مجلس أبوظبي للتعليم
Abu Dhabi Education Council
Education First التعليم أولاً

سياسة أمن المعلومات

التحكم في الوثيقة

النسخة	**3.3**
الحالة	**نهائية**
إعداد الوثيقة	**شركة** مجلس أبوظبي للتعليم
تاريخ الإعداد	سبتمبر 2010
آخر تاريخ لتحديث الوثيقة	يوليو 2011
عدد الصفحات	**80**
فترة المراجعة	**عام**
التصنيف	**للاستخدام الرسمي**

فهرس المحتويات

الشخص/الجهة المسئولة عن هذه الوثيقة

اعتماد الوثيقة

مصدر وجهة التحكم في الوثيقة:

مقدمة

القسم الأول: السياسة الأمنية

1-1 سياسات أمن المعلومات

1-2 مراجعة سياسة أمن المعلومات

1-3 وضع خطط أمن المعلومات

القسم الثاني: أمن المجلس

2-1 التزام إدارة المجلس بحماية أمن المعلومات

2-2 التنسيق بشأن أمن المعلومات

2-3 توزيع المسؤوليات الخاصة بأمن المعلومات

2-4 الاستثناء من هذه السياسة

2-5 التصريح باستخدام مرافق معالجة المعلومات

2-6 اتفاقيات سرية المعلومات

2-7 العلاقات مع الجهات والسلطات المختصة

2-8 العلاقات مع الجماعات ذات المصالح الخاصة

2-9 المراجعة المستقلة لأمن المعلومات

2-10 تحديد المخاطر المتعلقة بالأطراف الخارجية

2-11 يجب مراعاة المتطلبات التالية عند إبرام الاتفاقيات مع الغير

2-12 الاتصالات والتواصل

2-13 إدارة الأداء

القسم الثالث: إدارة الأصول

3-1 جرد الأصول

3-2 ملكية الأصول

3-3 تصنيف المعلومات

3-4 التعامل المتناغم مع المعلومات

3-5 الاستخدام المقبول للأصول

القسم الرابع: مسؤولية موظفي المجلس

4-1 الأدوار والمسئوليات الأمنية

4-2 التحريات الأمنية

4-3 بنود وشروط التوظيف

4-4 مسئوليات الإدارة

4-5 زيادة الوعي بأمن المعلومات والتدريب والتثقيف

4-6 الإجراءات التأديبية

4-7 المسئوليات الخاصة بإنهاء الخدمة

8-4 إعادة الأصول

القسم الخامس: الأمن المادي والبيئي

5-1 حدود الأمن المادي

5-2 أدوات التحكم بدخول الأشخاص

5-3 المكاتب والغرف والمرافق المحظورة

5-4 الحماية من التهديدات الخارجية والبيئية

5-5 العمل في المناطق المحظورة

5-6 الأجهزة والمعدات الحساسة

5-7 مرافق الدعم

5-8 أمن الوصلات (الكابلات والأسلاك)

5-9 صيانة الأجهزة والمعدات

5-10 أمن الأجهزة والمعدات خارج المبنى

5-11 التخلص الآمن من الأجهزة والمعدات أو إعادة استخدامها

5-12 عدم نقل الأصول (الأجهزة والمعدات)

القسم السادس: إدارة الاتصالات والعمليات

6-1 إجراءات التشغيل الموثقة

6-2 إدارة التغييرات

6-3 الفصل بين المهام والواجبات

6-4 الفصل بين التطوير والاختبار والمرافق التشغيلية

6-5 الخطط الخاصة بالطاقة الاستيعابية

6-6 اعتماد النظام

6-7 الحماية من الفيروسات ومكافحتها
6-8 أدوات التحكم في الشفرة/الأكواد المتنقلة
6-9 النسخ الاحتياطية من المعلومات
6-10 أدوات التحكم بالشبكات
6-11 أمن خدمات الشبكات
6-12 إدارة الوسائط القابلة للإزالة
6-13 التخلص من الوسائط
6-14 إجراءات التعامل مع المعلومات
6-15 أمن وثائق النظام
6-16 سياسات وإجراءات تبادل المعلومات
6-17 اتفاقيات تبادل المعلومات
6-18 الوسائط المادية أثناء النقل
6-19 الرسائل الإلكترونية
6-20 أنظمة معلومات العمل
6-21 المعلومات المعلنة
6-22 سجلات التدقيق
6-23 مراقبة استخدام الأنظمة
6-24 حماية المعلومات المتعلقة بالسجلات
6-25 سجلات المديرين والمشغلين
6-26 تسجيل الأعطال
6-27 تزامن التوقيت
6-28 تقديم الخدمات
6-29 متابعة ومراجعة خدمات الغير
6-30 إدارة التغييرات التي تستحدث على خدمات الغير
6-31 الربط البيني

القسم السابع: التحكم بالوصول

7-1 متطلبات العمل الخاصة بالتحكم في الوصول (ACCESS CONTROL)

7-2 إدارة وصول المستخدمين

7-3 إدارة الامتيازات

7-4 إدارة كلمات مرور المستخدمين

7.5 مراجعة حقوق وصول المستخدم

7-6 استخدام كلمة المرور

7-7 التعامل مع الأجهزة عند عدم تواجد المستخدم

7-8 إخلاء المكتب والشاشات

7-9 السياسة المتبعة بشأن خدمات الشبكات

7-10 التحقق من هوية المستخدم فيما يخص الاتصال من الخارج

7-11 التعرف على الأجهزة في الشبكات

7-12 منفذ التشخيص عن بعد والتهيئة

7-13 الفصل بين الشبكات

7-14 التحكم في اتصال الشبكات

7-15 التحكم في توجيه الشبكات

7-16 إجراءات تسجيل الدخول الآمن

7-17 التعرف على المستخدم والتحقق منه

7-18 نظام إدارة كلمات المرور

7-19 استخدام مرافق النظام

7-20 إنهاء الجلسات غير النشطة/غير المستخدمة

7-21 تحديد زمن الاتصال

7-22 تقييد الوصول إلى المعلومات

7-23 عزل الأنظمة الحساسة

7-24 أجهزة الحاسب والاتصال النقالة

7-25 العمل من خارج المجلس

القسم الثامن: تطوير وصيانة الأنظمة

8-1 المتطلبات الأمنية للأنظمة

8-2 التحقق من صحة البيانات المدخلة

8-3 التحكم في المعالجة الداخلية

8-4 سلامة الرسائل

8-5 التحقق من المخرجات

8-6 السياسة المتعلقة باستخدام أدوات التحكم في التشفير

8-7 التحكم في برامج التشغيل

8-8 حماية بيانات اختبار النظام

8-9 التحكم في الوصول لكود مصدر البرنامج

8-10 إجراءات التحكم في التغيير

8-11 المراجعة الفنية للتطبيقات بعد إدخال التغييرات على أنظمة التشغيل

8-12 القيود المتعلقة بتغيير حزم البرامج

8-13 تسرب المعلومات

8-14 تطوير البرامج عن طريق التعهيد

8-15 التحكم في نقاط الضعف الفنية

القسم التاسع: إدارة الحوادث المتعلقة بأمن المعلومات

9-1 الإبلاغ عن حوادث أمن المعلومات

9-2 الإبلاغ عن نقاط الضعف الأمنية

9-3 المسئوليات والإجراءات

9-4 التعلم من خلال التعامل مع حوادث أمن المعلومات

9-5 جمع الأدلة

القسم العاشر: إدارة استمرارية العمل

10-1 إدخال أمن المعلومات ضمن عملية إدارة استمرارية العمل

10-2 استمرارية العمل وتقييم المخاطر

10-3 تطوير وتطبيق خطط لضمان استمرارية العمل تشمل أمن المعلومات

10-4 إطار خطط استمرارية العمل

10-5 اختبار خطط ضمان استمرارية العمل وصيانتها وإعادة تقييمها

القسم الحادي عشر: الالتزامات القانونية

11-1 التعرف على التشريعات الملزمة

11-2 حقوق الطبع والنشر الخاصة بالبرامج

11-3 حماية سجلات المجلس

11-4 حماية البيانات وخصوصية المعلومات الشخصية

11–5 منع إساءة استخدام مرافق معالجة البيانات

11–6 اللوائح الحاكمة للتشفير

11–7 الالتزام القانوني بالسياسات والمعايير الأمنية

11–8 مراجعة الالتزامات الفنية

11–9 تدقيق أدوات التحكم بأنظمة المعلومات

مقدمة

أ. فكرة عامة

هناك العديد من التهديدات والمخاطر التي يمكن أن تهدد سلامة موظفي المجلس ومعلوماته ، وهي تأخذ أشكالاً عديدة تتراوح بين الأفعال الضارة التي يرتكبها الأشخاص عن عمد (وتشمل مجرمي الإنترنت بكافة أنواعهم) والثغرات الأمنية التي تحتويها مختلف الأنظمة الإلكترونية التي يستخدمها المجلس وكذلك المخاطر الناجمة عن الأنشطة التي يقوم بها موظفو المجلس أو غيرهم من غير المختصين. وغالباً ما يتسبب غياب الوعي بالاعتبارات الخاصة بأمن المعلومات في تسهيل استغلال الأخرين لهذه المخاطر.

