخدم بعد كل فترة زمنية.

معلومات أخرى

ان تحديد وتغيير زمن الارتباط بخدمات الشبكة يقلل فرص وصول المستخدمين غير المصرح لهم للنظام.

6.11 التحكم في الوصول للتطبيق والمعلومات

الهدف: هو منع المستخدمين غير المصرح لهم من الوصول للمعلومات التي تحملها تطبيقات النظام.
يجب أن يتم استخدام وسائل أمنية لتقييد الوصول للتطبيق وللتعامل داخل التطبيق.
ان الوصول لبرمجيات ومعلومات التطبيق يجب أن يكون قاصراً فقط على المستخدمين المصرح لهم، لهذا يجب على تطبيقات النظام أن:
أ) تتحكم في وصول المستخدم للمعلومات ولوظائف التطبيق بناء على سياسة معرفة للتحكم في الوصول للتطبيق.
ب) توفر حماية من الوصول غير المشروع الذي قد يستخدم أي من برامج النظم المساعدة أو برمجيات نظم التشغيل أو البرامج الضارة التي لها القدرة على تجاوز ضوابط وتحكمات التطبيق.
ج) لا تخرب التطبيقات الأخرى التي تتشارك معها في الموارد.

1.6.11 تقييد الوصول للمعلومات.

التحكم

يجب تقييد وصول المستخدمين ومشغلي التطبيق للمعلومات ووظائف التطبيق بناء على سياسة معرفة للتحكم في الوصول.

توجيهات التطبيق

ان القيود على الوصول يجب ان توضع بناءاً على متطلبات العمل لكل تطبيق. إن سياسة التحكم في الوصول للتطبيق المعين يجب ان تكون منسجمة مع السياسة العامة للوصول في المنظمة (انظر1.11).
ان تطبيق الموجهات التالية يجب ان يؤخذ في الاعتبار لدعم متطلبات تغيير الوصول:

أ) توفير قوائم تساعد على ضبط الوصول لوظائف التطبيق.

ب) التحكم في صلاحيات المستخدمين كمثال القراءة، الكتابة، المسح، التشغيل.

ج) التحكم في صلاحيات التطبيقات الأخرى.

د) التأكد من ان مخرجات نظم التطبيقات التي تعالج معلومات حساسة تشتمل فقط على معلومات ذات علاقة بإستخدام المخرجات وأنها مرسلة لطرفيات أو أماكن مصرح بها.

2.6.11 عزل النظم الحساسة

التحكم

يجب أن تكون للنظم الحساسة بنية حوسبة مخصصة و معزولة.

توجيهات التطبيق

النقاط التالية يجب أخذها في الاعتبار لعزل النظم الحساسة

أ) إن أهمية وحساسية نظام التطبيق يجب ان تحدد بوضوح وتوثق بواسطة مالك التطبيق.

ب) عندما يكون التطبيق الحساس يعمل في بيئة متشاركة مع تطبيقات اخرى، يجب تحديد هذه التطبيقات والمخاطر الناجمة عن هذا التشارك وان يتم قبولها بواسطة مالك التطبيق الحساس.

معلومات أخرى

إن بعض نظم التطبيقات تكون عالية الحساسية لفقدان مؤثر مما يتطلب أن تعامل بشكل خاص. إن هذه الحساسية قد تكون مؤشراً لأن يتم التعامل مع نظام التطبيق:

أ) بالتنفيذ على حاسوب مخصص، أو

ب) بالتشارك مع الموارد فقط مع أنظمة تطبيقات موثوق بها.

إن عزل التطبيقات الحساسة يمكن أن يتم بإستخدام طرق منطقية او فيزيائية (مادية). (انظر 5.4.11).

7.11 الحوسبة المتنقلة

الهدف: ضمان امن المعلومات عند استخدام الحوسبة المتنقلة ومرافق العمل عن بعد.
إن الحماية المطلوبة يجب ان تتناسب مع المخاطر الناتجة عن استخدام هذه الطرق في العمل.
عند استخدام الحوسبة المتنقلة يجب التحسب للمخاطر الناشئة عن العمل في بيئة غير محمية وتطبيق حماية مناسبة.
في حالة العمل عن بعد يجب على المنظمة حماية موقع العمل عن بعد وضمان ان ترتيبات مناسبة قد تم اتخاذها لهذه الطريقة من العمل.

1.7.11 الحوسبة المتنقلة والاتصالات

التحكم

يجب أن تكون هنالك سياسة موضوعة كما يجب أن تكون هنالك قياسات أمنية للحماية ضد المخاطر الناشئة عن استخدام وسائل الحوسبة المتنقلة والاتصالات.

توجيهات التطبيق

عند استخدام وسائل الحوسبة المتنقلة والاتصالات كالحواسيب المحمولة، الكروت الذكية، الهواتف الخلوية، ...الخ. يجب إعطاء اهتمام خاص للتأكد من أن معلومات العمل ليست عرضة للاستخدام غير المشروع. إن سياسة الحوسبة المتنقلة للمنظمة يجب أن تحتوي على متطلبات الحماية المادية، ضوابط الوصول، طرق التشفير، النسخ الاحتياطي والحماية من الفيروسات. أيضا يجب أن تشتمل هذه السياسة على قواعد ونصائح في ربط الوسائل المتنقلة بالشبكات وعلى دليل لاستخدام هذه الوسائل في الأماكن العامة .

يجب الاحتياط والحذر عند استخدام وسائل الحوسبة المتنقلة في الأماكن العامة، وفي غرف الاجتماعات وغيرها من الأماكن خارج محيط المنظمة. يجب أن تكون الحماية متوفرة لتجنب الوصول غير المشروع للمعلومات المخزنة أو المعالجة بواسطة الوسائل المتنقلة أو كشفها.

على مستخدمي الوسائل المتنقلة في الأماكن العامة أخذ الحيطة والحذر من مخاطر التلصص بالنظر من أشخاص غير مخولين ووضع إجراءات مضادة للبرمجيات الضارة (انظر 10-4).

يجب أن يتم عمل نسخ احتياطية لمعلومات العمل الهامة بشكل دوري، كما يجب أن تتوفر الأدوات التي تمكن من إجراء عملية النسخ الاحتياطي للمعلومات بسهولة وسرعة. إن هذه النسخ الاحتياطية يجب أن تحمى بشكل مناسب ضد السرقة أو فقدان المعلومات.

يجب أن تعطى الوسائل المتنقلة الحماية المناسبة عند ربطها بالشبكات، كما يجب أن تكون عمليات الوصول عن بعد لمعلومات العمل عبر الشبكات العامة باستخدام الوسائل المتنقلة مرتبطة بعملية تحديد وتوثيق للهوية مع وجود آليات للتحكم في الوصول.

إن وسائل الحوسبة المتنقلة يجب أن تحمى مادياً ضد السرقة، كما يجب أن تكون هنالك إجراءات محددة في حالة السرقة أو الفقدان تأخذ في الاعتبار الجوانب القانونية، التأمين وغيرها من متطلبات أمن المنظمة.

إن الأجهزة والمعدات التي تحمل معلومات مهمة وحساسة يجب أن لا تترك دون مستخدم أو أن يتم استخدام أقفال خاصة لتأمين الجهاز.(انظر 5.2.9).

يجب أن يتم تدريب مستخدمي وسائل الحوسبة المتنقلة لزيادة إدراكهم بالمخاطر الناجمة عن استخدام مثل هذه الوسائل والضوابط الأمنية التي يجب تطبيقها لحماية هذه الوسائل.

معلومات أخرى

إن الارتباط اللاسلكي بالشبكات هو ارتباط مماثل لأنواع الارتباط الأخرى بالشبكات، ولكن هنالك اختلافات مهمة يجب أخذها في الاعتبار عند تحديد التحكمات، إن الاختلافات الأساسية هي:

أ) بعض بروتوكولات الأمن اللاسلكي غير ناضجة وبها ضعف معروف.

ب) المعلومات المخزنة في حواسيب متنقلة قد لا يمكن عمل نسخ احتياطي لها نتيجة لمحدودية السعة العريضة للشبكة أو لأن الحواسيب المتنقلة قد لا تكون مرتبطة بالشبكة في الزمن المجدول لعملية النسخ الاحتياطي.

2.7.11 العمل عن بعد

التحكم

يجب أن يتم وضع وتطبيق سياسة وإجراءات وخطط تشغيل لأنشطة العمل عن بعد.

توجيهات التطبيق

يجب على المنظمات السماح بأنشطة العمل عن بعد فقط عندما تكون المنظمة مطمئنة لوجود تمكمات وترتيبات أمنية مناسبة منسجمة مع السياسة الأمنية للمؤسسة.

يجب أن تتوفر حماية مناسبة لمواقع العمل عن بعد ضد سرقة الأجهزة والمعلومات، الكشف والاطلاع غي المشروع على المعلومات، الوصول غير المشروع للنظم الداخلية للمنظمة أو الاستخدام السيئ لمرافق المنظمة.

إن أنشطة العمل عن بعد يجب أن تخصص وتضبط بواسطة الإدارة التي يجب عليها التأكد من وجود ترتيبات أمنية مناسبة لمثل هذا النوع من العمل.

عند التفكير في استخدام مواقع عمل عن بعد يجب أخذ الأمور التالية في الحسبان :

أ) وجود أمن مادي لموقع العمل عن بعد آخذين في الاعتبار الأمن المادي للمباني وللبيئة المحلية.

ب) البيئة المادية المقترحة عن للعمل عن بعد.

ج) متطلبات أمن الاتصالات، آخذين في الاعتبار الحاجة للوصول عن بعد للنظم الداخلية للمؤسسة، أهمية المعلومات التي يتم الوصول إليها ونقلها عبر روابط الاتصال وحساسية النظم الداخلية.

د) المخاطر الناجمة عن استخدام مواقع العمل عن بعد من قبل أشخاص غير مصرح لهم الوصول للمعلومات ومصادر المنظمة (مثل أفراد العائلة والأصدقاء).

هـ) استخدام شبكات المنازل في تهيئة خدمات الشبكات اللاسلكية.

و) السياسات والإجراءات اللازمة لمنع الاعتراضات المتعلقة بحقوق الملكية الفكرية على الأجهزة المملوكة لأشخاص.

ز) الوصول للمعدات والأجهزة الخاصة (عند اختبار أمن الجهاز أو إجراء تحقيق)، الذي يمكن أن يكون ممنوعاً بالقانون.

ح) إتفاقيات ترخيص البرامجيات التى تعطى المنظمات حق الترخيص للبرامجيات العميلة على محطات العمل المملوكة بشكل خاص للموظفين، المتعاقدين ومستخدمى الطرف الثالث.

ط) الحماية باستخدام مضادات الفيروسات ومتطلبات جدار النار.

إن الإرشادات التي يجب أخذها في الاعتبار هي:

أ) توفير المعدات المناسبة والأثاث لأنشطة العمل عن بعد، حيث يحظر استخدام المعدات الخاصة التي لا تخضع لتحكم المنظمة.

ب) تعريف العمل المسموح به، ساعات العمل، تصنيف المعلومات التي يمكن الوصول اليها والنظم الداخلية والخدمات التي يصرح للمستخدم عن بعد بالوصول اليها.

ج) توفير معدات الاتصال بما في ذلك طرق تأمين الوصول عن بعد.

د) الأمن المادي.

هـ) قواعد وإرشادات حول وصول أفراد العائلة والزوار للمعدات والمعلومات.

و) توفير الدعم العتادي والبرمجي والصيانة.

ز) توفير التأمين.

ح) إجراءات للنسج الاحتياطي واستمرارية العمل.

ط) المراجعة ومراقبة الأمن

ي) إزالة الترخيص وحقوق الوصول وإعادة المعدات عند انتهاء أنشطة العمل عن بعد.

<u>معلومات اخرى</u>

ان العمل عن بعد يستخدم تقنيات الاتصالات لتمكين الأفراد من العمل عن بعد من مواقع محددة خارج منظماتهم.

12 حيازة وتطوير وصيانة أنظمة المعلومات

1.12 متطلبات أمن نظم المعلومات

الهدف: ضمان ان الأمن عبارة عن جزء لا يتجزأ من نظم المعلومات.
تشمل نظم المعلومات أنظمة التشغيل ,البنية التحتية, تطبيقات الأعمال، حاضرة المنتجات والخدمات وتطوير تطبيقات للمستخدم. التصميم والتنفيذ لنظام المعلومات الداعمة للعملية التجاريـة يمكـن أن يكون حاسما بالنسبة للأمن. المتطلبات الأمنية ينبغي تحديدها والاتفاق عليها قبل وضـع أو تنفيـذ المعلومات.
جميع متطلبات الأمن ينبغي أن تحدد عند مرحلة متطلبات المشروع و تبرر وتوثـق كجـزء مـن مجمل الأعمال التجارية في حالة نظام المعلومات.

1.1.12 تحليل وتحديد مواصفات متطلبات الأمن

التحكم

بيانات متطلبات العمل الجديدة لنظم المعلومات، أو إدخال تحسينات على قائمة نظـم المعلومـات ينبغي أن يحدد الاحتياجات الأمنية التي تسيطر عليه.

توجيهات التطبيق

مواصفات متطلبات الضوابط ينبغي أن تنظر إلى أن الضوابط آليـة تكـون مدخلـة فـي نظـام المعلومات، والحاجة إلى دعم دليل الضوابط. اعتبارات مماثلة ينبغي تطبيقها عند تقييم مجموعـات البرمجيات, تطويرها أو شراؤها لتطبيقات الأعمال.

المتطلبات الأمنية والضوابط التجارية يجب أن تعكس قيمـة المعلومـات والموجـودات المعنيـة والأعمال التجارية والأضرار المحتملة التي قد تنجم عن فشل أو عدم وجود الأمن.