لقد تم وضع سياسات المجلس المتعلقة بأمن المعلومات بغرض وضع قواعد العمل الواضحة التي يجب إتباعها والالتزام بها حتى يمكن تحسين حالة أمن المعلومات في إطار حماية موظفي المجلس ومعلوماته، وبغرض تحقيق الأهداف والتوقعات الإدارية لموظفي المجلس والأطراف الخارجية من أجل توفير الحالة الأمنية المطلوبة على الدوام.

من الأهمية بمكان التأكيد على أن سياسات الأمن بالمجلس مبنية على أساس شهادة الإيزو ISO 27001:2005 "كود تكنولوجيا المعلومات لممارسة إدارة أمن المعلومات"، وهو كود معترف به ويطبق دولياً.

ب. الغرض

إن الغرض من وضع سياسات أمن المعلومات بالمجلس هو حماية موظفي المجلس ومعلوماته بصورة أمنة وعملية واقتصادية. وتتعلق المخاطر التي تعالجها تلك السياسات بالأمور التالية:

- المعلومات التي يحتفظ بها ويعالجها المجلس نيابة عن العملاء أو لأغراض الاستخدام الداخلي.
- المعلومات التي تحتفظ بها وتعالجها الأطراف الخارجية نيابة عن المجلس.
- تكنولوجيا المعلومات.
- موظفو المجلس.
- المباني والمرافق والأبنية وغيرها من الأملاك التي يملكها أو يشغلها المجلس.
- رأس المال الفكري للمجلس.
- سمعة المجلس ومصداقيته واستمراره.

ج. النطاق

توفر سياسات المجلس لأمن المعلومات الإرشادات اللازمة لجميع المستخدمين بما في ذلك كافة العاملين التابعين للمجلس بالمقر الرئيسي والمناطق التعليمية/المكاتب الإقليمية والمدارس ، ومن المتوقع من كافة المستخدمين الالتزام والتقيد بالإرشادات والتعليمات الواردة في هذه السياسات من أجل وضع وإعداد الإجراءات التشغيلية اللازمة والتي تسهم في تحقيق أهداف إدارة المجلس ومتطلباتها فيمل يتعلق بحماية أصول المعلومات التي يمتلكها المجلس

وتنطبق هذه السياسة على جميع الأنظمة سواء تلك التي يمتلكها المجلس و/أو التي يشرف عليها موظفوه علاوة على جميع الأنظمة التي يقوم باستخدامها أطراف أخرى لصالح تحقيق أهداف العمل بالمجلس.

تنطبق هذه السياسة أيضاً على كافة الأطراف الأخرى التي تقوم بأداء أعمال لصالح المجلس.

د. الأدوار والمسؤوليات

لضمان فعالية أمن المعلومات يجب أن يكون العمل محصلة مجهود جماعي، ويجب أن يتضمن ذلك مشاركة ودعم من قبل جميع المستخدمين الذين يتعاملون مع المعلومات و/أو أنظمة المعلومات. ولهذا الغرض فإن هذه السياسة تنص بوضوح على مسؤوليات المستخدمين والخطوات الواجب عليهم اتخاذها لحماية الأصول المعلوماتية وأنظمة المعلومات الخاصة بالمجلس، حيث تتضمن الوثيقة وصفاً للطرق التي يمكن من خلالها حماية المعلومات والأنظمة والاستجابة لمجموعة إلى التهديدات ومن بينها الدخول غير المصرح به وإفشاء المعلومات ونسخها وتعديلها والاستيلاء عليها وتدميرها وفقدها وإساءة استخدامها ومنع استخدامها.

هـ. التعريفات:

من الواضح أن موظفي المجلس المكلفون بمراجعة سياسات أمن المعلومات الخاصة بالمجلس ليس لديهم معرفة كافية بالمصطلحات الواردة في هذه الوثيقة، ولتجنب اللبس أو الفهم الخاطئ فقد أوردنا التعريفات اللازمة أدناه:

- **المستخدم:**

يشمل تعريف "المستخدم" لأغراض هذه السياسة أي شخص لدية إمكانية الوصول للمعلومات، ويشمل ذلك على سبيل المثال لا الحصر كافة الموظفين و/أو الأفراد و/أو الاستشاريين و/أو الموظفين المنتدبين لاستشاريين أو وكلائهم أو ممثليهم من يعملون لصالح المجلس أو يؤدون خدمات للمجلس.

- **مالكو الأصول المعلوماتية:**

مالكو الأصول المعلوماتية هم كبار المديرين المسئولين عن حماية أصول معلوماتية معينة هامة.

- **النظام:**

النظام هو عبارة عن مصطلح عام يشمل أي تطبيق أو شبكة/مكونات/أجهزة بنية تحتية أو جهاز خادم أو أنظمة الصوت أو جهاز تحكم (على سبيل المثال البطاقات الممغنطة) أو قواعد البيانات وغيرها من الأجهزة/الحلول التي لا تعد أحد أجهزة حاسب المستخدم.

- **الأطراف الخارجية (الغير)**

تشير "الاطراف الخارجية" إلى كافة الاستشاريين أو المتعهدين أو المقاولين أوالمقاولين من الباطن أو المنتدبين الخارجين ممن يتعاملون مع المجلس ويقدمون خدماتهم للمجلس.

و. الالتزام

ليس من الممكن تطبيق سياسات أمن المعلومات الخاصة بالمجلس بفعالية ونجاح دون تعاون جميع المستخدمين، ولذلك يصبح من الضروري أن يتم الحفاظ على سرية المعلومات الخاصة بالعمل من خلال وعي المستخدمين بالمتطلبات والشروط الأمنية التي تنص عليها سياسات أمن المعلومات الخاصة بالمجلس والالتزام التام بها.

ز. أقسام السياسة

تتكون سياسة أمن المعلومات الخاصة بالمجلس من أحد عشر قسماً كالتالي:

1- نبذة عن السياسة الأمنية
2- الأمن المؤسسي

3- إدارة الأصول
4- أمن الموظفين
5- الأمن المادي والبيئي
6- إدارة الاتصالات والعمليات
7- التحكم في الوصول
8- تطوير وصيانة الأنظمة
9- إدارة حوادث أمن المعلومات
10- إدارة استمرارية العمل
11- الالتزام

القسم الأول

السياسة الأمنية

1. السياسة الأمنية

إن الغرض من السياسات التي يتضمنها هذا القسم هو ضمان الإدارة والدعم الموحدين فيما يتعلق بأمن المعلومات وفقاً للشروط والمتطلبات المعمول بها في هذا المجال والقوانين واللوائح ذات الصلة.

1-1 سياسات أمن المعلومات

تعتبر سياسات أمن المعلومات المتضمنة في هذه الوثيقة دليلاً شاملاً لجميع المستخدمين بغرض تمكينهم من حماية الأصول المعلوماتية الخاصة بالمجلس، وهي تحتوي على مجموعة القواعد الأساسية التي سوف يضع المجلس بشأنها الخطط والمعايير والإجراءات التفصيلية المتعلقة بأمن المعلومات بغرض الوفاء بالشروط والمتطلبات المعمول بها في هذا المجال.

1-2 مراجعة سياسة أمن المعلومات

يعد مسئول/أخصائي أمن المعلومات هو المسؤول عن سياسات أمن المعلومات الخاصة بالمجلس، في حين تكون لجنة أمن المعلومات مسئولة عن تطبيق السياسة بعد اعتمادها من قبل مجلس الإدارة.

يجب أن يتم مراجعة السياسة بصورة رسمية:

- على فترات منتظمة بواسطة المستوى الإداري الملائم.
- في حال تغيير بيئة العمل أو إستراتيجية المؤسسة.
- في حال تغيير الالتزامات القانونية أو التنظيمية.

1-3 تخطيط أمن المعلومات

يتم وضع وإدارة برنامج لأمن المعلومات.

- يتم استحداث منصب مسؤول أول أمن المعلومات أو ما يعادله ليشغله شخص يتمتع بالكفاءات اللازمة ليكون مسئولاً عن إدارة برنامج أمن المعلومات بالمجلس والإشراف على تنفيذه.
- يتم تحديد نطاق وحدود كل خدمة من الخدمات من ناحية خصائص العمل الذي تساندها تلك الخدمة والجهة والموقع والأصول (بما يشمل ملاك الأصول) والتكنولوجيا المتعلقة بذلك العمل إضافة إلى أي تفاصيل/مبررات أي استثناءات موجودة من نطاق التحكم.

- يتم إنشاء سجل للمخاطر الخاصة بكل خدمة من الخدمات، ويجب أن يشمل السجل تعريفاً وتقييماً لتلك المخاطر بالنسبة لأصول النظام، وتتضمن عملية تقييم المخاطر تحديد التهديدات التي تواجه الأصول والثغرات الأمنية التي قد تستغلها تلك المخاطر والآثار المحتملة على فقدان سرية وسلامة وتوفر المعلومات، كما ينبغي أن يشمل تحليل سجل المخاطر الخاص بكل خدمة الآثار المترتبة على العمل في حال إخفاق إجراءات أمن النظام واحتمالية حدوث ذلك الإخفاق الأمني وتحديد المخاطر المقبولة ومستوى المخاطر المتوقع.
- يتم اختيار وتطبيق أدوات التحكم الملائمة لضمان تقليل المخاطر أو الحد من آثارها إلى المستوى المقبول، على أن تكون عملية اختيار وتطبيق أدوات التحكم متماشية تماماً مع القوانين المعمول بها مع الالتزام بحقوق الملكية الفكرية وحماية سجلات المؤسسة والبيانات الشخصية والحيلولة دون إساءة استخدام المعلومات بواسطة مرافق معالجة المعلومات.

القسم الثاني

الأمن المؤسسي

2. الأمن المؤسسي

إن الغرض من السياسات التي يتضمنها هذا القسم هو ضمان وضع إطار إداري للحفاظ على سياسات أمن المعلومات الخاصة بالمجلس والتأكد من تماشي هذه السياسات مع متطلبات ومبادرات المجلس ودعمها لتلك المتطلبات والمبادرات.

2-1 التزام إدارة المجلس بحماية أمن المعلومات

تعتبر الإدارة العليا للمجلس هي المسئولة عن تطبيق أسس ومبادئ الحوكمة المؤسساتية ككل، وبالتالي فهي مسئولة عن إدارة مخاطر أمن المعلومات والتحكم فيها باعتبار ذلك جزء لا يتجزأ من حوكمة المؤسسات.

يعتمد المديرون التنفيذيون بصورة كبيرة على لجنة أمن المعلومات من أجل تنسيق الأنشطة عبر إدارات وأقسام المجلس، والتأكد من وضع السياسات المناسبة موضع التطبيق بغرض دعم المبادئ والمبادرات الأمنية للمجلس، كما يعتمد المديرون التنفيذيون أيضاً على الآراء والملاحظات التي يقدمها أخصائي أول أمن المعلومات ولجنة أمن المعلومات والمدققون والشؤون القانونية وغيرها من الجهات لضمان تطبيق المبادئ والسياسات على أرض الواقع.

تظهر لجنة أمن المعلومات التزامها بضمان بأمن المعلومات عن طريق القيام بما يلي:

- الالتزام الواضح والصريح بدعم تطبيق نظام إدارة أمن المجلس والإشراف عليه
- مراجعة وإعادة اعتماد السياسات كل عام
- اعتماد ميزانية أمن المعلومات والتي يام إعدادها كجزء من ميزانية تكنولوجيا المعلومات بالمجلس
- استلام تقارير الإدارة الخاصة بمقاييس أداء أمن المعلومات والحوادث الأمنية وطلبات الاستثمار وغيرها ومن ثم العمل بناء على تلك التقارير.

2-2 التنسيق بشأن أمن المعلومات

يتم إنشاء لجنة لأمن المعلومات لها صلاحيات القيادة الإدارية بغرض التصديق على سياسة أمن المعلومات وتوزيع الأدوار الأمنية والتنسيق بشأن تطبيق الإجراءات الأمنية عبر إدارات وأقسام المجلس، على أن تكون اللجنة مسؤولة بالكامل عن سياسات أمن المعلومات.

إن الهدف من إنشاء اللجنة هو ضمان التوجيه السليم والواضح وتوفير الدعم الإداري الملموس لمبادرات أمن المعلومات، وتتألف اللجنة من الأعضاء التالية أسماؤهم:

- مدير عام المجلس
- المديرون التنفيذيون
- مدير إدارة تكنولوجيا المعلومات
- مدير إدارة المشتريات والعقود
- مدير إدارة البنية التحتية والمرافق
- مدير إدارة الشؤون المالية
- مدير إدارة الموارد البشرية
- مدير إدارة التدقيق الداخلي
- مدير إدارة السياسات والتخطيط والأداء
- مدير إدارة الشؤون القانونية
- مدير إدارة المناهج والتقييم
- مدير إدارة تراخيص واعتماد المدارس
- مدير إدارة البعثات والإرشاد – قطاع التعليم العالي
- مدير إدارة برامج التربية الخاصة

تشمل مسئوليات اللجنة ما يلي:

- إدارة عملية الإشراف على الجوانب المادية والمنطقية للأمن وبصفة خاصة أمن المعلومات.
- التنسيق بشأن إطار الأمن بالكامل في المجلس وإدارته بما يشمل أدوات التحكم في أمن المعلومات في جميع مواقع المجلس المعنية.
- التكليف بالبيانات الخاصة بسياسة أمن المعلومات أو إعدادها ومن ثم اعتمادها تمهيداً لاستخدامها في المجلس.
- مراجعة البيانات الخاصة بسياسة أمن المعلومات بصفة دورية لضمان فعالية وكفاءة البنية التحتية لأدوات التحكم بأمن المعلومات ككل واقتراح التعديلات الملائمة عند الحاجة.
- مراجعة الحوادث الأمنية الخطيرة ووضع مقترحات بالحلول الإستراتيجية اللازمة، كلما أمكن ذلك، بغرض معالجة أسبابها الجذرية.
- رفع التقارير الدورية بشأن حالة البنية التحتية لأدوات التحكم بأمن المعلومات.

تكون لجنة أمن المعلومات بالمجلس جهة استشارية بشأن أمن المعلومات تقدم الآراء والتوصيات لمسئول أمن المعلومات بالمجلس.

3-2 تحديد المسؤوليات الخاصة بأمن المعلومات

تتمثل مسئوليات ومهام **أخصائي أول أمن المعلومات** فيما يلي:

- دعم ملاك الأصول المعلوماتية والمديرين فيما يخص تحديد وتطبيق أدوات التحكم والعمليات وأدوات الدعم بما يضمن الالتزام بالدليل الخاص بالسياسة وإدارة المخاطر المتعلقة بأمن المعلومات.
- مراجعة والإشراف على الالتزام بالبيانات المتعلقة بالسياسة.
- جمع وتحليل البيانات الخاصة بمقاييس وحوادث أمن المعلومات والتعليق عليها.
- إجراء التنسيق اللازم مع الجهات الداخلية ذات الصلة كعمليات تكنولوجيا المعلومات وإدارات الأعمال والتدقيق الداخلي إضافة إلى لجنة أمن المعلومات والجهات الخارجية.
- تنظيم حملة لرفع وعي الموظفين بشأن الأمن وفهمهم للمتطلبات والشروط الأمنية اللازمة.

تتمثل مسئوليات ومهام مديري إدارات المجلس فيما يلي:

- الحرص على تطبيق سياسات أمن المعلومات بصفة يومية.
- التحقق من وضع أدوات التحكم الفنية والمادية والإجرائية موضع التطبيق وفقاً لهذا الدليل والتأكد من تطبيق جميع الموظفين لها بالصورة السليمة.
- التوجيه وتوفير الموارد والدعم وأعمال المراجعة الضرورية لضمان حماية الأصول المعلوماتية التي في نطاق مسؤولياتهم بالصورة السليمة.