متطلبات النظام لأمن المعلومات وعمليات لأمن التطبيقات ينبغي ان تكون متكاملة فـي المراحـل الأولى من مشاريع نظام المعلومات. الضوابط المعروضة في مرحلة التصميم أرخص بشكل ملحوظ للتنفيذ والصيانة أكثر من تلك المدرجة أثناء أو بعد التنفيذ.

إذا كانت المنتجات مشتراة، هنالك تجارب رسمية و عملية مكتسبة ينبغي إتباعها. العقود التي مع الممول ينبغي أن تتناول متطلبات الأمن المحددة. عندما تكون وظيفة الأمن في منتج مقترح لا تلبي

المتطلبات المحددة سيكون هنالك خطر وينبغي إعادة النظر في الضوابط قبل شراء المنتج. عند توريد وظيفة إضافية اصبحت تسبب خطرا امنيا تعطل أوهيكل التحكم المقترح ينبغي أن يستعرض لتحديد ما إذا كان يمكن الإفادة من الوظائف المعززة المتاحة.

معلومات أخرى

لأسباب تتعلق بالتكاليف، والإدارة قد يمكن الاستفادة من تقييم مستقل ومعتمد للمنتجات. مزيد من المعلومات عن معايير التقييم لتكنولوجيا منتجات الأمن يمكن العثور عليها في المنظمة الدولية للتوحيد القياسي واللجنة الانتخابية المستقلة 15408 وغيرها من معايير التقييم أو التصديق.

المنظمة الدولية للتوحيد القياسي واللجنة الانتخابية المستقلة 13335-3 يعطيان توجيهات بشأن استخدام عمليات إدارة المخاطر لتحديد الاحتياجات اللازمة لضوابط أمنية.

2.12 *تصحيح المعالجة في التطبيقات*

الهدف: منع الأخطاء والخسائر، والتعديل غير المصرح به أو إساءة استخدام المعلومات الواردة في الطلبات. ضوابط ملائمة وينبغي أن تصمم في التطبيقات، بما في ذلك تطبيقات مستخدم مطورة لضمان معالجة صحيحة. وينبغي أن تشمل هذه الضوابط التثبت من صحة البيانات المدخلة، المعالجةالداخلية والبيانات المخرجة.
ضوابط إضافية قد تكون لازمة لأنظمة تعالج ، أو لديها تأثير على معلومات حساسة، قيمة أو حرجة. مثل هذه الضوابط لابد أن تحدد على أساس متطلبات الأمن وتقييم المخاطر.

1.2.12 التحقق من صحة البيانات المدخلة

التحكم

البيانات المدخلة إلى التطبيقات ينبغي التحقق منها لضمان أن هذه البيانات صحيحة ومناسبة.

توجيهات التطبيق

ضوابط يجب أن تطبق على مدخلات المعاملات التجارية، البيانات الواقفة (مثل أسماء وعناوين، حدود الرصيد, أرقام العملاء المرجعية)، و جداول المعاملات (مثل أسعار البيع أسعار تحويل العملة ، معدلات الضرائب). المبادئ التوجيهية التالية يجب أخذها في عين الاعتبار:

أ) المدخلات المزدوجة أو غيرها من مدخلات الضوابط، مثل التحقق من الحدود أو الحد من الحقول لمجالات محددة من البيانات المدخلة، للكشف عن الأخطاء التالية:

1) خارج إطار مجموعة القيم.

2) الحروف الغير صحيحة في مجال بيانات .

3) بيانات مفقودة أو غير كاملة.

4) تجاوز الحدود العليا والسفلى لحجم البيانات.

5) بيانات مراقبة غير مصرح بها أو متعارضة .

ب) الاستعراض الدوري لمحتوى مجالات رئيسية أو ملفات البيانات للتأكد من صحتها وصلاحيتها.

ج) تفقد مطبوعة الوثائق المدخلة لأية تغييرات غير مصرح بها(جميع التغييرات للوثائق إلمدخلة ينبغي أن يؤذن بها).

د) إجراءات للاستجابة للأخطاء المتحققة.

هـ) إجراءات اختبار معقولية مدخلات البيانات.

و) تحديد مسؤوليات جميع الموظفين المشاركين في عملية إدخال البيانات.

ز) إنشاء سجل للأنشطة التي تشارك في عملية إدخال البيانات .

معلومات أخرى

الفحص التلقائي والتثبت من البيانات المدخلة يمكن اعتباره، عند الاقتضاء، للحد من احتمال حدوث أخطاء لمنع الهجمات بما في ذلك فيض العازل وحقن الرمز.

2.2.12 مراقبة المعالجة الداخلية

التحكم

مراجعات التحقق ينبغي أن تدرج في طلبات للكشف عن أي فساد معلومة خلال معالجة الأخطاء أو الأفعال المتعمدة.

توجيهات التطبيق

التصميم والتنفيذ للتطبيقات ينبغي أن تكفل ان مخاطر معالجة الفشل التي تؤدى إلى فقدان النزاهـة قد قل. للنظر في مجالات محددة تشمل:

أ) استخدام إضافة وتعديل وحذف وظائف لتنفيذ تغييرات على البيانات؛

ب) إجراءات لمنع تشغيل برامج بطريقة خطا أو التشغيل بعد فشل قبل المعالجة .

ج) استخدام برامج ملائمة للتعافي من الفشل لضمان المعالجة الصحيحة البيانات؛

د) الحماية من الهجمات باستخدام التجاوزات الفاصلة / المفرطة.

ينبغي إعداد قائمة مرجعية مناسبة و توثيق الأنشطة، والنتائج ينبغي أن تظـل آمـن أمثلـة عـن الضوابط التي يمكن إدخالها:

أ) الدورة أو دفعة ضوابط ، للتوفيق بين ملف بيانات موازين المعاملات بعد استكمال؛

ب) تحقيق التوازن بين ضوابط للتحقق من الأرصدة الافتتاحية ضـد الأرصـدة الختاميـة السابقة، وهي:

1) الاستعداد للضوابط التي تديرها؛

2) ملف تحديث مجاميع؛

3) برنامج لبرنامج الرقابة؛

ج) المصادقة على نظام توليد بيانات المدخلات .

د) التحقق من السلامة والصحة أو غيرها من السمات الأمنية للبيانات أو البرمجيات المنزلة أو المحملة ، بين أجهزة الكمبيوتر المركزية وأجهزة الكمبيوتر عن بعد.

هـ) بعثرة مجاميع السجلات والملفات؛

و) التحقق للتأكد من أن تطبيق هذه البرامج تدار في الوقت الصحيح؛

ز) التحقق للتأكد من أن البرامج الشغالة في الترتيب الصحيح وإنهاءها في حالة وجود فشل والمزيد من المعالجات توقف إلى أن تحل المشكلة.

ح) إنشاء سجل للأنشطة التي تشارك في المعالجة.

<u>معلومات أخرى</u>

البيانات التي تم ادخالها بشكل صحيح يمكن أن تفسدت بسبب أخطاء الأجهزة، أو من خلال أخطاء المعالجة والأفعال المتعمدة.الفحوص المطلوبة سوف تسعتمد على طبيعة الطلب و أثر الأعمال فـي أي من البيانات الفسادة.

3.2.12 صحة الرسالة

التحكم

الاحتياجات اللازمة لضمان صحة وسلامة وحماية الرسالة التي في التطبيقات، ينبغي أن تحدد,كذلك تحديد ضوابط مناسبة وتنفيذها.

توجيهات التطبيق

تقييما للمخاطر الأمنية ينبغي الاضطلاع بها لتحديد مـا إذا كانـت تـصحيح الرسـالة مطلـوب ولتحديد أنسب الطرق للتنفيذ.

معلومات أخرى

تقنيات التشفير يمكن استخدامها كوسيلة ملائمة لتنفيذ رسالة توثيق.

4.2.12 التحقق من صحة البيانات المخرجة

التحكم

البيانات الناتجة من تطبيق ينبغي التحقق منها للتأكد من ان معالجة المعلومات المخزنـة صـحيحة وملائمة للظروف.

توجيهات التطبيق

التحقق على المخرجات قد يشمل ما يلي:

أ) معقولية الفحوص لاختبار ما إذا كانت البيانات الناتجة معقولة.

ب) حساب تحكم المصالحة لضمان معالجة جميع البيانات.

ج) توفير ما يكفي من المعلومات للقارئ، أو لاحقة لنظام المعالجة لتحديد الدقة والكمال والدقة، وتصنيف المعلومات؛

د) إجراءات للاستجابة على اختبارات التحقق من المخرجات.

هـ) تحديد مسؤوليات جميع الموظفين العاملين في عملية إنتاج البيانات.

و) إنشاء سجل للأنشطة في عملية المصادقة على البيانات الناتجة.

معلومات أخرى

عادة،النظم والتطبيقات شيدت على افتراض قيامها مناسبة التثبت والتحقق والاختبار،الناتج سـتكون دائما صحيحة. ومع ذلك، فإن هذا الافتراض ليس صحيحا دائما، أي أن النظم التي تم اختبارها قـد لا تزال تنتج نتائج غير صحيحة في بعض الظروف.

3.12 *ضوابط التشفير*

الهدف: لحماية سرية، صحة أو سلامة المعلومات من خلال وسائل الترميز. ينبغي أن توضع سياسة عند استخدام ضوابط التشفير. وينبغي أن تكون هنالك إدارة رئيسية لدعم استخدام تقنيات التشفير.

1.3.12 السياسات بشأن استخدام ضوابط التشفير

التحكم

ينبغي وضع وتنفيذ سياسة عنداستخدام ضوابط الترميز لحماية المعلومات.

توجيهات التطبيق

عند وضع سياسة ترميز ينبغي النظر فيما يلي:

أ) نهج الإدارة نحو استخدام ضوابط الترميز عبر المنظمة، بما في ذلك المبادئ العامـة التي تحدداي معلومات تجارية يجب أن تكون محمية.

ب) بناءا على تقييم المخاطر، يجب تحديد مستوى الحماية المطلوب مع الأخـذ الاعتبـار نوع, قوة ونوعية خوارزمية التشفير المطلوبة.

ج) استخدام التشفير لحماية المعلومات الحساسة المنقولة عن طريق وسائط متحركـة أو قابلة للإزالة، أجهزة أو عبر خطوط الاتصالات؛

د) النهج للإدارة الرئيسية، بما في ذلك طرق التعامل مع حماية مفاتيح الترميز واسترجاع المعلومات المرمزة في حالة خسارة المفاتيح، تضررها أو تعرضها للخطر

هـ) الأدوار والمسؤوليات، على سبيل المثال من هو المسؤول عن

1) تنفيذ السياسة.

2) الإدارة الرئيسية، بما فيها توليد المفتاح .

و) المعايير التي يتعين اعتمادها من أجل التنفيذ الفعال لجميع أنحاء المنظمة (وهو الحل الذي يستخدم في العمليات التجارية).

ز) أثر استخدام معلومات مشفرة في الضوابط التي تعتمد على تفتيش المحتوى (على سبيل المثال للكشف عن الفيروس).

عند تنفيذ سياسة التشفير للمنظمة، ينبغي النظر إلى اللوائح والقيود العالمية التي يمكـن أن تنطبـق على استخدام تقنيات الترميز في أجزاء مختلفة من العالم وعلى المسائل العابرة للحدود مـن تـدفق المعلومات المشفرة.

ضوابط التشفير يمكن استخدامها لتحقيق أهداف أمنية مختلفة، مثل:

أ) السرية: استخدام التشفير لحماية معلومات حساسة أو حرجة، إما مخزنة أو منقولة.

ب) السلامة/الصحة: استخدام التوقيعات الرقمية او رموز توثيق الرسائل لحماية صحة وسلامة معلومات حساسة أو حرجة سواء كانت مخزنة أومرسلة .

ج) عدم التنصل: استخدام تقنيات الترميز للحصول على دليل وقوع أو عدم وقوع حدث أو عمل.

<u>معلومات أخرى</u>

اتخاذ قرار بشأن ما إذا كان حل الترميز مناسب يجب أن ينظر إليه باعتباره جزءا مـن العمليـة الأوسع لتقييم المخاطر واختيار الضوابط. هذا التقييم يمكن أن يستخدم لتحديد ما إذا كـان ضـابط الترميز مناسب، كذلك أي نوع من الرقابة يجب أن يطبق ولأي غرض ولأي عمليات تجارية.

وجود سياسة عند استخدام ضوابط الترميز امر ضروري لتحقيق أقصى قدر من المنـافع وتقليـل مخاطر استخدام تقنيات الترميز إلى أدنى حد، وكذلك لتجنب الاستخدام غير المناسب أو الـصحيح.

عند استخدام التوقيعات الرقمية، وينبغي النظر في أي من التشريعات ذات الصلة، ولا سيما التشريعات التي تصف الشروط تحت اي توقيع رقمي ملزم قانونيا.

ينبغي السعي وراء مشورة متخصصة لتحديد المستوى المناسب من الحماية وتحديد مواصفات مناسبة يمكنها توفير الحماية المطلوبة ودعم تنفيذ نظام إدارة رئيسية آمنة.

المنظمة الدولية للتوحيد القياسي واللجنة الانتخابية المستقلة JTC1 SC27 وضعتا العديد من المعايير المتعلقة بضوابط التشفير. أبعد المعلومات يمكن العثور عليها أيضا في IEEE P1363 ، والمبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية في الترميز.

2.3.12 إدارة المفتاح

التحكم

إدارة المفتاح يجب أن تكون قائمة على دعم استخدام المنظمة لتقنيات التشفير.

توجيهات التطبيق

جميع مفاتيح التشفير ينبغي أن تكون محمية من التعديل،الخسارة والدمار. وعلاوة على ذلك، المفاتيح السرية والخاصة تحتاج للحماية من الإفصاح غير المرخص به. المعدات المستخدمة في توليد، تخزين وحفظ المفاتيح ينبغي حمايتها جسديا.

نظام إدارة المفتاح ينبغي أن تستند إلى مجموعة متفق عليها من المعايير والإجراءات، وطرق آمنة:

أ) توليد مفاتيح لنظم ترميز مختلفة وتطبيقات مختلفة.