تتمثل مسئوليات ومهام **ملاك الأصول المعلوماتية** فيما يلي:

- تصنيف وحماية الأصول المعلوماتية بالصورة السليمة
- السماح بالوصول إلى المعلومات وفقاً للتصنيف المتبع واحتياجات العمل
- التحقق من إجراء المراجعات الدورية اللازمة للوصول إلى النظام/البيانات

- مراقبة الالتزام القانوني للمتطلبات والشروط المتعلقة بحماية الأصول الخاصة بهم
- [فيما يخص التطورات الجديدة الخاصة بتطبيق الأنظمة] القيام بعمليات التقييم الخاصة بأمن المعلومات أو تعهيدها Outsourcing بغرض ضمان تحديد وتوثيق المتطلبات والشروط المتعلقة بأمن المعلومات في مرحلة مبكرة من ذلك التطوير.

تتمثل مسئوليات ومهام **جميع موظفي المجلس** (على سبيل المثال: الموظفون الذين يتلقون رواتبهم من المجلس وغيرهم ممن يعمل بصورة مماثلة كالمقاولين والاستشاريين والمختصين بتقييم الطلبة وغيرهم) كالتالي:

- الالتزام بالسياسات المنصوص عليها في هذا الدليل في الأمور التي تتعلق بعملهم.
- الحفاظ على أمن كافة المعلومات التي بعهدتهم.

ويجب أن تتضمن إجراءات وشروط تعيين الموظفين الجدد الالتزام بالسياسات الخاصة بأمن المعلومات المعمول بها في المجلس، وفي حال عدم التزام الموظف بتلك السياسات يتعرض للإجراءات التأديبية التي قد تشمل إنهاء عمله أو عقد عمله و/أو وملاحقته قضائياً.

2-4 الاستثناء من هذه السياسة

يجوز لمسئول أمن المعلومات اقتراح استثناء أحد الأصول المعلوماتية التي بعهدته من نصوص السياسة المتضمنة في هذا الدليل. ويكون مدير أمن المعلومات مسئولا عن تحليل المخاطر التي تنشأ عن الاستثناءات المقترحة، وفي معظم الحالات يجب عليه تحديد أدوات التحكم التي من شأنها الحد من آثار تلك المخاطر.

في حال تعارض أو عدم تناغم أي حكم من أحكام هذه السياسة مع أي حكم محدد بالقانون أو بسياسة حكومة أبوظبي، يسود الحكم الخاص بالقانون أو السياسة الحكومية على الحكم الخاص بهذه السياسة.

2-5 التصريح باستخدام مرافق معالجة المعلومات

تعتمد لجنة أمن المعلومات المرافق والأنظمة والتطبيقات الجديدة الهامة وغيرها فيما يتعلق بتكنولوجيا المعلومات، مع تحديد/تأكيد الغرض منها واستخدامها، والتأكد من الالتزام بتطبيق كافة السياسات الأمنية ذات الصلة وغيرها من المتطلبات الخاصة بأدوات التحكم. وفي سياق هذه العملية، يجب تحديد واحد أو أكثر من مسئولي أمن المعلومات.

عند الضرورة تقوم إدارة تكنولوجيا المعلومات وإدارة أمن المعلومات وغيرها بفحص أجهزة وبرامج تكنولوجيا المعلومات للتحقق من تماشيها مع باقي مكونات النظام وهذا الدليل، كما يجب أن تتحقق إدارة تكنولوجيا المعلومات من البرامج التي يطورها الموظفون باستخدام برنامج "OFFICE" وغيره من برامج سطح المكتب (كجداول Excel وقواعد البيانات) لضمان الدقة وغيرها من العناصر الخاصة بأمن المعلومات في حال التخطيط لاستخدامها في معالجة البيانات المالية وغيرها من البيانات الهامة.

2-6 اتفاقيات سرية المعلومات

تقوم الإدارة بتحديد المتطلبات والشروط الخاصة بسرية المعلومات أو "اتفاقيات عدم الإفشاء" التي تعكس حاجة المجلس إلى حماية معلوماته المتعلقة بالممتلكات والمعلومات الشخصية، على أن يتم مراجعة تلك المتطلبات والشروط بصورة دورية.

2-7 العلاقات مع السلطات والجهات المختصة

يقوم رؤساء الأقسام المعنية بإقامة العلاقات والصلات الملائمة مع السلطات المختصة والحفاظ على تلك الصلات من خلال تنفيذ القوانين والجهات التنظيمية ومقدمي الخدمات المعلوماتية وشركات الاتصالات.

2-8 العلاقات مع الجماعات ذات المصالح الخاصة

يتم إقامة العلاقات والصلات الملائمة مع الجماعات ذات المصالح الخاصة وغيرها من المنتديات الخاصة بالأخصائيين الأمنيين والجمعيات المهنية.

2-9 المراجعة المستقلة لأمن المعلومات

تقوم لجنة أمن المعلومات بتخطيط والعمل على تنفيذ عملية تدقيق داخلي على حالة أمن المعلومات وفقاً للسياسات الأمنية، على أن تجرى عمليات التدقيق الداخلي بواسطة فريق تدقيق يتم تشكيله داخل المجلس أو بواسطة استشاريين خارجيين، كما تقرر اللجنة مدى تكرار عمليات التدقيق الداخلي بما يتلائم مع عملياتها ولكن بما لا يقل عن مرة واحد سنوياً.

يجب أن تجرى عمليات لتقييم دورية للمخاطر المتعلقة بأمن المعلومات ومراجعة لأدوات التحكم الأمنية المستخدمة بغرض ضمان معالجة سياسات أمن المعلومات بالمجلس لمتطلبات وأولويات ومخاطر والثغرات الأمنية المتعلقة بعمل المجلس بصورة كافية وفعالة.

2-10 تحديد المخاطر المتعلقة بالأطراف الخارجية

يجب اقتصار عملية الوصول إلى الأصول المعلوماتية الخاصة بالمجلس من قبل الأطراف الخارجية على المؤسسات والأشخاص المصرح بوصولهم لأغراض ضرورية تدعم عمل المجلس. ويجب ألا يتم السماح بوصول الأطراف الخارجية إلى شبكة المجلس أو أنظمته سواء عن بعد أو من داخل المجلس إلا في حالة حاجة العمل إلى ذلك:

- يجب الحصول على الموافقة المسبقة الصريحة من مسئول أمن المعلومات لوصول الأطراف الخارجية إلى الأصول عن بعد
- يجب مراجعة قائمة اتصالات الأطراف الخارجية لدى إدارة أمن المعلومات كل ستة أشهر بغرض التأكد من استمرار حاجة العمل لمثل هذا الاتصال.
- يجب إلغاء التصريح بالوصول عن بعد الممنوح للأطراف الخارجية فوراً بمجرد انتهاء علاقة العمل مع تلك الأطراف الخارجية أو انتهاء مدة الاتفاقيات/العقود أو إصدار مالك الأصول المعلوماتية أو أخصائي أول أمن المعلومات لقرار يقضي بإنهاء تلك الاتفاقات لأي سبب من الأسباب.
- يحق للمدير العام في أي وقت من الأوقات التوجيه نحو مراجعة قائمة الاتصالات المصرح بها لدى إدارة أمن المعلومات بغرض تأكيد وجود حاجة عملية مستمرة وإجراء الترتيبات اللازمة بشأنها، وذلك خلال فترة قصيرة يمكن أن تكون ثلاثة أيام عمل من وقت صدور ذلك التوجيه.

2-11 يجب مراعاة المتطلبات التالية عند إبرام الاتفاقيات مع الأطراف الخارجية (عندما ينطبق ذلك):

- الآثار المترتبة على الوضع الأمني ككل ويشمل ذلك المتطلبات والشروط القانونية والتعاقدية.
- المتطلبات والشروط المنطقية الخاصة بوصول المستخدم والمدير (انظر البند السابع "التحكم في الوصول")
- مدى حساسية المعلومات التي سوف تصل إليها الأطراف الخارجية
- عملية إدارة التغييرات التي سوف تستخدمها الأطراف الخارجية (انظر البند 6-2 "إدارة التغييرات")
- متطلبات وشروط الوصول المادي (انظر البند الخامس "الأمن المادي")

- المستوى المستهدف من الخدمة والأمن (انظر البند 6-28 "تقديم الخدمات" والبند 6-29 "الإشراف على خدمات الأطراف الخارجية ومراجعتها")
- تأثير الاتفاقية على المتطلبات الخاصة باستمرارية الخدمات (انظر البند العاشر "خطة استمرارية الأعمال")
- يجب تحديد المتطلبات والشروط الخاصة بسرية المعلومات وسلامتها وتوفرها وتضمينها قي العقد

2-12 الاتصالات والتواصل

يعمل مسئول أمن المعلومات مع مركز أبوظبي للأنظمة الإلكترونية والمعلومات بغرض إقامة وتقديم أنشطة اتصالات داخلية محددة تخص أمن المعلومات بهدف زيادة وعي الجمهور بالمجالات ذات الأهمية الحيوية والمتعلقة بأمن المعلومات. ومن بين تلك المجالات برنامج أمن المعلومات التابع لحكومة أبوظبي ومدى تقدم عملية تحقيق أهداف البرنامج الأمني. ويجب أن يعمل مسئول أمن المعلومات بالمجلس بالتعاون مع مركز أبوظبي للأنظمة الإلكترونية والمعلومات لتحديد المتطلبات والشروط الخاصة بالاتصال مع الأطراف الخارجية من خارج المجلس والتنسيق معها بغرض تسهيل الوفاء بمتطلبات الاتصالات مع هذه المجموعات.

2-13 إدارة الأداء

يعمل مسئول أمن المعلومات مع مركز أبوظبي للأنظمة الإلكترونية والمعلومات لتطوير مقاييس كمية لقياس مدى نجاح برنامج أمن المعلومات بالمجلس وجمع الدلائل التي تشير إلى أداء برنامج أمن المعلومات من الجهات المعنية والمستخدمين ومعالجة والإبلاغ بالنتائج الخاصة بهذه الدلائل.

القسم الثالث

إدارة الأصول

3. إدارة الأصول

إن الغرض من السياسات المنصوص عليها في هذا القسم هو ضمان حماية كافة المعلومات التي بحوزة المجلس بالصورة الملائمة ضد إساءة الاستخدام والأضرار وحمايتها من المخاطر المتعلقة بسوء التوزيع أو الإدارة.

3-1 جرد الأصول

يجب جرد كافة الأصول المعلوماتية بغض النظر عن درجة حساسيتها أو حيويتها مع تحديد مالك تلك الأصول.

3-2 ملكية أصول المعلومات

يتأكد ملاك البيانات من توفير الحماية الكافية للمعلومات التي بعدتهم ضد إساءة الاستخدام والأضرار.

3-3 تصنيف المعلومات

يتم تصنيف جميع المعلومات التي بحوزة المجلس بناء على درجة السرية، مع وضع وتطبيق أدوات التحكم الأمنية التي تشمل وضع المسميات والعناوين وفقاً لفئات تصنيف المعلومات بغرض ضمان توفير الحماية الكافية للمعلومات ضد إساءة الاستخدام والأضرار.

3-4 التعامل المتناغم مع المعلومات

يجب حماية المعلومات التي تؤتمن إلى المجلس ضد إساءة الاستخدام والأضرار بصورة تتناغم مع درجة حساسية وحيوية تلك المعلومات، ويجب اتخاذ الإجراءات الأمنية اللازمة بغض النظر عن نوع الوسائط التي تحفظ عليها المعلومات أو النظام الذي يعالجها أو وسيلة بثها، كما يجب توفير الحماية الكافية للمعلومات ضد إساءة الاستخدام والأضرار بغض النظر عن حالتها الحالية ضمن دورة الحياة التي تتراوح بين إنشاء المعلومات وتدميرها.

3-5 الاستخدام المقبول للأصول

يجب الالتزام بالقواعد التالية المتعلقة بالاستخدام المقبول للمعلومات والأصول المرتبطة بمرافق معالجة البيانات:

البريد الإلكتروني:

- يجب أن تحتوي الرسائل الإلكترونية الصادرة على بيان لإخلاء المسئولية
- استخدام البريد الإلكتروني في المعاملات الخاصة بالعمل أو الأغراض المتعلقة بالتعليم، وتعتبر مراسلات البريد الإلكتروني ملزمة قانوناً
- يمنع إنشاء أو إرسال رسائل غير مرغوب بها أو غير ذات علاقة أو غير ملائمة أو الرسائل التسلسلية
- يمنع فتح المرفقات المجهولة أو المشتبه بها أو الضغط على الروابط التي تتضمنها الرسائل الإلكترونية التي يرسلها مجهولون.
- جميع عناوين البريد الإلكتروني مملوكة للمجلس وتخضع لإشرافه
- إضافة عنوان البريد الإلكتروني الخاص بالمجلس إلى القوائم البريدية والمدونات والمنتديات وغيرها أو الاشتراك في مواقع الإنترنت غير ذات الصلة بالمجلس باستخدام ذلك العنوان
- يجب تشفير رسائل البريد الإلكتروني الصادرة

<u>شبكة الإنترنت</u>

- يمنع مشاهدة أو تنزيل المواد غير الملائمة (الصور المهينة أو الجنسية والنكات والتعليقات المهينة أو غيرها من التعليقات التي تعتبر مهينة لأي شخص بناء على إعاقتهم الجسدية أو العقلية أو العمر أو الدين أو الحالة الاجتماعية أو الميول الجنسي أو الآراء السياسية أو المعتقدات الدينية أو البلد الأصلي)
- يخضع استخدام شبكة الإنترنت لمراقبة إدارة تكنولوجيا المعلومات بالمجلس
- يمنع استخدام الإنترنت لمحاولة الدخول غير المصرح به إلى أجهزة الحاسب الآلي الأخرى أو المعلومات أو الخدمات
- يمنع تنزيل أو نسخ أية مواد محمية بموجب حقوق الطبع والنشر بما يشمل البرامج والكتب والمقالات والصور وغيرها من المواد غير المسموح للمجلس باستخدامها
- يمنع استخدام الإنترنت في الأغراض التي لا تتعلق بالتعليم وبالعمل
- يمنع القيام بأية أنشطة من شأنها إصابة شبكة المجلس بالفيروسات أو غيرها من البرامج المضرة

البريد الصوتي

- يجب ألا تتضمن الرسائل الصوتية التي يتركها الموظفون أية معلومات حساسة

- يجب أن يفحص مالك صندوق البريد الصوتي الرسائل الواردة بصورة دورية ومسح الرسائل التي تم الاستماع إليها بالفعل في أقرب وقت ممكن

سياسة الهاتف النقال

- يجب الإبلاغ عن أجهزة الهواتف النقالة فوراً في حال فقدها أو سرقتها
- يجب تشفير أجهزة الهواتف النقالة (بناء على درجة الحساسية)
- يجب تشغيل خاصية قفل الهاتف في حالة عدم الاستخدام
- يجب الالتزام بضبط الأوضاع وفقاً للسياسات الخاصة بكلمة المرور (انظر البند 7–4 "إدارة كلمات المرور الخاصة بالمستخدمين")
- يجب ضبط الأوضاع الخاصة بمواقيت وأقفال الهاتف بالصورة الملائمة

السياسة الخاصة بأجهزة الحواسب النقالة (Laptops)

- يمنع استخدام الحواسب النقالة دون جدار ناري (firewall) ("انظر البند 6–10 "أدوات التحكم بالشبكات")
- يجب تثبيت برامج مكافحة الفيروسات المحدثة على الأجهزة (انظر البند 6–7 "الحماية من الفيروسات")
- يجب الالتزام بضبط الأوضاع وفقاً للسياسات الخاصة بكلمة المرور (انظر البند 7–4 "إدارة كلمات المرور الخاصة بالمستخدمين")
- يجب تأمين وتثبيت الأجهزة طوال الوقت (المطارات والسيارات والمنازل والمكاتب وغيرها ... انظر البند 5 "الحماية المادية والبيئية")
- يجب الاحتفاظ بنسخة احتياطية للمواد المحفوظة على الأجهزة بصورة دورية (انظر البند 6–9 "النسخ الاحتياطية من المعلومات")
- يجب تشفير المعلومات المحفوظة على الأجهزة طوال الوقت (انظر البند 7–24 "الحواسب والاتصالات النقالة")
- يمنع تغيير الأوضاع الأمنية (المنفذ والجدار الناري وغيرها)
- يجب ضبط الأوضاع الخاصة بمواقيت وأقفال الهاتف بالصورة الملائمة

السياسة الخاصة بالمعلومات المعلنة للجمهور

- يراعى حماية سلامة المعلومات المنشورة إلكترونياً للجمهور (على سبيل المثال المعلومات المنشورة على الموقع الإلكتروني الخارجي للمجلس)، ويجب الحصول على تصريح رسمي قبل نشر أية معلومات للجمهور بغرض ضمان دقة تلك المعلومات وتماشيها مع معايير الجودة المتبعة.