ب) توليد والحصول على شهادات المفتاح العام.

ج) توزيع المفاتيح للمستخدمين المقصودين ، بما في ذلك كيفية تنشيط المفاتيح عند استقبالها.

د) تخزين المفاتيح ، بما في ذلك كيفية أذن للمستخدمين الحصول على المفاتيح ؛

هـ) تغيير أو تحديث المفاتيح بما في ذلك قواعد بشأن متى ينبغي تغيير المفاتيح وكيفية تحقيق ذلك .

و) التعامل مع المفاتيح المشبوهة.

ز) إلغاء المفاتيح بما في ذلك كيفية سحب أو عدم استخدام المفاتيح ، على سـبيل المثـال عندما تتم الشبهة في المفاتيح أو عندما يقوم المستخدم بترك المنظمة (وفي هذه الحالة يجب وضع المفاتيح في الأرشيف) .

ح) استعادة المفاتيح التي فقدت أو فسدت في إطار إدارة استمرارية الأعمال ، على سبيل المثال لاسترداد معلومات مشفرة .

ط) حفظ المفاتيح على سبيل المثال للحصول على المعلومات المحفوظة أو المدعومة.

ي) تدمير المفاتيح .

ك) مراجعة الأنشطة المتصلة بإدارة المفتاح.

من أجل تقليل احتمال الضرر، التنشيط، والتعطيل يجب تحديد مواعيد للمفاتيح حتى يمكن استخدامها لفترة محدودة من الزمن. هذه الفترة الزمنية ينبغي ان تعتمد على الظروف التي يستخدم فيها تحكـم الترميز ، وكذلك المخاطر المتصورة.

بالإضافة إلى إدارة المفاتيح السرية والخاصة بامان، ينبغي أيضاالخذ صحة المفاتيح العموميـة فـي الاعتبار. عملية التوثيق هذه يمكن أن تتم باستخدام شهادات مفتاح عمومي والتي عادة ما تـصدرها سلطة تصديق، والتي ينبغي أن تكون منظمة معترف بها مع ضوابط وإجراءات مناسبة لتوفير القدر اللازم من الثقة.

مضمون اتفاقيات مستوى الخدمة، أو عقود مع موردين خارجيين لخدمات الترميـز علـى سـبيل المثال مع سلطة التصديق ، ينبغي أن يشمل مسائل مسؤولية وموثوقية الخدمات وأوقات الاسـتجابة لتوفير الخدمات.

<u>معلومات أخرى</u>

إن إدارة مفاتيح الترميز ضرورية للاستخدام الفعال لتقنيات التشفير.

المنظمة الدولية للتوحيد القياسي واللجنة الانتخابية المستقلة 11770 تزود بمزيد من المعلومات عن إدارة المفتاح. هنالك نوعان من تقنيات الترميز وهما:

أ) تقنيات مفتاح سري، حيث طرفين أو أكثر يشتركان في نفس المفتاح ويـستخدم هـذا المفتاح لتشفير وفك المعلومات, هذا المفتاح يجب ان يبقى سريالأن أي شخص يصل الـى المفتاح يستطيع أن يفك شفرة جميع المعلومات المشفرة بهذا المفتاح ، أو لإدخال معلومـات غير مصرح بها باستخدام المفتاح.

ب) تقنيات مفتاح عمومي، حيث كل مستخدم لديه زوج مفاتيح ، مفتاح عمـومي(والـذي يمكن كشفه لأي احد)، ومفتاح خاص (والذي يجب ان يبقى سريا)؛ تقنيات المفتاح العمومي يمكن أن تستخدم للتشفير ولإنتاج توقيعات رقمية.

هناك تهديد بخروج توقيع رقمي عن طريق استبدال مفتاح المستخدم العمومي. هذه المشكلة تعـالج عن طريق استخدام شهادة مفتاح عمومي.

تقنيات الترميز يمكن أيضا استخدامها لحماية مفاتيح الترميز. إجراءات يمكن ان تؤخذ في الاعتبار لمعالجة طلبات قانونية للوصول الى مفاتيح ترميز، على سبيل المثال قد تكون هناك حاجـة لجعـل المعلومات المرمزة متوفرة في شكل غير مرمز ، كدليل في دعوى قضائية.

4.12أمن ملفات النظام

الهدف: لضمان أمن ملفات النظام. يجب التحكم في الوصول إلى ملفات النظام و شفرة مصدر البرنامج، ومشاريع تكنولوجيا المعلومات ودعم الأنشطة التي أجريت في طريقة آمنة. ينبغي اخذ الحيطة لتجنب تعرض بيانات حساسة في بيئات اختبار.

1.4.12 مراقبة البرامج التشغيلية

<u>التحكم</u>

ينبغي أن تكون هناك إجراءات للتحكم في تركيب البرمجيات على نظم التشغيل.

<u>توجيهات التطبيق</u>

للتقليل من خطر الفساد للنظم التشغيلية،المبادئ التوجيهية التالية ينبغي أن تعتبـر للـسيطرة علـى التغييرات:

أ) تحديث البرمجيات التشغيلة،التطبيقات ، و مكتبات البرنامج يجب فقـ ـ ـ ـط أن تقـ ـام بواسطة مدراء مدربين على الإدارة المناسبة المصرح به

ب) نظم التشغيل ينبغي ان تتعامل مع رمز تنفيذي مثبت وليس تطوير رمز أو مجمعين.

ج) نظام التشغيل وبرامج التطبيقات لا يمكن تنفيذها إلا بعد تجارب مكثفة وناجحة وينبغي أن تشمل الاختبارات اختبارات على قابلية الاستخدام، والأمن، والآثار على أنظمة أخـرى وسهولة الاستعمال، وينبغي أن تتم الاختبارات على نظم مستقلة. ويجب التأكـد مـن أن جميع مكتبات مصادر البرنامج المقابلة تم تحديثها.

د) ونظام التحكم في التكوين ينبغي أن يستخدم للاحتفاظ بالسيطرة على جميع برامج التنفيذ كذلك توثيق النظام.

هـ) يجب أن تكون هنالك إستراتيجية تراجع قبل التغييرات التي ستنفذ.

و) ينبغي عمل سجل مراجعة بكل تحديثات مكتبات برنامج التشغيل.

ز) ينبغي الإبقاء على الإصدارات السابقة من برامج التطبيقات كتدبير طوارئ

ح) النسخ القديمة من البرنامج ينبغي أن تحفظ، مع كـل مـا يلـزم مـن معلومـات و معاملات وإجراءات وتفاصيل الضبط ، كذلك برامج الدعم طالمـا ظلـت البيانـات فـي الأرشيف.

برنامج توريد البائع المستخدم في نظم التشغيل ينبغي ان يحفظ فى مستوى مدعوم من المورد. مـع مرور الوقت ، بائعي البرامج ستتوقف على دعم الإصدارات القديمة من البرنامج. يجب أن تنظـر المنظمة في مخاطر الاعتماد على البرمجيات غير المدعومة.

أي قرار لرفـع مـستوى إصـدار جديـد ينبغـي أن يأخـذ فـي الاعتبـار متطلبـات العمـل للتغيير ، وأمن الإصدار الجديد.مثال استحداث وظائف أمنية جديدة أو عدد وجسامة المشاكل الأمنية

التي تؤثر على هذه النسخة. البرمجيات يجب أن تطبق عندما يمكن أن تساعد على إزالة أو تقليـل نقاط الضعف الأمنية.

يجب إعطاء الموردين الوصول الفيزيائي أو المنطقي عند الضرورة لأغراض الدعم مـع موافقـة الإدارة.كما ينبغي مراقبة أنشطة المورد.

برامج الحاسوب يمكن ان تعتمد على البرمجيات المزودة خارجيا والنماذج ، والتي يجب مراقبتهـا والسيطرة عليها لتجنب التغييرات غير المصرح بهاالتي يمكن أن تسبب ضعف أمني.

معلومات أخرى

يجب أن يتم رفع مستوى أنظمة التشغيل فقط عندما تكون هنالك حاجة للقيام بذلك على سبيل المثال إذا كانت النسخة الحالية مـن نظـام التـشغيل لـم تعـد تـدعم متطلبـات العمـل. الترفيعـات لا ينبغي أن تحدث لمجردان هنالك نسخة جديـدة مـن نظـام التـشغيل. الإصـدارات الجديـدة. لأنظمة التشغيل قد تكون أقل أمنا وأقل استقرارا ، وأقل فهما من النظم الحالية.

2.4.12 حماية بيانات اختبار النظام

التحكم

يجب اختيار بيانات الاختبار بعناية، وحمايتها والتحكم بها.

توجيهات التطبيق

يجب تجنب استخدام قواعد بيانات التشغيل التي تحتوي على معلومات شخـصية أو أي معلومـات حساسة.

لأغراض الاختبار. إذا تم استخدام معلومات شخصية أو حساسة لأغراض التجارب يجب إزالة أو تعديل المحتويات والتفاصيل الحساسة بعد التعرف عليها قبل الاستخدام. يجـب تطبيـق المبـادئ التوجيهية التالية لحماية البيانات التشغيلية عند استخدامها لأغراض الاختبار:

أ) إجراءات تحكم الدخول، والتي تطبق على نظـم التطبيـق التـشغيلية ، كمـا ينبغـي إن تطبق على نظم تطبيق الاختبار.

ب) ينبغي أن يكون هنالك إذن منفصل في كل مرة يتم نسخ المعلومات العملية لاختبار تطبيق النظام.

ج) يجب أن تمحى المعلومات العملية من نظام تطبيق الاختبار فور انتهاء الاختبار.

د) نسخ واستخدام المعلومات العملية يجب أن يكون مسجلا لتقديم مراجعة الحسابات.

معلومات أخرى

عادة يتطلب اختبار القبول والنظام كميات كبيرة من البيانات التجريبية التي هي أقرب ما تكون من البيانات التشغيلية.

3.4.12 مراقبة الدخول إلى شفرة مصدر البرنامج

التحكم

الوصول إلى شفرة مصدر البرنامج يجب أن يكون مقيدا.

توجيهات التطبيق

يجب التحكم بصرامة تامة في الوصول الى شفرة مصدر البرنامج والمواد المرتبطة بها (مثل التصاميم والمواصفات و خطط التحقق وخطط المصادقة) ، وذلك لمنع دخول وظيفة غير مصرح بها وتفادي التغييرات غير المقصودة. يمكن تحقيق ذلك لشفرة مصدر البرنامج، عن طريق السيطرة على الخزينة المركزية لمثل هذه الشفرة، ويفضل في مكتبات مصدر البرنامج. المبادئ التوجيهية التالية يجب ان تؤخذ في عين الاعتبار لسيطرة الوصول إلى مكتبات مصدر البرنامج من أجل الحد من احتمالات فساد برامج الكومبيوتر:

أ) حيثما كان ذلك ممكنا ، لا يجب ان تحمل مكتبات مصدر البرنامج في نظم تشغيل.

ب) يجب التحكم في شفرة مصدر البرنامج و مكتبات مصدر البرنامج وفقا للإجراءات المعمول بها.

ج) لا يجب اعطاء موظفي الدعم وصول غير مقيد إلى مكتبات مصدر البرنامج.

د) يجب ان يتم تحديث مكتبات مصدر البرنامج والمواد المرتبطة بها،وإصدار مصادر البرنامج للمبرمجين فقط بعد استقبال الإذن المناسب.

هـ) يجب وضع قوائم البرنامج في بيئة آمنة.

و) يجب حفظ جميع المنافذ التي تمت لمكتبات مصدر البرنامج في سجل مراجعة.

ز) صيانة ونسخ مكتبات مصدر البرنامج يجب أن تخضع لإجراءات مراقبة تغيير

صارمة.

معلومات أخرى

شفرة مصدر البرنامج عبارة عن شفرة تمت كتابتها بواسطة مبرمجين كما تم جمعها(وربطها) لخلق تنفيذات. بعض لغات البرمجة لا تميز رسميا بين شفرة المصدر والتنفيذات حيث ان التنفيذات تم إنشاءها في الوقت الذي يتم تنشيطها.

معايير ايزو 10007 والمنظمة الدولية للتوحيد القياسي واللجنة الانتخابية المستقلة 12207 تقدم مزيد من المعلومات عن إدارة الضبط وعملية دورة حياة البرمجيات.

5.12 الأمن في دعم وتطوير العمليات

الهدف : المحافظة على أمن برمجيات ومعلومات نظام التطبيق. يجب أن تكون هنالك رقابة صارمة على المشروع وبيئات الدعم. المديرين المسئولين عن أنظمة التطبيق يجب أن يكونوا مسئولين أيضا عن أمن المشروع أو بيئة الدعم.حيث أنهم يجب أن يتأكدوا من أن جميع تغييرات النظام المقترحة تم إعادة النظر فيها للتأكد من أنهم لا ينالوا من أمن كل من النظام أو بيئة العمل.

1.5.12 تغيير إجراءات المراقبة

التحكم

تنفيذ التغييرات يجب السيطرة عليها عن طريق استخدام إجراءات مراقبة تغيير رسمية.

توجيهات التطبيق

الإجراءات الرسمية لرقابة التغيير يجب ان تكون موثقة وقسرية لتقليل فساد نظم المعلومات إلى أدنى حد. استحداث نظم جديدة وتغييرات كبيرة على نظم موجودة يجب ان تتبع عملية رسمية للتوثيق،المواصفات،الاختبار، مراقبة الجودة و تنفيذ متحكم به.

هذه العملية يجب أن تشمل تقييم المخاطر، وتحليل الآثار المترتبة على التغييرات، وتحديد الضوابط الأمنية اللازمة. كما ينبغي لهذه العملية أن تضمن بان الأمن و إجراءات الرقابة المتواجدين ليسا مشبوهين، أيضا تضمن بان مبرمجي الدعم قد أعطوا الدخول فقط لتلك الأجزاء من النظام اللازمة لعملهم ، كذلك يتم الحصول على موافقة واتفاق رسميين لأي تغيير.