القسم الرابع

مسؤولية موظفي المجلس

4. مسؤولية موظفي المجلس

إن الغرض من السياسات المنصوص عليها في هذا القسم هو بيان مسئولية المجلس في ضمان توفير الحماية الكافية لأصوله المعلوماتية ضد إساءة الاستخدام والضرر فيما يخص جميع المرشحين للعمل والمستخدمين الحاليين، كما أن هذه السياسات تتضمن المتطلبات الخاصة بالتدريب المتعلق برفع الوعي بأمن المعلومات ومسئوليات المستخدمين.

4-1 الأدوار والمسئوليات الأمنية

يقوم مدير الموارد البشرية، بالتشاور مع مديري الإدارات وهيئات التدريس، بتحديد المسئوليات الأمنية الخاصة بالموظفين/المجموعات وفقاً لتصنيفات التحكم في الدخول والنص صراحة على تلك المسئوليات في التوصيف الوظيفي للموظف وبيان المسئولية، ويشمل ذلك أية مسئوليات عامة تخص تطبيق أو مواصلة تطبيق السياسة الأمنية والمسئوليات والحقوق القانونية علاوة على أية مسئوليات خاصة محددة تتعلق بحماية أصول معينة. انظر دليل سياسات وإجراءات الموارد البشرية.

4-2 التحريات الأمنية

يجب توفير الحماية الكافية للأصول المعلوماتية الخاصة بالمجلس ضد إساءة الاستخدام والأضرار خلال عملية استقطاب وتوظيف العاملين الجدد، وذلك عن طريق جمع التحريات الكافية عن المرشحين للعمل، كما يجب تضمين المسئوليات المتعلقة بأمن المعلومات في بنود وشروط التوظيف وتقديمها إلى جميع المرشحين للعمل. انظر عملية التحريات الخاصة بشرطة أبوظبي.

4-3 بنود وشروط التوظيف

يتعين أن تنص بنود وشروط التوظيف التي تتضمنها عقود التوظيف صراحة، أو غيرها من العقود المشابهة، بوضوح على التزام الموظف بإتباع السياسات الخاصة بأمن معلومات المجلس، وذلك بالتوقيع الدال على فهمهم وموافقتهم الصريحة على بنود وشروط التوظيف قبل السماح لهم بالوصول إلى الأصول المعلوماتية للمجلس.

4-4 مسئوليات الإدارة

يحرص المديرون، من خلال عملية الاستقطاب والتوظيف، على التأكد من كون الموظفين:

- يتمتعون بالدوافع اللازمة للالتزام بالمسئوليات الموكلة إليهم وذلك من خلال الإشراف المتواصل والتشجيع والتحفيز من جانب الإدارة.
- المحافظة على قدراتهم ومهاراتهم ومؤهلاتهم الخاصة بأمن المعلومات من خلال زيادة الوعي والتثقيف والتدريب (انظر البند 4-5 "زيادة الوعي بأمن المعلومات والتدريب والتثقيف").

4-5 زيادة الوعي بأمن المعلومات والتدريب والتثقيف

يتلقى جميع المستخدمين القادرين على الوصول للأصول المعلوماتية الخاصة بالمجلس القدر الملائم من المعلومات والتدريب بغرض ضمان فهمهم لسياسات أمن المعلومات بالمجلس بصورة كاملة.

4-6 الإجراءات التأديبية

في حال عدم الالتزام بسياسة أمن المعلومات يخضع غير الملتزمين لإجراءات تبدأ من اللوم والتحذير وقد تصل إلى الإجراءات التأديبية التي تمتد إلى إنهاء الخدمة.

4-7 المسئوليات الخاصة بإنهاء الخدمة

يشرف مدير الموارد البشرية على تضمين الفقرات والإجراءات الملائمة المتعلقة بأمن المعلومات في إجراءات تغيير الوظيفة/إنهاء الخدمات بالنسبة لجميع موظفي المجلس، على أن يراعي المدير أيضاً اتخاذ الإجراءات الملائمة في الوقت المناسب لضمان عدم الإخلال بالضوابط الداخلية والأمنية في تلك الحالات. انظر قائمة إنهاء الخدمات الخاصة بإدارة الموارد البشرية.

4-8 إعادة الأصول

يلتزم جميع المستخدمين سواء من الموظفين أو المتعهدين أو الأطراف الخارجية بإعادة جميع الأصول المحفوظة بعهدتهم والتي تخص المجلس عند إنهاء خدماتهم أو فسخ عقدهم أو الاتفاق المبرم معهم.

4-9 يتم إلغاء حقوق جميع المستخدمين سواء من الموظفين أو المتعهدين أو الأطراف الخارجية في الوصول إلى المعلومات ومرافق معالجة المعلومات في حال إنهاء خدماتهم أو عقدهم أو الاتفاق المبرم معهم، أو يتم تعديل تلك الحقوق في حال حدوث تغيير.

القسم الخامس

الأمن المادي والبيئي

5. الأمن المادي والبيئي

إن الغرض من السياسات المنصوص عليها في هذا القسم هو بيان الأمن المادي والبيئي المطلوب المحافظة عليه بغرض حماية مرافق وأنظمة وأجهزة وسجلات معالجة البيانات الخاصة بالمجلس.

5-1 حدود الأمن المادي

يجب وضع وتطبيق أدوات التحكم اللازمة للحد من المخاطر الأمنية المادية والتي تشمل:

- التحديد الواضح للنطاقات الأمنية (على سبيل المثال " غرف الحاسبات الآلية") مع عزلها عن طريق حدود أمنية فعالة مزودة بنقاط دخول/خروج تخضع لسيطرة المختصين.
- جدران قوية محيطة بالمكان وأبواب تخضع لسيطرة المختصين.
- تخصيص أقسام استقبال يديرها موظفون مختصون إضافة إلى غيرها من الوسائل اللازمة لقصر الدخول إلى الموقع/المبنى على الموظفين فقط والموافقة على دخول الزوار بعد استخدام وسائل تحديد الهوية.

5-2 أدوات التحكم بدخول الأشخاص

يتم توفير الحماية الكافية للأماكن المخصصة لحفظ الأصول المعلوماتية الهامة عن طريق أدوات التحكم في دخول الأشخاص لضمان عدم دخول أي أشخاص سوى الأشخاص المصرح لهم بالدخول.

- يتم السماح لموظفي الأطراف الخارجية وغيرهم من الزوار بالدخول المقيد بضوابط إلى الأماكن المحظورة وذلك في حالة الضرورة فقط (على سبيل المثال: لأغراض الصيانة ودعم) وعلى أن يكون ذلك بموجب تصريح من الإدارة وتحت إشراف الموظفين المختصين الذين يتعين عليهم تسجيل مواعيد وأوقات الدخول والخروج في سجل الزيارات المؤمنة.
- يمكن إضافة مزيد من حدود وحواجز التحكم في الدخول بين المناطق التي تحظى بمتطلبات أمنية مختلفة داخل الحد الأمني الواحد (على سبيل المثال: استخدام صناديق/حجيرات مقفلة للمعدات بغرض الحيلولة دون وصول أي شخص غير مصرح له إلى المعدات والأجهزة الخاصة بالمجلس في المواقع المشتركة).
- يتعين على الموظفين والزوار إظهار بطاقة التعريف الشخصية طوال الوقت أثناء تواجدهم بالموقع. ويقوم الموظفون وحراس الأمن – بأدب وحزم– باعتراض والتحقق من هوية الزوار غير الخاضعين للإشراف/غير المرافقين أو الأشخاص الذين لا يبرزون هويتهم بوضوح.

- تتم مراجعة حقوق الدخول إلى المناطق المحظورة بصفة دورية وفي حالة الضرورة تحديثها بواسطة الإدارة (على سبيل المثال لمنع دخول الموظفين السابقين).

5-3 المكاتب والغرف والمرافق المحظورة

- تخضع المكاتب والغرف والمرافق المعينة للحماية اللازمة بواسطة أدوات التحكم:
- يتم إغلاق جميع المكاتب في حال عدم وجود المختصين بداخلها وخاصة الأبواب والنوافذ الخاصة بالمناطق المحظورة
- يتم تصميم وتركيب واختبار وصيانة أدوات كشف المتسللين الملائمة (كأنظمة أجهزة الإنذار جهاز رصد الحركة و/أو كاميرات المراقبة التليفزيونية
- يمنع استخدام مرافق المجلس سوى في الأنشطة المتعلقة بالعمل ما لم تصدر موافقة صريحة من الإدارة.

يتعين على المختصين بأمن الموقع، بالتعاون مع المختصين بأمن المرافق والمعلومات، القيام بما يلي:

- تسيير دوريات حراسة داخل المرافق (وخاصة خارج أوقات العمل الرسمية)
- التحقق من عمل إجراءات الأمن بصورة سليمة
- متابعة كاميرات المراقبة التليفزيونية وأجهزة الإنذار ورصد المتسللين والاستجابة الفورية للأعطال
- التحديد والتعامل الفوري مع المسائل/المخاطر الفعلية أو المحتملة المتعلقة بالأمن المادي كالمتسللين والعلامات التي تدل على تسرب المياه وارتفاع درجة الحرارة وغيرها
- التنسيق مع الإدارة بشأن الحوادث والمسائل والمخاطر

5-4 الحماية من التهديدات الخارجية والبيئية

تشمل أدوات التحكم في التهديدات البيئية ما يلي:

- حفظ الوثائق ذات الأهمية الحيوية في خزائن مقاومة للحرائق
- تصميم وتركيب وصيانة أجهزة إطفاء الحرائق في غرف الحاسبات الآلية بصورة احترافية
- استخدام أجهزة إطفاء الحرائق اليدوية من النوع الملائم لإطفاء الحرائق الكهربائية مع الاحتفاظ بها بالقرب من مخارج الطوارئ المناسبة بحيث يمكن للشخص الذي يقاوم الحرائق الوصول للمخرج. ويجب صيانة مخارج الطوارئ وفقاً للممارسات المهنية واختبارها بانتظام حتى لو كانت تقع في المناطق المحظورة.
- تدريب موظفي غرف الحاسبات الآلية بصورة سليمة على إجراءات التعامل مع الحرائق ومن بينها الاستجابة للإنذارات وإخلاء المبنى بأمان ومكافحة الحرائق الصغيرة.

- الاحتفاظ بالمواد الخطرة أو القابلة للاشتعال مثل الصناديق الكرتونية والأغلفة البلاستيكية والمذيبات بصورة أمنة في مكان يبعد مسافة أمنة من غرف الحاسبات.
- الاحتفاظ بأجهزة النظام الاحتياطي (Fallback) ووسائل حفظ النسخ الاحتياطية (Backup) بعيداً عن الموقع الأساسي
- حظر الأكل والشرب والتدخين في المناطق المحظورة وفي غيرها من الأماكن القريبة من الأصول المعلوماتية الهامة
- مراقبة والتحكم في الظروف البيئية (كالحرارة والرطوبة ووحدة الإمداد بالطاقة) في المواقف التي يمكنها خلق أثار عكسية أثناء تشغيل المرافق التكنولوجية

5-5 العمل في المناطق المحظورة (Secure Areas)

يتم وضع وتطبيق إجراءات وإرشادات الحماية المادية الخاصة بالعمل في المناطق المحظورة، على أن يتم إغلاق المناطق المحظورة الخالية وتفتيشها بصورة دورية بواسطة حراس الأمن/الموظفين.

6-5 الأجهزة والمعدات الحساسة

يجب الاحتفاظ بالأجهزة والمعدات الحساسة في مكان من شأنه تقييد وصول الجمهور إليها.

7-5 مرافق الدعم

يجب حماية الأجهزة والمعدات من انقطاع التيار الكهربائي عنها وعن مرافق الدعم:

- حماية الأجهزة والمعدات التكنولوجية من انقطاع التيار الكهربائي والارتفاع المفاجئ في التيار الكهربائي وانخفاض الفولتية والتداخل الكهربائي وغيرها من المشاكل المشابهة حسب الحال
- تزويد الأجهزة والمعدات التي تؤدي أو تساند الخدمات الحيوية بأجهزة التيار المتواصل (UPS) مع فحص واختبار تلك الأجهزة وبطارياتها وفقاً لتعليمات المصنع.
- وضع مفاتيح "فصل التيار في حالات الطوارئ" المغلقة بالقرب من مخارج الطوارئ بغرف الأجهزة والمعدات بغرض تسهيل فصل التيار بسرعة في حالة الطوارئ
- مراقبة مرافق الدعم بالصورة الكافية والإنذار في حالة الأعطال (من خلال أجهزة إنذار موضعية مقروءة عن بعد) وخاضعة للمراقبة على مدار الساعة، مع إبداء الاستجابة المناسبة وتطبيق الإجراءات المتبعة في حالة الحوادث

5-8 أمن الوصلات (الكابلات والأسلاك)

يجب حماية كابلات وأسلاك الطاقة والاتصالات التي تغذي المرافق التكنولوجية ضد الاعتراض والتلف، على أن يتم توصيلها من تحت الأرض كلما أتيح ذلك أو حمايتها بواسطة كابلات مصفحة أو أنابيب، ويتعين تحديد مساراتها بصورة ملائمة بحيث تتجنب المناطق عالية الخطورة مثل الأركان القريبة من مسارات المرور، كما يجب قدر الإمكان فصل كابلات وأسلاك الطاقة عن كابلات وأسلاك الاتصالات للحد من التداخل بينهما.

يجب حماية نقاط فحص وإنهاء الكابلات والأسلاك (ومن بينها حزم الكابلات patching racks) ضد الوصول غير المصرح به عن طريق استخدام غرف أو صناديق أو حجيرات مغلقة على سبيل المثال.

5-9 صيانة الأجهزة والمعدات

يجب صيانة الأجهزة والمعدات بصورة سليمة حسب فترات الخدمة والمواصفات المقترحة من جانب المتعهد لضمان توفرها وسلامتها بصورة متواصلة، ولا يسمح سوى لموظفي الصيانة المصرح لهم بالقيام بالإصلاحات وأعمال صيانة الأجهزة والمعدات، على أن يتم الاحتفاظ بسجلات ملائمة، على سبيل المثال سجل لأعمال الصيانة، تضم كافة الأعطال سواء المشكوك فيها أو الفعلية وأعمال الصيانة الوقائية والإصلاحية التي أجريت.

5-10 أمن الأجهزة والمعدات خارج المبنى

لا يجوز ترك الأجهزة أو المعدات في الأماكن العامة دون حراسة ويجب حمل أجهزة الـ لابتوب بعناية في الحقائب المخصصة لذلك الغرض عند السفر.

5-11 التخلص الآمن من الأجهزة والمعدات أو إعادة استخدامها

يجب تدمير أجهزة التخزين التي تحتوي على معلومات حساسة أو الكتابة فوقها عن طريق البرامج والإجراءات المعتمدة، ويجب فحص أجزاء الأجهزة التي تحتوي على وسائط التخزين، كالأقراص الصلبة (HARD DISK)، قبل التخلص منها للتأكد من مسح أو الكتابة فوق أية معلومات حساسة.

5-12 عدم نقل الأصول (الأجهزة والمعدات)

لا يجوز نقل الأجهزة التكنولوجية أو المعلومات أو البرامج من موقعها دون الحصول على موافقة مسبقة من الإدارة. انظر نموذج تسجيل نقل/خروج الأصول.

القسم السادس

إدارة الاتصالات والعمليات

6. إدارة الاتصالات والعمليات

إن الغرض من السياسات المنصوص عليها في هذا القسم هو بيان المتطلبات والشروط اللازمة لضمان البث والتخزين الآمن للأصول المعلوماتية الخاصة بالمجلس.

6-1 إجراءات التشغيل الموثقة

يتم وضع وتطبيق إجراءات التشغيل بكافة مرافق المجلس، مع تحديد مسئوليات الدعم الإداري والتشغيلي بوضوح.

6-2 إدارة التغييرات

يجب أن تلتزم كافة التغييرات بإجراءات إدارة التغييرات ذات الصلة:

- لا يتم تطبيق التغييرات سوى بعد الموافقة الرسمية من جانب مالك النظام أو التطبيق أو الوثيقة وغيرها (أو من ينوبه)
- يجب إبلاغ الموظفين المختصين بتفاصيل تلك التغييرات قبل تطبيقها حتى يمكنهم القيام بالمراجعات اللازمة
- يجب تقييد التغييرات والتعديلات على حزم البرامج التي يوردها المتعهدين بمقتضيات العمل
- يجب توثيق الإجراءات والمسئوليات فيما يخص الإلغاء و/أو الاستعادة بعد التغييرات غير الناجحة
- يجب الاحتفاظ بسجل لمستويات التفويض (من من حقه تفويض ماذا)
- يجب الاحتفاظ بسجل للتدقيق على كافة طلبات التغييرات

6-3 الفصل بين المهام والواجبات

يجب الفصل بين مسئوليات إدارة مهام وواجبات الأعمال من جهة والتنفيذ من جهة أخرى بغرض التحقق من وجود نظام تدقيق داخلي فعال والحد من المخاطر الناجمة عن إساءة استخدام النظام بعمد أو دون عمد، على أن تقع مسئولية تحقيق ذلك الفصل على رؤساء الأقسام المعنية بالتطبيق والتشغيل، ومن بين المجالات الحيوية التي تحتاج إلى الفصل بين المهام تحديث الملفات الرئيسية (Master Files) والملفات القياسية (Parameter Files) واعتماد وتسجيل الدفعات المالية ومجالات معينة بالأنظمة المالية وإدارة النظم والتدقيق الأمني إضافة إلى تطوير وصيانة الأنظمة.