حيثما يكون ذلك عمليا، إجراءات مراقبة التغيير التنفيذي والتطبيق ينبغي أن تكون متكاملة.

إجراءات التغيير ينبغي أن تشمل :

أ) المحافظة على سجل مستويات تصريح متفق عليها.

ب) ضمان ان التغييرات مقدمة بواسطة مستخدمين مصرح لهم.

ج) إعادة النظر في الضوابط وإجراءات السلامة للتأكد من أنها لن تتاثر بالتغييرات .

د) التعرف على جميع البرامج، والمعلومات، وقواعد البيانات والأجهزة التي تتطلب تعديل.

هـ) الحصول على موافقة رسمية لمقترحات مفصلة قبل بدء العمل.

و) ضمان أن المستخدمين المصرح لهم يقبلون التغييرات قبل تنفيذها.

ز) ضمان أن يتم تحديث مجموعة وثائق النظام عند انتهاء كل تغيير وحفظ أو التخلص من الوثائق القديمة.

ح) المحافظة على التحكم في الإصدار لجميع تحديثات البرامج.

ط) الحفاظ على مراجعة الحسابات لجميع طلبات التغيير.

ي) لضمان ان وثائق التشغيل و إجراءات المستخدم تغير عن الضرورة لتبقى مناسبة.

ك) ضمان ان تنفيذ التغييرات يتم في الوقت المناسب،ولا يخل بالعمليات التجارية ذات الصلة.

معلومات أخرى

تغيير البرامج التي يمكن أن يؤثر على البيئة التنفيذية.

الممارسات الجيدة تشمل اختبار البرمجيات الجديدة في بيئة منفصلة من كل مـن بيئـات الإنتـاج والتطوير. وهذا يوفر وسيلة للسيطرة على البرمجيات الجديدة والسماح لمزيد من حماية المعلومات العملية المستخدمة لاغراض اختباريه. وينبغي أن تشمل هذه البقع، وحزم الخدمات، وغيرهـا مـن المستجدات. التحديثات الآلية لا يجب أن تستخدم على النظم الحرجة حيث بعض التحديثات قد تسبب الفشل للتطبيقات الحرجة.

2.5.12 استعراض فني للتطبيقات بعد تغييرات نظام التشغيل

التحكم

عندما يتم تغيير نظم التشغيل تطبيقات الأعمال الحاسمة يجب ان تستعرض وتختبر لضمان عدم وجود تأثير سلبي على عمليات تنظيمية أو أمنية.

توجيهات التطبيق

هذه العملية ينبغي أن تشمل:

أ) إعادة النظر في رقابة التطبيق وإجـراءات الـسلامة للتأكـد مـن أنهـا لـم تتـأثر بسبب تغييرات نظام التشغيل.

ب) التأكد من أن خطة الدعم السنوية والميزانية ستشمل الاستعراضات واختبـار النظـام الناجمة عن تغيرات نظام التشغيل.

ج) ضمان ان إخطار تغييرات نظام التشغيل تقدم في الوقت المناسب لإتاحة حدوث اختبارات مناسبة واستعراضات قبل التنفيذ.

د) ضمان أن تتم التغييرات المناسبة لخطط استمرارية العمل.

مسؤولية رصد نقاط الضعف وإطلاقات البائعين للبقع والثوابت يجب أن تعطى لمجموعة معينـة أو فرد.

3.5.12 تقييد التغييرات الى حزم البرمجيات

التحكم

ينبغي عدم تشجيع التعديلات الى حزم برمجيات، وقصرها على التغييرات الضرورية،ايضا جميع التغييرات يجب أن تتم مراقبتها بصرامة.

توجيهات التطبيق

إلى أقصى حد ممكن، وعمليا، مجموعات البرمجيات المزودة من البائع يجـب أن تـستخدم بـدون تعديل. عندما تتم الحوجة الى تعديل حزمة برمجيات يجب اخـذ النقـاط التاليـة فـي الاعتبـار:

أ) مخاطر الدمج في عمليات الرقابة والنزاهة المشبوهة.

ب) ما اذا كان ينبغي الحصول علي موافقة البائع.

ج) إمكانية الحصول على التغييرات المطلوبة من البائع وفقا لمعايير تحديثات البرنامج.

د) التأثير إذا أصبحت المنظمة مسؤولة عن الصيانة المستقبلية للبرمجيات كنتيجة للتغييرات

إذا كانت هنالك ضرورة للتغييرات فانه يجب الإبقاء على البرمجيات الأصلية وتطبيـق التغييـرات على نسخة واضحة ومحددة. يجب تنفيذ عمليـة إدارة تحـديث البرمجيـات لـضمان ان معظـم البقع الموافق عليها وتحديثات التطبيـق المواكبـة تـم تثبيتهـا لجميـع البرمجيـات المـصرحة. يجب اختبار كل التغييرات وتوثيقها، بحيث يمكن إعـادة تطبيقهـا مـن جديـد اذا لـزم الأمـر لتحديثات البرامج المستقبلية.إذا اقتضى الأمر يجب اختبار التعديلات والتأكد من صحتها مـن قبـل هيئة التقييم المستقلة.

4.5.12 تسرب المعلومات

التحكم

يجب منع فرص تسرب المعلومات.

توجيهات التطبيق

للحد من خطر تسرب المعلومات يجب النظر فيما يلي، (على سبيل المثال خلال استخدام واستغلال القنوات السرية):

أ) مسح المتجهين من وسائط الإعلام والاتصالات للمعلومات الخفية.

ب) الإخفاء ونظام التعديل وسلوك الاتصالات للحد من احتمالات وجـود طـرف ثالـث لديه القدرة على استخلاص المعلومات من مثل هذا السلوك.

ج) الاستفادة من النظم والبرامج التي تعتبر ذا نزاهة عالية، على سبيل المثـال اسـتخدام المنتجات المقيمة.

د) المراقبة المنتظمة للموظفين وأنشطـة النظـام والتي يسمح بها تحت التشريعـات أو اللوائح الموجودة.

هـ) مراقبة استخدام الموارد في النظم الحاسوبية.

معلومات أخرى

القنوات السرية هي المسارات التـي لا يقـصد منهـا سـلوك تـدفق المعلومـات، ولكـن التـي ومع ذلك قد توجد في النظام أو الشبكة. على سبيل المثال، في حزم بروتوكول الاتصالات التلاعب بالبتات يمكن استخدامه كطريقة خفية للإشارة. بحكم طبيعتها، سيكون من الصعب منع وجود جميع القنوات السرية المحتملة ، هذا إن لم يكن مستحيلا. ومع ذلك ، فإن استغلال هذه
القنوات غالبا ما تقوم بها شفرة طروادة. اتخاذ تدابير للحماية من شفرة طروادة وبذلك يقلـل مـن خطر استغلال قناة سرية.

منع الدخول غير المرخص به لشبكة، كذلك السياسات والإجراءات لتني إساءة اسـتخدام خـدمات المعلومات من قبل الأفراد، سوف يساعد على الحماية ضد القنوات السرية.

5.5.12 جهة خارجية لتطوير البرمجيات

التحكم

الاستعانة بمصادر خارجية لتطوير البرمجيات يجب ان يخضع لإشراف ورقابة المنظمة.

توجيهات التطبيق

عند التعاقد مع جهات خارجية لتطوير البرمجيات، وينبغي اخذ النقاط التالية في عين الاعتبار:

أ) ترتيبات الترخيص، قانون الملكية، وحقوق الملكية الفكرية.

ب) شهادة للجودة ودقة العمل المقام به.

ج) وضع ترتيبات لحسابات الضمان في حال عدم قيام طرف ثالث ؛

د) حقوق الوصول لمراجعة جودة ودقة العمل الذي تم القيام به.

هـ) الشروط التعاقدية للأمن لنوعية الأداء الوظيفي للشفرة.

و) الاختبار قبل التركيب للكشف عن الشفرات الخبيثة ،وشفرة وطروادة.

6.12 إدارة الثغرات التقنية

الهدف: للحد من المخاطر الناجمة عن استغلال نقاط الضعف التقنية المنشورة.

معايير

إدارة ضعف التقنية يجب تنفيذها على نحو فعال ومنتظم، وبطريقة قابلة للتكرار مع اخذ قياسات للتأكد من الفعاليه هذه الاعتبارات يجب ان تشمل أنظمة التشغيل، وغيرها من التطبيقات المستخدمة.

1.6.12 مراقبة نقاط الضعف التقني

التحكم

يجب الحصول المعلومات عن مواطن الضعف لأنظمة المعلومات المستخدمة في الوقـت المناسـب تعرض المنظمة لتقييم نقاط الضعف هذه كما يتم اتخاذ التدابير الملائمة لمعالجة المخاطر المرتبطـة بها.

توجيهات التطبيق

جرد حالي وكامل للأصول هو شرط أساسي لفعالية إدارة الضعف التقني. هنالك معلومات محـددة لازمة لدعم إدارة الضعف التقني وتشمل بائع البرمجيات ، أرقام الإصدار، الحالة الراهنـة للنـشر (مثل ما البرمجيات التي تم تثبيتها وعلى اي أنظمة)، والأشخاص داخل المنظمة المـسئولين عـن البرمجيات.

يجب اتخاذ الإجراء المناسب في الوقت المناسـب للـرد علـى تحديـد نقـاط الـضعف التقنيـة. فيما يلي إرشـادات يجـب اتباعهـا لوضـع نظـام فعـال لإدارة مـواطن الـضعف التقنـي:

أ) يجب على المنظمة أن تحدد الأدوار والمسؤوليات المرتبطة بإدارة الضعف التقنيـة، بمـا فـي ذلك مراقبة الضعف ، تقييم مخاطر الضعف، تتبع الأصول، وأي مسؤوليات تنسيق مطلوبة.

ب) مصادر المعلومات التي ستستخدم لتحديد مواطن الضعف التقنية ذات الصلة وللحفاظ على الوعي بها يجب أن تحدد للبرمجيات والتكنولوجياالاخرى. يجب تحديث هذه المعلومات استنادا على التغيرات في المخزونات أو عند ايجاد موارد اخرى جديدة أو مفيدة.

ج) يجب تحديد جدول زمني للرد على إخطارات الضعف التقنية ذات صلة.

د) فور تحديد ضعف الإمكانات التقنية ينبغي للمنظمة تحديد المخاطر المرتبطة بها والإجـراءات التـي يتعـين اتخاذهـا. مثـل هـذا الإجـراء يمكـن أن ينطـوي ترميم النظم الضعيفة و/أو تطبيق ضوابط أخرى.

هـ) اعتمادا على ضرورة الاحتياج لمعالجة الضعف التقني ، يجب اتخاذ الاجراء وفقا للضوابط المتعلقة بإدارة التغيير أو عن طريق اتباع إجراءات الاستجابة لحوادث أمن المعلومات.

و) إذا كان التصحيح متاح ، يجب تقييم المخاطر المرتبطة بتركيب القطعة (المخاطر الناجمة عن الضعف يجب مقارنتها مع خطر تثبيت القطعة).

ز) يجب اختبار القطع وتقييمها قبل أن يتم تركيبها للتأكد من أنها فعالة وانها لا تؤدي إلى آثار جانبية لا يمكن التغاضي عنها ؛ في حالة عدم توفر القطعة، يجب النظر في ضوابط أخرى، مثل:

1) إيقاف تشغيل الخدمات أو القدرات المتعلقة بالضعف.

2) تكييف أو إضافة ضوابط وصول ، على سبيل المثال الجدران النارية في حدود الشبكة.

3) زيادة المراقبة لكشف ومنع الهجمات الفعلية.

4) زيادة الوعي حول الضعف.

ح) يجب حفظ سجل مراجعة بكل الإجراءات الماخوذة.

ط) يجب مراقبة عملية إدارة الضعف التقني بانتظام وتقييمها لضمان فعاليتها وكفاءتها.

ي) يجب معالجة النظم عالية المخاطر أولا.

<u>معلومات أخرى</u>

ان الأداء الصحيح لعملية إدارة الضعف التقني حرج للعديد من المنظمات، لذا ينبغي مراقبتها بانتظام. الجرد الدقيق أمر ضروري لضمان تحديد مواطن الضعف التقني .

إدارة الضعف التقنية يمكن النظر إليها على أنها دون وظيفة لإدارة التغيير هذا ويمكن الاستفادة من عمليات وإجراءات إدارة التغيير.

الباعة غالبا ما يكونوا تحت ضغط كبير للافراج عن القعة في أقرب وقت ممكن. ولذلك القطعة قـد لا تعالج المشكلة على نحو كاف وربما يكون لها آثار جانبية سلبية. أيضا، في بعض الحالات، إلغاء تثبيت قطعة قد لا يكون من السهل تحقيقه بمجرد تطبيق القطعة.

إذا لم يكن هنالك اختبارات قطع كافية، على سبيل المثال نظرا للتكاليف أو نقـص المـوارد، فـان التأخر في الترميم يمكن اخذه في عين الاعتبار لتقييم المخاطر المرتبطة بها، استنادا إلى تجارب تم تسجيلها بواسطة المستخدمين.

13 إدارة حوادث أمن المعلومات

13.1 الإبلاغ عن نقاط الضعف، والأحداث الأمنية

الهدف: ضمان أمن المعلومات والتبليغ عن مواطن الضعف الموجودة في انظمة المعلومات ويـتم التبليغ في الوقت المناسـب بطريقـة تـسمح باتخـاذ إجـراءات تـصحيحية باقـصي سـرعة. في حالة تقديم بلاغ رسمي وتصعيد الإجراءات ينبغي أن تكون جميع الاجـراءات فـي متاحـة . ينبغي توجيه جميع الموظفين والمتعاقدين و المستخدمين و الفنيين بإجراءات البلاغ عـن الأنـواع المختلفة من الأحداث الحادثة ومعرفة نقاط الضعف التي قد يكون لها تأثير على أمن النظم.ولذلك تكون هنالك حوجة ماسة لأن يتم التبليغ جميع نقاط الضعف والاحداث الأمنية ليتم التعامـل معهـا ومراجعتها, في أسرع وقت ممكن .

1.1.13 التبليغ عن أحداث أمن المعلومات

<u>التحكم</u>

ينبغي تقديم البلاغات عن الاحداث الامنية الحاصلة في النظام عبر القنوات الرسمية في أقرب وقت ممكن.

<u>توجيهات التطبيق</u>

ينبغي أن تتخذ إجراءات رسمية لتأمين المعلومات والإبلاغ عن أى حالـة، مـع ومتابعـة اتخـاذ الأجراء اللازم ، الذي يحدد الإجراءات الواجب اتخاذها بشأن ورود تقرير من أمـن المعلومـات. وثمة نقطة اتصال ينبغي أن تنشأ للإبلاغ أمن المعلومات والأحداث. وينبغي التأكد مـن أن نقطـة الاتصال هذه معروفة في جميع أنحاء النظام و متاحة دائما، وأصبحت قادرة على توفير ما يكفـي من والاستجابة في اقرب وقت باسرع استجابة.

جميع الموظفين والمتعاقدين والمستخدمين طرف ثالث ينبغي توعيتهم بمسؤوليتها التبليغ عـن أي حدث حصل لأمن المعلومات في أسرع وقت ممكن. كما ينبغي لها أن تكـون علـى بينـة مـن الإجراءات الأمنية اللازم اتباعها، ونقطة الاتصال.

وينبغي أن تشمل إجراءات الإبلاغ ما يلي:

أ) عمليات تغذية مرتـدة مناسـبة لـضمان إبـلاغ عـن أحـداث أمـن المعلومـات قـد أخطرت بالنتائج بعد التعامل مع المسألة وغلقها.

ب) نماذج تقارير التبليغ عن الأحداث يدعم التبليغ عن الأحداث ويساعد المبلغ في تذكر جميع الاحداث عند وقوع حدث يؤثر علي امن المعلومات أمن المعلومات .

ج) السلوك الصحيح الواجب اتخاذها في حالة وقوع حدث يؤثر علي أمن المعلومات يتمثل في الاتي:

1) مع ملاحظة جميع التفاصيل المهمة علي الفور (مثل الأختراق، حدوث عطل ، ظهور رسائل على الشاشة ، والسلوك الغريب) .

2) عدم القيام بأي شئ وإبلاغ نقطة الاتصال علي الفور؛

د) الشروع في محاسبة ومعاقبة رسمية للموظفين، المقاولين أو لطرف ثالـث للمـستخدمين الذين يرتكبون مخالفات أمنية.

في بيئات شديدة الخطورة، والإكراه alarm4 يمكن أن تقدم فيها الشخص تحت الإكراه يمكن وتشير مثل هذه المشاكل. إجراءات الاستجابة للإنذارات الإكراه وينبغي أن تعكس مخاطر عالية هذه الحالة تشير إلى الإنذارات.

<u>معلومات أخرى</u>

أمثلة على أمن المعلومات والأحداث والوقائع هي:

أ) فقدان الخدمات والمعدات والمرافق.

ب) أعطال النظام

ج) الأخطاء البشرية.

د) عدم الامتثال للسياسات أو المبادئ التوجيهية.

هـ) الانتهاكات المادية للترتيبات الأمنية، وتغيير نظام السيطرة.

ز) أعطال الأجهزة أوأعطال البرمجيات.

ح) انتهاكات الخصوصية.

بذل الجهد اللازم لتتوفير الخصوصية والسرية ، وحوادث أمن المعلومات يمكن أن تـستخدم فـي التدريب لتوعية المستخدمين بالأخطار الممكن وقوعها حيث انها تكون أمثلة حية على ما يمكن أن يحدث، وكيفية الرد على مثل هذه الحوادث ، وكيفية تفاديها في المستقبل.

أن تكون قادرة على التعرف علي الأحداث والحوادث على الوجه الصحيح لتمكن من جمع الأدلة في أقرب وقت ممكن بعد وقوع .

أعطال النظام أو غيره من التصرفات الشاذة التي قد تكون مؤشرا لهجوم أمني أو فعلي او اختـراق أمني، ولذلك ينبغي أن تكون دائما وأفادت و معلومات أمنية صحيحة.

2.1.13 الإبلاغ عن الضعف في الأنظمة الأمنية

التحكم

جميع الموظفين والمقاولين والطرف الثالث من مستخدمي نظم المعلومات والخدمات ينبغي أن يـتم الإبلاغ عن أي ملاحظة أو اشتباه في نقاط الضعف في الأنظمة الأمنية والخدمات.

توجيهات التطبيق

جميع الموظفين والمتعاقدين والمستخدمين لطرف ثالث يجب ان يتم الإبلاغ إما للإدارة أو مباشـرة إلى مزود الخدمة في أسرع وقت ممكن من أجل منع وحماية المعلومات المخاطر الأمنيـة. آليـة تقديم البلاغ ينبغي أن تكون سهلة وان يتم الوصول إليها بأسرع ما يمكن . ينبغي أن يـتم التنبيـه على أنه لا يمكن إثبات حالات الضعف في الأنظمة .

معلومات أخرى

الموظفين والمتعاقدين والمستخدمين طرف ثالث ينبغي نصحهم بعدم المحاولة لإثبات ما يشتبه فـي النظام بأنه يمكن اختراقه . اختبار نقاط الضعف يمكن أن تفسر على أنها إساءة اسـتخدام محتمـل للنظام وكما يمكن أن تسبب ضررا على نظام معلومات أو الخدمة، ويؤدي ذلـك إلـى المـسؤولية القانونية للأفراد الذين يؤدون الاختبار.

2.13 إدارة وتأمين حوادث المعلومات والتحسينات

الهدف ضـمان وجـود نهـج متـسق وفعـال لتطبيـق إدارة المعلومـات للحـوادث الأمنيـة. المسؤوليات والإجراءات التي يجب أن تكون قائمة عند التعامل مع الأحداث، وتأمين المعلومات من نقاط الضعف عندما يكون قد تم التبليغ عنها. عملية التحسين المستمر ينبغي أن تكون ينطبق علـى الاستجابة لرصد وتقييم، والإدارة العامة لأمن المعلومات الحوادث. يطلب فيها تقديم الـدليل علـى ذلك، ينبغي جمعها لضمان الامتثال للمتطلبات القانونية.

1.2.13 المسؤوليات والإجراءات

التحكم

المسؤوليات الإدارية و الاجراءات ينبغي تفعل لضمان سرعة وفعالية الرد عند وقوع حدث يـضر بامن النظام .

توجيهات التطبيق

بالإضافة إلى الإبلاغ عن الاختراقات ونقاط الضعف ،يجب استخدام وسائل اخري مثل الرصد من نظم إنذار، ومواطن الضعف وينبغي أن تستخدم للكشف عن المعلومات وقوع اختراقات و حـوادث أمنية.

المبادئ التوجيهية التالية لأمن المعلومات وإدارة الحوادث ينبغي أن تهتم ب :

أ) ينبغي وضع إجراءات للتعامل مع أنواع مختلفة من المعلومات عن الحوادث الأمنيـة، بما في ذلك :

1) اصابة النظام بعطب وفقدان الخدمات
2) الشيفرات الخبيثة ؛
3) فقدان الخدمة.
4) من الأخطاء الناتجة عن البيانات الغير صحيحة أو الناقصة
5) انتهاك السرية والخصوصية

6) إساءة استخدام نظم المعلومات.

ب) بالإضافة إلي خطط الطوارئ ، والإجراءات التي ينبغي أن يشمل أيضا :

1) تحليل وتحديد سبب وقوع الحادث.

2) المحتويات

3) تخطيط وتنفيذ إجراءات تصحيحية لمنع تكرارها ، إذا لزم الأمر.

4) الاتصال مع المتضررين أو المشاركة في الشفاء من الحادث.

5) تقديم تقارير عن العمل إلى السلطة المختصة.

ج) مراجعة الحسابات والأدلة المماثلة التي ينبغي أن تجمع والمضمون ، كما الاقتضاء ، من أجل :

1) تحليل المشاكل الداخلية.

2) استخدامه كدليل طب شرعي في ما يتعلق بالإخلال المحتمل للعقد او المتطلبات التنظيمية أو في حالة الدعاوى المدنية أو الجنائية ، على سبيل المثال في سوء استخدام الكمبيوتر أو تشريعات حماية البيانات.

3) للتفاوض للحصول على تعويض من البرمجيات وموردي الخدمات.

د) يجب العمل على التعافي من الخروقات الأمنية وتصحيح فشل النظام بعناية والسيطرة عليه رسميا؛ يجب أن تكفل الإجراءات الاتي:

1) فقط الشخص المصرح له والمحدد بوضوح يسمح له الوصول إلى نظم العيش والبيانات.

2) توثيق جميع إجراءات الطوارئ التي اتخذت بالتفصيل.

3) يتم عمل تقرير عن حالات الطوارئ للإدارة وعرضها بنحو منظم.

4) سلامة نظم العمل والضوابط تؤكد بأقل قدر من التأخير.

يجـ ـب الاتفـ ـاق مـ ـع الإدارة علـ ـى أهـ ـداف إدارة أمـ ـن المعلومـ ـات، و ايـ ـضا يجـ ـب التأكـ ـد مـ ـن أن المـ ـسئولين عـ ـن هـ ـذه الإدارة يفهمـ ـون أولويات المنظمة للتعامل مع المعلومات الأمنية.

معلومات أخرى

حوادث امن المعلومات قد تتجاوز الحدود التنظيمية والوطنية. للرد على مثل هذه الحـوادث هنـاك حاجة متزايدة لتنسيق الاستجابة وتبادل المعلومات حول هذه الحوادث مع المنظمات الخارجية حسب الاقتضاء.

2.2.13 التعلم من الحوادث الأمنية للمعلومات

التحكم

ينبغي أن تكون هنـاك آليـات لتفعيـل أنـواع وأحجـام وتكـاليف حـوادث أمـن المعلومـات لتعرف كميا ويتم رصدها.

توجيهات التطبيق

المعلومات التي يكتسبونها من خلال تقييم حوادث المعلومات الامنية يجب استخدامها لتحديد تـأثير ارتفاع أو تكرار هذه الحوادث.

معلومات أخرى

تقييم حوادث المعلومات الأمنية قد يشير إلى الحاجة إلى تعزيز ضوابط أو إضافتها للحد من وتيرة ، ضرر ، وتكلفة الحوادث في المستقبل ، أو أن تؤخذ في الاعتبار في عملية استعراض السياسة الأمنية.

3.2.13 جمع الأدلة

التحكم

حيثما تتم متابعة إجراء ضد شـخص أو منظمـة، بعـد شـمول حـوادث المعلومـات الأمنيـة إجراءات قانونية (سواء كانت مدنية أو جنائية)، فانه يجب جمع الأدلة، والاحتفاظ بهـا، وعرضـها لكى تتفق مع قواعد الأدلة المبينة في الولاية القضائية ذات الصلة.

توجيهات التطبيق

يجب تطوير وإتباع الإجراءات الداخلية عند جمع وتقديم الأدلة لأغراض إجـراءات تأديبيـة يـتم التعامل بها داخل المنظمة.

بصفة عامة، تشمل قواعد الأدلة الاتي:

أ) قبول الأدلة: سواء كان من الممكن استخدامها او عدم استخدامها في المحكمة.

ب) وزن الأدلة: نوعية واكتمال الأدلة.

لتحقيق قبول الأدلة، يجب على المنظمة أن تتاكد بان نظم معلوماتها يمتثل لأي معيـار أو مدونـة منشورين لإنتاج أدلة مقبولة. وزن الأدلة المقدمة يجب أن تمتثل لأي شروط قابلة تطبيقية. لتحقيـق وزن الأدلة، نوعية واكتمال الضوابط التي تستخدم لحماية الدليل على الوجه الصحيح على الدوام ، (مثال دليل مراقبة العملية) طوال الفترة التي يتم فيها استرداد الأدلة تخزينها ومعالجتها يجب أن يتم الدلالة عليها بدرب أدلة قوية. عموما، مثل هذا الدرب القوي يمكن أن ينشأ وفقا للشروط التالية:

أ) للوثائق الورقية: يتم الاحتفاظ بالأصلي بآمان مع سجل الفرد الذي عثر على هذه الوثيقة، كذلك مكان العثور على الوثيقة، وزمنها والذي شهد على الاكتشاف .أي تحقيقـات يجب أن تكفل بانه لم يتم العبث بالوثائق الأصلية.

ب) للمعلومات على وسائط الحاسوب: صور مرآة، أو نسخ (وفقا للاحتياجات التطبيقة)لأي وسائط قابلة للإزالة، يجب اخذ المعلومات عن الأقراص الثابتة أو الـتي في الذاكـرة لضمان التوافر؛ يجب حفظ سجل جميع إجراءات عملية النسـخ كما يجـب أن تشهـد العملية؛ يجب حفظ الوسائط الأصلية والسجل (اذا لم يكن ذلك ممكنا ، نسخة واحـدة أو صورة طبق الأصل على الأقل) بآمان وان لا تمس عمل الطب الشرعي.

يجب أن يكون بشكل نسخ من مواد الإثبات. يجب حماية سلامة جميع مواد الأدلـة. كمـا يجـب الاشرف على نسخ مواد الأدلة بواسطة شخص جدير بالثقة وتسجيل المعلومات عن متى واين نفذت عملية النسخ، من قام بأنشطة النسخ والبرامج والأدوات التي استخدمت.

<u>معلومات أخرى</u>

عندما يتم رصد حدث أمن معلومات لأول مرة، قد لا يكون واضحا ما اذا كان سينتج عن الحـدث اجراء محكمة او لا. ولذلك، فإن هناك خطر يتمثل في تدمير الأدلة الضرورية عن قـصد أو عـن غير قصد من قبل ان تتحقق خطورة الحادث. ومن المستصوب إشراك محام أو الشرطة في وقـت مبكر في أي إجراء خطوة قانونية واخذ المشورة بشأن الأدلة المطلوبة.

الأدلة قد تتجاوز الحدود التنظيمية و/أو القضائية. في مثل هذه الحالات، يجب التأكد من ان المنطمة لها الحق لجمع المعلومات المطلوبة كأدلة. كما يجب النظر في احتياجات مختلـف الاختـصاصات لتكبير فرص القبول عبر المحاكم المختصة إلى أقصى حد ممكن .

14 إدارة استمرارية الأعمال

1.14 إدارة نواحي أمن المعلومات واستمرارية الأعمال

الهدف: مكافحة إعاقة أنشطة الأعمال وحماية عمليات الأعمال الحرجة من مؤثرات الأعطال الرئيسية أو الكوارث على نظم المعلومات، وضمان توكيد استئناف تشغيلها بالتوقيت المضبوط المناسب.

ينبغي تنفيذ عملية إدارة استمرارية الأعمال ليتسنى تقليل التأثير السالب على المنظمة، واسترداد عافيتها باسترجاع أصول المعلومات المفقودة (إذ أن التأثير يمكن أن تكون نتيجة للكوارث الطبيعية، والحوادث، وتعطل المعدات، والأفعال التخريبية المعتمدة على سبيل المثال) ببلوغ المستوى المرغوب عبر تطبيق توليفة الضوابط الوقائية والانتعاشية. إن هذا النسق يجب أن يحدد عمليات الأعمال الحرجة، وعليه أن يُكامل ما بين متطلبات إدارة استمرارية أمن المعلومات لمواصلة الأعمال مع الاحتياجات الأخرى لاستمرارية الأعمال ذات الصلة بجوانب العمليات، والتوظيف، والموارد، والنقل والوسائل التسهيلية.

يجب إخضاع الآثار المترتبة عن الكوارث، والقصور الأمني، وفقدان الخدمات، وتيسر الخدمات لتحليل تأثير الأعمال. ينبغي تطوير وتنفيذ خطط استمرارية الأعمال لتوكيد ضمان استئناف العمليات الضرورية في الوقت المناسب. يتحتم الأمر بأن يكون أمن المعلومات جزءاً متمماً لعملية استمرارية الأعمال عموماً والعمليات الإدارية الأخرى داخل إطار المنظمة.

ينبغي أن تشمل مهام إدارة استمرارية الأعمال على ضوابط لتحديد وتقليل المخاطر بالإضافة إلى عملية تقييم المخاطر عموماً، والحد من الآثار المترتبة عن الحوادث المدمرة، وضمان توفر المعلومات المطلوبة لإنجاز عمليات الأعمال بسهولة.

1.1.14 تضمين أمن المعلومات في عملية إدارة استمرارية الأعمال

التحكم

يجب تطوير نسق متحكماً فيه للحفاظ على تتابع الأعمال في جميع أنحاء المنظمة، إذ أن النسق الإجرائي المتحكم فيه سيتناول متطلبات أمن المعلومات المطلوبة لدى المنظمة لضمان استمرارية الأعمال.

توجيهات التطبيق

ينبغي أن تجمع العملية النسقية المعنية ما بين العناصر الرئيسية لإدارة استمرارية الأعمال التالية:

أ) إدراك المخاطر التي تواجهها المنظمة فيما يختص باحتمالية حدوثها وتأثيرها الزمني عاجلاً أو آجلاً بخاصة في مضمار تحديد وترتيب الأولوية الزمنية لعمليات الأعمال الحرجة (انظر 14-1-2):

ب) تحديد كل الأصول المستخدمة في عمليات الأعمال الحرجة (انظر 17-2)؛

ج) الإلمام بتأثير الأعطال المحتملة التي تسبب حوادث أمن المعلومات على الأعمال (ومن المهم إتمام إيجاد الحلول التي تتناول الحوادث التي تسبب في إحداث تأثير زهيد، وكذلك الحوادث الخطيرة التي يمكن أن تهدد حيوية المنظمة)، وتأسيس أهداف أعمال مرافق معالجة المعلومات؛

د) الأخذ بعين الاعتبار بشراء قسط التأمين المناسب الذي يمكن أن يكون جزءاً من عملية استمرارية الأعمال عموماً، فضلاً أنه سيكون جزءاً من إدارة عمليات المخاطر (الإدارة ذات الصلة بعمليات المخاطر)؛

هـ) تحديد وتنفيذ ضوابط وقائية وتخفيفية إضافية؛

و) تحديد موارد مالية، وتنظيمية، و فنية، وبيئية كافية للتعامل مع الاحتياجات المحددة لأمن المعلومات؛

ز) ضمان سلامة الموظفين وحماية مرافق معالجة المعلومات والممتلكات التابعة للمنظمة؛

ح) صياغة وتوثيق خطط تواصل الأعمال التي تتناول احتياجات أمن المعلومات المتسقة مع إستراتيجية استمرارية الأعمال المتفقة عليها (انظر 14-1-3)؛

ط) إجراء الفحوص الدورية المنتظمة وتحديث الخطط والإجراءات الموضوعة في الموضع الصحيح والوقت الملائم (انظر 14-1-5)؛

ي) توكيد الضمان بأن إدارة استمرارية الأعمال مدمجة في عمليات وتركيبة المنظمة، وينبغي أن تكون مسؤولية عملية إدارة تواصل الأعمال مخصصة التكليف على مستوى ملائم في جميع أنحاء المنظمة (انظر 6-1-1).

2.1.14 تواصل الأعمال وتقييم المخاطر

التحكم

يجب تحديد الأحداث التي يمكن أن تسبب في انقطاع عمليات الأعمال بالاتساق مع احتمال حدوث مثل هذه الأعطال، وتأثيراتها وعواقبها المتمخضة على أمن المعلومات.

توجيهات التطبيق

ينبغي تأسيس نواحي أمن معلومات استمرارية الأعمال اعتماداً على الأحداث المشخّصة (أو الأحداث المتعاقبة) التي يمكن أن تسبب في إعاقة عمليات أعمال المنظمات مثلاً: تعطل المعدات، والأخطاء البشرية، والسرقة، واندلاع الحرائق، والكوارث الطبيعية، والأعمال الإرهابية. وهذه الخطوة يجب إتباعها بعملية تقييم المخاطر لتحديد احتمالية وتأثير مثل هذه الأعطال فيما يخص الزمن، وحجم الأضرار الناتجة عن الأعطال وفترة استعادة عافية المنظمة.

يجب تنفيذ توليفات تقييم مخاطر سيرورة الأعمال بالمشاركة الكاملة من قبل ممتلكي موارد الأعمال والعمليات. وأن يُراعى هذا التقييم كل عمليات الأعمال وينبغي ألاّ يكون مقتصراً على مرافق معالجة المعلومات، ولكن يجب أن يشمل النتائج المختصة تحديداً بأمن المعلومات. ومن المهم الربط ما بين جوانب المخاطر المختلفة على نحو متصل ليتسنى الحصول على صورة كاملة لمتطلبات استمرارية أعمال المنظمة. ينبغي أن يعرف التقييم المعنى ويحدد ويرتب أولويات المخاطر بالمقارنة مع المعايير والأهداف المناسبة للمنظمة وعلى أن يتضمن التقييم تحديد الموارد الحرجة وتأثيرات الانقطاع، والأزمنة الممسوحة بها للانقطاع، وترتيب أولويات استعادة التعافي اعتماداً على نتائج تقييم المخاطر، فأنه يجب تطوير إستراتيجية استمرارية الأعمال حتى يمكن تحديد النهج العام لتواصل الأعمال. وعند صياغة هذه الإستراتيجية فإن الإدارة ينبغي أن توافق عليها، وبمقتضى أن الخطة قد وُضعت، وتمت المصادقة عليها لتنفيذ هذه الإستراتيجية.

3.1.14 وضع وتنفيذ خطط الاستمرارية المتضمنة على أمن المعلومات

التحكم

ينبغي وضع وتنفيذ الخطط للحفاظ أو استعادة ممارسة العمليات، لضمان توفير المعلومات على المستوى المرغوب في الوقت المطلوب على الحجم المناسب الذي يلي انقطاع العمليات أو توقف عمليات الأعمال الحرجة.

توجيهات التطبيق

تحتم عملية تخطيط تواصل الأعمال مراعاة النقاط التالية:

أ) تحديد وإقرار جميع مسئوليات وإجراءات استمرارية الأعمال؛

ب) تحديد الخسارة المعقولة التي يمكن تحملها في مجال المعلومات والخدمات؛

ج) تنفيذ الإجراءات التي تتيح استرداد حيوية المنظمة، وتجديد تواصل عمليات الأعمال وتيسير المعلومات على حسب المعلومات الزمنية المطلوبة، ويجب وضع اعتبار خاص لتقييم الملحقات التابعة للأعمال الداخلية والخارجية والعقودات الملائمة في الموضع الصحيح؛

د) الإجراءات العملية لتنفيذ متابعة إنجاز استرداد الحيوية وإكمال تجديدها؛

هـ) توثيق الإجراءات وتدابير العمليات المتفقة عليها؛

و) توفير التعليم المناسب للموظفين في مجالات الإجراءات والعمليات المتفقة عليها، وعلى أن يشمل هذا التعليم إدارة الأزمات؛

ز) إجراء اختبار فعالية الخطط وتحديثها.

ينبغي أن تضع طريقة التخطيط نصب أعينها على أهداف الأعمال المطلوبة على سبيل المثال: استعادة تجديد تواصل خدمات الاتصالات المحددة للزبائن في غضون فترة معقولة من الزمن.

يجب تعريف الخدمات والموارد الميسرة لهذه العملية، على أن تتضمن التوظيف، و موارد معالجة المعلومات غير الجوهرية، بالإضافة إلى الترتيبات الاحتياطية لمرافق معالجة المعلومات. إن مثل هذه الترتيبات الاحتياطية يجب أن تشمل الترتيبات مع أطراف ثالثة في شكل اتفاقات تبادلية بالمثل أو خدمات تجارية بالاشتراك.

ينبغي أن تعالج خطط استمرارية الأعمال في المناحي التنظيمية مدى قابلية، المنظمة للهجوم واقتحام خصوصياتها، وبناء عليه يمكن اشتمال تلك الخطط على المعلومات الحساسة التي تتطلب الحماية بالضبط. يجب تخزين صور من خطط سيرورة الأعمال في مكان نائي على مسافة بعيدة معقولة حتى يتسنى تفادي إلحاق أية أضرار بها من جراء حدوث كارثة في الموقع الرئيسي. ويتحتم الأمر بأن تتكفل الإدارة ضمان أن نسخ خطط استمرارية الأعمال قد تم تحديثها وحمايتها بنفس القدر من

الحماية المتاحة للنسخ الموجودة في الموقع الرئيسي. و أما المواد الضرورية الأخرى التي تكفل استمرارية سلامة الخطط يجب تخزينها في موقع بعيد.

وإذا ما تم استخدام مواقع بديلة مؤقتة للتخزين فأن مستوى ضوابط السلامة المنفذة في هذه الموقع ينبغي أن تكون معادلة لضوابط الأمن المتخذة في المقر الرئيسي.

معلومات أخرى

يجب الملاحظة بأن خطط إدارة الأزمات والأنشطة (انظر 14-1-3 ف) يمكن أن تكون مختلفة عن خطط إدارة استمرارية الأعمال مثلاً: يمكن أن تحدث أزمة بالإمكان احتوائها بتطبيق إجراءات الإدارة العادية.

4.1.14 الهيكل الإطاري لتخطيط تواصل الأعمال:

التحكم

ينبغي الحفاظ على نطاق نسقي واحد لخطط استمرارية الأعمال لتوكيد الضمان بأن جميع الخطط متسقة، ينبغي تناول مستلزمات أمن المعلومات بتناسق تام، ولتحديد ترتيب أولويات الاختيار وتطويرها في إطار المحافظة عليها.

توجيهات التطبيق

يجب أن تصف أي خطة لتواصل الأعمال نهج كيفية استمرارية الأعمال مثلاً: أن النهج ينبغي أن يضمن توفر المعلومات ومتاحية نظام المعلومات وأمنها. ينبغي أن يحدد كل خطة أيضاً مخططاً لترقية الخطة وشروط تنشيطها، فضلاً عن تحديد الأفراد المسئولين عن تنفيذ كل عناصر الخطة.

وعند تحديد متطلبات جديدة للخطة، فإن إجراءات حالات الطوارئ على سبيل المثال: خطط الإخلاء، أو الترتيبات الاحتياطية ينبغي تعديلها حسب اقتضاء الضرورة. يجب أن تتضمن الإجراءات المعنية على برامج إدارة التغيير في أنحاء المنظمة لتوكيد الضمان بأن مسائل استمرارية الأعمال قد تم تداولها بشكل ملائم. ينبغي أن تخصص كل واحد من الخطط لمسئول مالك محدد لتكون تحت رعايته تحديداً. ويجب أن تكون إجراءات الطوارئ والخطط الاحتياطية الموجزة وخطط الاستئناف تحت مسئولية مالكين لموارد أعمال مناسبة أو العمليات التي تنطوي عليها.

إن الترتيبات الاحتياطية للخدمات الفنية البديلة مثل معالجة المعلومات ووسائل مرافق الاتصالات ينبغي أن تكون عادة تحت مسئولية الممولين بالخدمات.

إن إطار تخطيط استمرارية الأعمال يجب أن يتناول متطلبات أمن المعلومات المحددة وبمراعاة التالية:

أ) شروط تفعيل الخطط التي تصف العملية التي يجب إتباعها (كيفية تقييم الوضع، ومن الذي يُسمح له بالمشاركة) قبل تنشيط أي واحد من الخطط.

ب) إجراءات الطوارئ التي تصف الإجراءات التي ينبغي اتخاذها أعقاب أي حادثة تعرض عمليات الأعمال للخطر.

ج) الإجراءات الاحتياطية التي تصف الإجراءات التي ينبغي اتخاذها لتحريك أنشطة الأعمال الضرورية أو الخدمات الداعمة إلى مواقع بديلة مؤقتة، ولإعادة تجديد عمليات الأعمال لتعمل في إطار المقاييس الزمنية المطلوبة.

د) الإجراءات التشغيلية المؤقتة التي تلي الانجاز غير المبتوت فيه لانتعاش المنظمة واستئناف حيويتها.

هـ) استئناف الخطوات التي تصف الإجراءات التي يجب اتخاذها لمواصلة عمليات الأعمال العادية.

و) البرنامج الدوري الزمني للصيانة الذي يحدد كيفية ومتى يتم اختبار الخطة، وعملية الحفاظ عليها.

ز) أنشطة خلق الوعي والتعليم والتدريب المصممة لبعث الإدراك بعمليات استمرارية الأعمال، وتوكيد ضمان استمرارية الأعمال على نحو فعال.

ح) تحديد المسئوليات التي يضطلع بها الأفراد، ووصف من المسئول عن تنفيذ عنصر معين من مكونات الخطة الموضوعة، وتعيين البدائل حسب اقتضاء الحاجة.

ط) الأصول الحرجة والمواد المطلوبة لتمكين أداء تنفيذ إجراءات الطوارئ والأساليب الاحتياطية وإجراءات
استئناف العمليات.

5.1.14 اختبار، وصيانة وإعادة تقييم خطط استمرارية الأعمال

التحكم

ينبغي فحص وتحديث خطط استمرارية الأعمال بانتظام لتوكيد الضمان بأنها محدثة وفعالة.

التوجيهات التطبيقية

يجب أن تثبت اختبارات خطط استمرارية الأعمال بأن جميع الأعضاء الضالعين في فريق إعادة انتعاش المنظمة، وغيرهم من الموظفين من ذوي الصلة بالأمر يدركون الخطط المعينة، وفهمهم مسئولياتهم تجاه استمرارية الأعمال وأمن المعلومات، ومعرفتهم لدورهم في تنفيذ الخطة ليتسنى تفادي التعريض للمخاطر.

ينبغي أن يشير جدول الاختبارات الدورية للخطة / أو الخطط لاستمرارية الأعمال إلى كيفية ومتى يتم فحص أي عنصر من عناصر الخطة الموضوعة. ويجب فحص أي عنصر من مكونات الخطة/ أو الخطط في فترات قصيرة.

ويحتم الأمر استخدام مجموعة متنوعة من التقنيات التي توفر الضمان بأن الخطة/ الخطط تعمل على نحو عملي فعلياً. وتشمل هذه التقنيات على الآتية:

أ) الاختبار المكشوف للمخططات المتنوعة/ "السيناريوهات" (بمناقشة ترتيبات تجديد انتعاش الأعمال باستخدام أمثلة من انقطاعات الأعمال)

ب) النمذجة/"المحاكاة" (بخاصة تدريب الناس في مجال أداء أدوارهم في إدارة آثار ما بعد وقوع الحادثة / إدارة الأزمات)

ج) الاختبار الفني لتجديد انتعاش المنظمة (أي ضمان أن نظم المعلومات قد استعادت عافيتها بفعالية)

د) اختبار مدى استعادة الانتعاش في موقع آخر بديل (مواصلة تشغيل عمليات الأعمال بالتوازي مع عمليات استعادة عافية المنظمة بعيداً عن المقر الرئيسي لها)

هـ) إجراء فحوصات لمرافق وخدمات الممولين (أي توكيد الضمان بأن الخدمات المقدمة خارجياً وكذلك المنتجات ستفي بالالتزامات التعاقدية)

و) تكرار التجارب الكاملة (أي بإجراء الفحص الذي يدل بـأن المنظمـة ومجموعـة الموظفين والمعدات والمرافق والعمليات الإجرائية يمكن أن تتعامل وتواكب الأعطال المتوقعة)

وهذه التقنيات يمكن استخدامها من قبل أي منظمة. وينبغي تطبيقها بأي طريقة مناسبة لخطة محددة لاستعادة الحيوية. وأن نتائج الاختبار يجب تسجيلها لاتخاذ الإجراءات التي تكفل تحسين الخطط عند اقتضاء الحاجة.

ينبغي تحديد المسئولية وإخضاع خطة استمرارية الأعمال للمراجعـة المنتظمـة. إن آليـة تحديـد التغييرات في ترتيبات الأعمال التي لم تنعكس بعد في خطط تواصل الأعمال يجب إتباعها بخطـة تحديث ملائمة. ينبغي أن تؤكد طريقة التحكم في التغييرات الرسمية بأن خطـط التحـديث سـيتم تصنيفها، وأنها سوف تُعزز بإنفاذ مراجعات استعراضية منتظمة للخطة الكاملة.

يجب مراعاة أمثلة التغييرات في مجال تحديث خطط استمرارية الأعمال لاكتساب معـدات جديـدة وترقية النظم والتغييرات في المجالات التالية:

أ) مجموعة الموظفين المستخدمين في المنظمة؛

ب) العناوين أو أرقام الهواتف؛

ج) إستراتيجية الأعمال؛

د) الموقع والمرافق والموارد؛

هـ) تشريع القوانين؛

و) المقاولين والممولين والزبائن الرئيسيين؛

ز) العمليات (الأساليب) الجديدة أو المنعزلة منها؛

ح) المخاطر (ذات العلاقة بالعمليات والمخاطر المالية).

15 الامتثال

الامتثال للمتطلبات القانونية

الهدف: تجنب أي خرق للقانون الأساسي والتنظيمية أو الالتزامات التعاقدية، على أي المتطلبات الأمنية. تصميم وتشغيل واستخدام وإدارة نظم المعلومات يمكن أن تخضع لوضعية التنظيمية والتعاقدية والمتطلبات الأمنية. المشورة بشأن متطلبات قانونية محددة ينبغي السعي من المستشارين القانونيين للمنظمة، أو الممارسين القانونيين المؤهلين تأهيلا مناسبا. المتطلبات التشريعية تختلف من بلد إلى آخر، ويجوز وتختلف المعلومات التي أنشئت في بلد واحد أن ينتقل إلى بلد آخر (أي عبر الحدود تدفق البيانات).

1.1.15 تعريف التشريعات المطبقة

التحكم

جميع الجهات ذات الصلة في النظام الأساسي، والتنظيمية، والشروط التعاقدية ونهج المنظمة عليها تلبية هذه الاحتياجات وينبغي أن تكون محددة بوضوح، ويجب توثيقها، و محافظة عليها محدثة كل ونظام معلومات المنظمة.

توجيهات التطبيق

الضوابط المحددة والمسؤوليات الفردية لتلبية هذه الاحتياجات ينبغي أن يكون كذلك تم تحديدها وتوثيقها.

2.1.15 حقوق الملكية الفكرية

التحكم

الإجراءات المناسبة ينبغي تنفيذها لضمان الامتثال مع متطلبات التشريعية والتنظيمية، والشروط التعاقدية على استخدام المواد في ما يتعلق التي قد تكون هناك ملكية الفكرية الإنسان، وعلى استخدام منتجات البرمجيات المسجلة الملكية.

توجيهات التطبيق

المبادئ التوجيهية التالية ينبغي النظر إلى حماية أي مادة يمكن أن تعتبر ملكية فكرية:

أ) نشر حقوق الملكية الفكرية والامتثال للسياسة القانونية التي تحدد استخدام المعلومات والبرمجيات والمنتجات؛

ب) إلا عن طريق الحصول على البرمجيات والسمعة المعروفة المصادر، لضمان حقوق التأليف والنشر لم تنتهك؛

ج) المحافظة على الوعي من السياسات لحماية حقوق الملكية الفكرية، وذلك بتقديم إشعار عن نية لاتخاذ إجراءات تأديبية ضد الموظفين مخالفين لها؛

د) الحفاظ على سجلات الأصول المناسبة، وتحديد جميع الاحتياجات للأصول حماية حقوق الملكية الفكرية؛

هـ) المحافظة على الدليل وامتلاك التراخيص، وأقراص الأساسية، ودليل التشغيل، وما إلى ذلك؛

و) تنفيذ ضوابط لضمان أن أكبر عدد ممكن من المستخدمين غير مسموح تجاوز؛

ز) تنفيذ عمليات التفتيش التي المأذون بها فقط البرمجيات والمنتجات المرخصة تركيبها؛

ح) توفير السياسات الملائمة للحفاظ على شروط الترخيص؛

ط) تقديم سياسة للتخلص أو نقل البرمجيات للآخرين؛

ي) باستخدام وسائل مراجعة مناسبة الحسابات؛

ك) والامتثال لأحكام وشروط البرمجيات والمعلومات التي حصلت عليها من الجمهور الشبكات؛

ل) عدم الازدواجية، والتحول إلى شكل أو آخر من انتـزاع التـسجيلات التجاريـة (فـيلم والسمعية) عدا ما يسمح به قانون حقوق التأليف والنشر؛

م) عدم النسخ كليا أو جزئيا (الكتب، المقالات، والتقارير، أو غيرها من الوثائق)، بخلاف ما يسمح به قانون حقوق التأليف والنشر.

معلومات أخرى

وتشمل حقوق الملكية الفكرية وحقوق المؤلف وثيقة مـن وثـائق البرنـامج أو حقـوق التـصميم والعلامات التجارية وبراءات الاختراع، وشفرة المصدر التراخيص.

منتجات البرمجيات المسجلة الملكية عادة الموردة بموجب اتفاقية الترخيص إن يحـدد التـرخيص شروط وأحكام، على سبيل المثال، الحد من استخدام هذه المنتجات على أجهزة معينة أو الحد منهـا نسخ إلى إنشاء نسخ احتياطية فقط. حقوق الملكية الفكرية في حالة البرامج التي تـضعها ويتطلـب التنظيم إلى توضيح مع الموظفين.

التشريعية والتنظيمية، والشروط التعاقدية قد تضع قيودا على نسخ من الملكية المادية. علـى وجـه الخصوص، قد تحتاج إلى أن المواد التي وضعتها تنظيم، أو مرخص أو المقدمة لتطوير المنظمـة، ويمكن استخدامها.

انتهاك حقوق النشر قد يؤدي إلى اتخاذ إجراءات قانونية، والتي قد تشمل الإجراءات الجنائية.

3.1.15 حماية السجلات التنظيمية

التحكم

سجلات هامة ينبغي حمايتها من الضياع، وتدمير وتزويـر، وذلـك وفقـا لإجـراءات القانونيـة والتنظيمية، والتعاقدية، ومتطلبات العمل.

توجيهات التطبيق

سجلات ينبغي تصنيفها إلى أنواع قياسية، على سبيل المثال سجلات المحاسـبة، وإنـشاء قواعـد البيانات وسجلات المعاملات الجذوع، ومراجعة السجلات، والإجراءات التنفيذية، مع كل التفاصـيل والاحتفاظ بها لفترات النوع من التخزين وسائل الإعلام، على سبيل المثـال ورقـة الميكـروفيش بصرية. أي ترميز المواد والقفل البرامج المرتبطة بـشفرة المحفوظـات أو التوقيعـات الرقميـة (12.3)، كما ينبغي لتخزين تمكين التشفير من السجلات لطول الفترة الزمنية التي يتم الاحتفاظ بها في السجلات.

ينبغي النظر في احتمال تدهور وسائل الإعلام وتستخدم لتخزين السجلات. إجراءات التخزين والمناولة وينبغي أن تنفذ وفقا لصانع التوصيات. للتخزين على المدى الطويل، واستخدام ورقة الميكروفيش وينبغي النظر فيها.

وسائط التخزين الإلكترونية حيث يتم اختيار، وإجراءات لضمان القدرة على الوصول إلى البيانـات (وسائل الإعلام على حد سواء وشكل قراءة) طوال فترة الاحتفاظ بها وينبغي أن تدرج ، لـضمان عدم ضياع بسبب تغير التكنولوجيا في المستقبل.
نظم تخزين البيانات وينبغي اختيار البيانات المطلوبة التي يمكن الاطلاع عليهـا بـصورة مقبولـة وشكل الجدول الزمني، وهذا يتوقف على الشروط التي يتعين الوفاء بها.

نظام التخزين والمناولة ينبغي أن تكفل تحديد واضح للسجلات والاحتفاظ بهم الفترة علـى النحـو المحدد في التشريعات الوطنية أو الإقليمية أو الأنظمة، إن وجدت. وينبغي لهذا النظام مناسبة تسمح تدمير السجلات بعد تلك الفترة، إن لم تكن تحتاج إليها المنظمة.

سجل لضمان تلبية هذه الأهداف، ينبغي اتخاذ الخطوات التالية في إطار المنظمة:

أ) ينبغي إصدار مبادئ توجيهية بشأن حفظ وتخزين والمناولة والـتخلص مـن الـسجلات والمعلومات؛

ب) الإبقاء على الجدول الزمني ينبغي وضع السجلات وتحديد الفترة الزمنيـة التـي ينبغـي الاحتفاظ بها؛

ج) إجراء حصر للمصادر المعلومات الرئيسية وينبغي الحفاظ ؛

د) ضوابط مناسبة ينبغي أن تنفذ لحماية السجلات والمعلومات من الضياع ، الشامل ، وتزييفها.

<u>معلومات أخرى</u>

بعض السجلات قد تكون هناك حاجة إلى الاحتفاظ بها بشكل آمـن لتلبيـة الاحتياجـات القانونيـة والتنظيمية أو التعاقدية، وكذلك لدعم الأنشطة الأساسية في الأنشطة التجارية. ومن الأمثلـة التـي يمكن أن تكون السجلات يطلب دليلا على أن المنظمة تعمل في إطار القواعد القانونية أو التنظيمية، وذلك لضمان ما يكفي للدفاع ضد احتمال اتخاذ إجراءات مدنية أو جنائية، أو للتأكد مـن الوضـع المالي فيما يتعلق بتنظيم حملة الأسهم ، والأطراف الخارجية ، ومراجعي الحسابات. الفترة الزمنية والبيانات الإبقاء على مضمون للحصول على معلومات قد تكون وضعتها قانون أو لائحة وطنيـة.

مزيد من المعلومات حول إدارة السجلات التنظيمية يمكن العثور عليها في المنظمة الدولية للتوحيـد القياسي 15489-1.

4.1.15 حماية البيانات والخصوصية والمعلومات الشخصية

التحكم

حماية البيانات والخصوصية، وينبغي ضمان لما هو منصوص عليه في التـشريعات ذات الـصلة، واللوائح، وإذا كان ينطبق ذلك، الشروط التعاقدية.

توجيهات التطبيق

وضع السياسات التنظيمية لحماية البيانات والخصوصية، وينبغي وتنفيذها. وينبغي تنفيذ هذه السياسة لجميع الأشخاص المشاركين في عملية معالجة المعلومات الشخصية.

امتثالا لهذه السياسة وجميع البيانات ذات الصلة بحماية التـشريعات والأنظمـة وتتطلـب الهيكـل التنظيمي المناسب والسيطرة عليه. كثيرا ما تكون هذه هي أفضل طريقة لتحقيق ذلك عـن طريـق تعيين شخص مسئول، مثل حماية البيانات، الذي كان ينبغي توجيه المديرين والمستخدمين، وعلـى مقـدمي الخـدمات الفرديـة والمـسؤوليات والإجـراءات المحـددة التـي ينبغـي ان يتبع. مسؤوليتها في معالجة المعلومات الشخصية وضمان الوعي البيانات مبادئ الحمايـة ينبغـي التعامل معها وفقا للتشريعات واللوائح ذات الصلة. التقنية المناسـبة والتـدابير التنظيميـة لحمايـة المعلومات الشخصية التي ينبغي أن تكون.

معلومات أخرى

هناك عدد من البلدان تضع تشريعات وضوابط على المجموعات ومعالجة ونقل البيانات الشخـصية (عادة معلومات عن الكائنات الحية من الأفراد الذين يمكن التعرف على مـن هـذه المعلومـات). اعتمادا على التشريعات الوطنية، وهذه الضوابط قد تفرض واجبات على تلك المجموعات وتجهيـز ونشر المعلومات الشخصية، ويمكن أن تحد من القدرة على نقل البيانات إلى بلدان أخرى.

5.1.15 منع إساءة استخدام المعلومات ومرافق المعالجة

التحكم

ينبغي أن يكون رادعا للمستخدمين من استخدام المعلومات ومرافق المعالجة لأغراض غير مـأذون بها.

توجيهات التطبيق

ينبغي للإدارة الموافقة على استخدام المعلومات ومرافق المعالجـة. أي اسـتخدام لهـذه المرافـق لأغراض غير تجارية دون موافقة الإدارة (انظر 6.1.4)، أو غير مأذون به الأغـراض، وينبغـي اعتبار الاستخدام للمرافق. وإذا كان أي نشاط غير مصرح به وحدد من خلال مراقبـة أو وسـائل أخرى، وهذا النشاط يجب توجيه اهتمام الفرد (المدير المعني) للنظر في التأديبية المناسـبة و / أو اتخاذ إجراءات قانونية.
المشورة القانونية التي ينبغي اتخاذها قبل تنفيذ إجراءات الرصد.
جميع المستخدمين ينبغي أن تدرك على وجه الدقة على نطاق وصول ويسمح للمراقبة فـي مكـان للكشف عن الاستخدام غير المسموح به. ويمكن تحقيق ذلك من خـلال إعطـاء المـستخدمين إذن خطي، نسخة من التي ينبغي أن تكون موقعة من المستخدمين بشكل آمـن والتـي احتفظـت بهـا المنظمة. من الموظفين المنظمة والمتعاقدين والمستخدمين والطرف الثالث ينبغي أن لا يحصلون إلا أن كان مأذون به.

عند الدخول، رسالة تهديد وينبغي أن تعرض معلومات تشير إلى أن مرفق تجهيز دخلت يجري هو ما تملكه المنظمة من الدخول غير المصرح به، وأنه أمر غيـر مـسموح بـه.وعلـى المـستخدم الاعتراف والاستجابة على نحو ملائم لهذه الرسالة التي تظهر على الشاشة لتواصل مع دخول على عملية (11.5.1).

معلومات أخرى
المعلومات وتجهيز مرافق المنظمة في المقام الأول، أو على سبيل الحصر أغراض تجارية.

كشف التسلل، والمحتوى والتفتيش والمراقبة وغيرها من أدوات قد تساعد في منع وكـشف سـوء استخدام المعلومات ومرافق المعالجة.

العديد من الدول لديها تشريعات لحماية ضد سوء استخدام الحاسوب. قـد يكـون جريمـة جنائيـة استخدام الكمبيوتر لأغراض غير مأذون بها.

مشروعية استخدام الرصد تختلف من بلد لآخر، وربما تحتاج إلى إدارة تقديم المشورة إلـى جميـع مستخدمي هذا الرصد و / أو الحصول على موافقتها. حيث دخل النظام ويستخدم للجمهـور (مثـل عامة خادم الويب)، ويخضع للمراقبة الأمنيـة، ورسـالة وقـال ينبغـي أن يـتم عـرض ذلـك.

6.1.15 لائحة ضوابط التشفير

التحكم

ضوابط التشفير ينبغي أن تستخدم في الامتثال لجميع الاتفاقات ذات الصلة والقوانين واللوائح.

توجيهات التطبيق

البنود التالية ينبغي النظر في الامتثال للاتفاقات ذات الصلة والقوانين واللوائح:

أ) القيود المفروضة على استيراد و/أو تصدير أجهزة وبرامج الحاسوب لأداء وظائف التشفير؛

ب) القيود المفروضة على استيراد و / أو تصدير أجهزة وبرامج الحاسوب والذي يستهدف لتشفير وظائف وأضاف إليها؛

ج) القيود المفروضة على استخدام التشفير؛

د) إلزامية أو تقديرية طرق الحصول عليها من السلطات في هذه البلدان إلى المعلومات مشفرة من خلال أجهزة أو برامج لتوفير سرية المضمون.

المشورة القانونية وينبغي السعي لضمان الامتثال للقوانين واللوائح الوطنية. قبل ترميز المعلومات المشفرة أو ضوابط انتقلت إلى بلد آخر ، وينبغي تقديم المشورة القانونية كما يتعين اتخاذها.

2.15 *الامتثال للسياسات والمعايير الأمنية والفنية*

الهدف: ضمان الامتثال للأنظمة والسياسات التنظيمية والمعايير الأمنية.

ينبغي إعادة النظر في أمن نظم المعلومات بصورة منتظمة. ويستعرض هذا ينبغي أن يقـوم علـى السياسات الأمنية المناسبة والتقنية مناهج ونظم المعلومات يجب المراجعة للامتثال للتطبيق الأمـن وتنفيذ معايير وضوابط أمنية موثقة.

1.2.15 الامتثال للسياسات والمعايير الأمنية

التحكم

ينبغي من المديرين التأكد من أن جميع الإجراءات الأمنية داخل المنطقة الخاضعة لمسؤوليتهم وتنفيذ صحيح لتحقيق الامتثال للسياسات والمعايير الأمنية.

توجيهات التطبيق

وينبغي لمديري استعراض بانتظام امتثال تجهيز المعلومات داخل مناطق المسؤولية الأمنية المناسبة مع السياسات والمعايير ، وغيرها من المتطلبات الأمنية.

إن وجدت الامتثال ونتيجة لهذا الاستعراض، ينبغي للمديرين أن:

أ) تحديد أسباب عدم الامتثال؛

ب) تقييم الحاجة إلى اتخاذ إجراءات لضمان عدم الامتثال لا تتكرر؛

ج) تحديد وتنفيذ الإجراءات التصحيحية؛

د) إعادة النظر في اتخاذ إجراءات تصحيحية.

نتائج الاستعراضات والإجراءات التصحيحية التي يقوم بها المديرون وينبغي تسجيلها والحفاظ على السجلات. وعلى المديرين عرض تقرير النتائج على الأشخاص الذين يتولون القيام بعملية الاستعراضات المستقلة (انظر 6.1.8) ، عندما تتم مراجعة مستقلة في المنطقة من المسؤولية.

معلومات أخرى

مراقبة التنفيذية لنظام استخدام يغطي 10.10.

2.2.15 التحقق من الامتثال التقني

التحكم

نظم المعلومات وينبغي فحصها بانتظام للتأكد من الامتثال لتنفيذ الأمن المعايير.

توجيهات التطبيق

تقنية التحقق من الامتثال ينبغي أن يقوم إما يدويا (بدعم من مناسبة أدوات البرمجيات ، وإذا لزم الأمر) عن طريق نظام متمرس مهندس ، و / أو بمساعدة الأدوات الآلية ، والتي تولد تقرير فني لاحقا تفسير تقني متخصص.

إذا تغلغل الضعف أو اختبارات التقييم المستخدمة، ينبغي توخي الحذر في حد ذاتها أنشطة يمكن أن تؤدي إلى حل وسط للأمن النظام. هذه التجارب ينبغي أن يخطط لها، وموثقة للتكرار.

أي فحص تقني الامتثال ينبغي إن تقوم بها جهة مختصة، أو تحت إشراف أشخاص متخصصين.

معلومات أخرى

يشمل تقنية التحقق من الامتثال دراسة النظم التشغيلية لضمان لأجهزة والبرمجيات وضوابط تم تنفيذها بشكل صحيح. هذا النوع من التحقق من الامتثال ويتطلب خبرة تقنية متخصصة.

كما يشمل التحقق من الامتثال، على سبيل المثال، اختبار الاختراق وقابلية التأثر،التي يمكن أن يقوم به خبراء مستقلون التعاقد تحديدا لهذا الغرض. وهذا يمكن أن تكون مفيدة في الكشف عن مواطن الضعف في النظام والتحقق من مدى فعالية الضوابط وفي منع الدخول غير المصرح به نظرا لنقاط الضعف هذه.

اختبار الاختراق وتقييم مدى التأثر تقديم لمحة سريعة عن نظام معين في الدولة وقت محدد. فإن لقطة يقتصر على تلك الأجزاء من النظام فعلا خلال اختبار محاولة اختراق. اختبار الاختراق وتقييم مدى التأثر ليست بديلا عن المخاطر تقييم.

3.15 *اعتبارات مراجعة نظم المعلومات*

الهدف: تحقيق أقصى قدر من الفعالية وتقليل التدخل من/إلى عملية مراجعة ومحاسبة نظم المعلومات. ينبغي أن تكون هناك ضوابط لحماية نظم التشغيل ومراجعة الحسابات ونظم المعلومات خلال أدوات لمراجعة الحسابات. مطلوب أيضا من الحماية للحفاظ على سلامتها ومنع إساءة استخدام وسائل المراجعة.

1.3.15 مراجعة ضوابط نظم المعلومات

التحكم

متطلبات مراجعة الحسابات والتحقق من الأنشطة التي تشمل النظم التشغيلية وينبغي أن يخطط لها بعناية واتفقوا على تقليل خطر الاضطرابات في مجال الأعمال التجارية.

توجيهات التطبيق

المبادئ التوجيهية التالية ينبغي مراعاتها:

أ) متطلبات مراجعة الحسابات ينبغي أن يتفق مع الإدارة المناسبة؛

ب) في نطاق الضوابط ينبغي الاتفاق والتي تسيطر عليها؛

ج) الفحص ينبغي أن تقتصر على قراءة فقط الحصول على البرمجيات والبيانات؛

د) عدم وصول للقراءة فقط وينبغي إلا يسمح لعزل نسخ من ملفات النظام، والتي ينبغـي أن تمحى عندما تكتمل فيها مراجعة الحسابات ، أو بالنظر إلى الحماية المناسبة في حـال هناك واجب الحفاظ على هذه الملفات في إطار مراجعة الوثائق المطلوبة؛

هـ) الموارد اللازمة لأداء الفحص ينبغي تحديدها صراحة وإتاحتها؛

و) الاحتياجات الخاصة أو الإضافية وتجهيزها وينبغي تحديدها والاتفاق ؛

ز) وصول جميع وينبغي رصد وتسجيل لإنتاج إشارة تعقب ؛ استخدام للوقت ختم بالإشارة إلى محاكمات ينبغيالنظر في البيانات أو النظم الدرجة ؛

ح) جميع الإجراءات والمتطلبات ، والمسؤوليات التي ينبغي أن تكون موثقة؛

ط) للشخص تنفيذ عملية المراجعة ينبغي أن تكون مستقلة عن أنشطة المراجعة.

2.3.15 حماية أدوات مراجعة نظم المعلومات

التحكم

الحصول على المعلومات ونظم المراجعة وينبغي حماية وسائل لمنع أي سوء استخدام أو وسط.

توجيهات التطبيق

مراجعة الحسابات ونظم المعلومات والأدوات ، على سبيل المثال برمجيات أو ملفـات البيانـات ، وينبغي أن يكون منفصلا عن والتنمية نظم التشغيل وليس في الشريط المكتبات أو المستعملة ، مـا لم يكن في ضوء مستوى مناسب من حماية إضافية.

معلومات أخرى

إذا كانت أطراف أخرى متورطة في مراجعة الحسابات، قد تكون هناك مخاطر سوء استخدام هـذه الأدوات المراجعة الثالثة الأطراف، والمعلومات التي يتم الحصول عليها عن طريق طرف ثالث في هذه المنظمة. ضوابط مثل 6.2.1 (لتقييم المخاطر و9.1.2 (لتقييد الوصول المادي) ويمكن النظـر للتصدي لهذه المخاطر، وأية، مثل تغيير كلمات السر والكشف عنها على الفور لمراجعي الحسابات، التي ينبغي اتخاذها.