6-4 الفصل بين التطوير والاختبار والمرافق التشغيلية

يجب الفصل بين بيئات التطوير والاختبار على الأقل من الناحية المنطقية لضمان النزاهة:

- يمنع كتابة أسماء المستخدمين المتعلقة بالمختصين بالتطوير والاختبار على أنظمة الإنتاج (ما عدا أسماء المستخدمين الخاصة بالمكالمات الطارئة والتي يجوز تفعيلها لاستخدام موظفي الدعم التكنولوجي المصرح لهم لأغراض معينة تخص الدعم في خلال عمليات التغيير الطارئة وفقاً لإجراءات التحكم في التغييرات)
- تتاح بيانات الإنتاج على أنظمة الإنتاج فقط، ويجب استخدام بيانات وهمية في عمليات التطوير والاختبار قدر الإمكان، وفي حال ضرورة استخدام بيانات شديدة الحساسية فيجب إخفائها أولاً (كأرقام بطاقات الائتمان والبيانات الشخصية)
- يجب أن تبين الرسائل التي تظهر على الشاشة وألوان الشاشة وغيرها بوضوح إذا كان النظام قيد الإنتاج أو الاختبار للحد من المخاطر التي يمكن أن تنتج من إدخال معاملات اختبار عن طريق الخطأ إلى أنظمة الإنتاج

6-5 الخطط الخاصة بالطاقة الاستيعابية

يجب وضع وإعداد خطط مسبقة لضمان توفر الطاقة الاستيعابية والموارد الكافية، مع مراعاة وضع متطلبات الطاقة الاستيعابية المستقبلية بصفة سنوية.

6-6 اعتماد النظام

يتعين إجراء اختبارات القبول المناسبة على أجهزة المعلومات "الجديدة" (ويشمل ذلك النسخ المحدثة والأنظمة الجديدة تماماً) قبل استخدامها في إنتاج المعلومات. ويجب أن يتأكد المديرون من تحديد متطلبات ومعايير اعتماد الأنظمة الجديدة بوضوح والموافقة عليها وتوثيقها واختبارها مع مراعاة ما يلي:

- التشاور مع قسم أمن المعلومات في جميع مراحل عملية التطوير للتأكد من مراعاة أدوات التحكم الأمنية المطلوبة في تصميم النظام المقترح
- التشاور مع جهات العمل ذات الصلة في جميع مراحل عملية التطوير للتأكد من الكفاءة التشغيلية لتصميم النظام المقترح
- متطلبات الأداء والمتطلبات والشروط المتعلقة بسعة الحاسب الآلي
- إجراءات إصلاح المشاكل (Error Recovery) وإعادة التشغيل وخطط الطوارئ
- إعداد واختبار إجراءات التشغيل الروتينية بغرض وضع المعايير ذات الصلة

- التحقق من عدم تأثير تثبيت الأنظمة الجديدة بالسلب على الأنظمة القائمة بالفعل أو غيرها من المرافق وخاصة في أوقات ذروة المعالجة
- اعتماد الإدارة لكافة الأدلة والمواد المقدمة إلى المستخدم النهائي أثناء استخدام أو تحديث البرامج
- توفير دليل تشغيل يغطي إجراءات التشغيل والإنهاء والاستعادة قبل طرح الأنظمة الجديدة
- الحصول على الموافقة المحددة وإتباع إجراءات التسليم (Sign off) قبل تطوير البرامج أو تعديلها على أي جهاز متعدد المستخدمين
- تقديم أي جهاز جديد أو أي تحديث للتطبيقات الحالية إلى المستخدمين من خلال دليل للمستخدمين
- حصول المستخدمين على التدريب المناسب كاملاً قبل استخدام تطبيقات العمل الجديدة أو النسخ الجديدة من التطبيقات الحالية
- مراجعة البرامج الجديدة إضافة إلى الأجزاء الجديدة من كود المصدر (كالاستعلامات والإجراءات الخاصة بلغة الاستعلامات البنائية) قبل الاستخدام كلما أمكن ذلك

7-6 الحماية من الفيروسات ومكافحتها

تقوم إدارة تكنولوجيا المعلومات بتنصيب البرامج المعتمدة لمكافحة الفيروسات وتهيئتها للعمل على جميع الأجهزة التكنولوجية المستخدمة بغرض توفير أعلى درجات الحماية، كما تقوم إدارة تكنولوجيا المعلومات بتحديث تلك البرامج فوراً في حال إطلاق التواقيع الفيروسية الجديدة (malware signatures) أو غيرها:

- لا يجوز للموظفين الآخرين غير المختصين بتغيير أو التدخل في عمل البرامج المكافحة للفيروسات أو تهيئتها أو عملية تحديثها أو تشغيلها
- يجب فحص رسائل البريد الإلكتروني ومرفقاتها بصورة دورية وتلقائياً قبل الاستخدام تحسباً لإصابتها بالبرامج الضارة
- لا يجوز تثبيت أية برامج غير مصرح بها على أنظمة المجلس، على أن تقوم إدارة تكنولوجيا المعلومات بمراجعة واعتماد البرامج، ولابد قبل قيام أي موظف مختص بتثبيت البرامج المعتمدة الحصول على موافقة صريحة من المدير الخاص بذلك الموظف، وينطبق ذلك أيضاً على كافة أشكال البرامج كالبرامج التجارية (commercial software) وبرامج تشغيل الأنظمة والمرافق وبرامج المشاركة (shareware) والبرامج المجانية (freeware) وبرامج التقييم (evaluation software).
- يقوم مسئول أمن المعلومات بمتابعة وتقييم تهديدات البرامج الضارة باستخدام الموارد الموثوق بها كالمواقع الإلكترونية الموثوق بها والدوريات المتخصصة والتوعية بالمعلومات المفيدة ونشرها وتقديم المشورة داخل المجلس.

6-8 أدوات التحكم في الشفرة/الأكواد المتنقلة

يجب تقييم المخاطر المتعلقة بأمن المعلومات والمرتبطة أو ذات الصلة بالشفرة/الأكواد المتنقلة، ويتعين الحد منها – في حال إمكان ذلك– من خلال أدوات التحكم مثل:

- منع الشفرات/الأكواد المتنقلة غير المصرح بها من التنزيل و/التنفيذ (على سبيل المثال عن طريق ضبط أوضاع أمن المتصفح بالصورة المناسبة.
- قصر تنفيذ الشفرات/الأكواد المتنقلة الشرعية على البيئات المعزولة منطقياً (كـ JavaScript)

6-9 النسخ الاحتياطية من المعلومات

يجب عمل نسخ احتياطية من المعلومات والبرامج الأساسية المتعلقة العمل بصورة دورية وبالقدر الذي يسمح باستعادة تلك المعلومات والبرامج بكفاءة في حال حدوث كارثة أو عطل بأحد الوسائط التي من شأنها التأثير على البيانات أو الأنظمة الرئيسية:

- يجب وضع جدول زمني خاص بعمل النسخ الاحتياطية يصمم ويوثق خصيصاً لكل نظام من الأنظمة بغرض الوفاء بمتطلبات العمل الشرعية أو القانونية أو التنظيمية المتعلقة بحفظ واستعادة البيانات؛
- يجب عمل الأنواع المناسبة من النسخ الاحتياطية (على سبيل المثال "نسخة احتياطية عبارة عن صورة" كاملة أسبوعياً إضافة إلى نسخ احتياطية أخرى يومية تمثل الفارق أو الإضافة إلى النسخة الأسبوعية)
- يجب أن يتم حفظ النسخ الاحتياطية إلكترونياً كلما أمكن ذلك
- يجب اختبار أجهزة ووسائط وعمليات صنع النسخ الاحتياطية بصورة دورية في الإنتاج لضمان إمكانية الاعتماد عليها
- يجب أن تحفظ النسخ الاحتياطية الخارجية مع السجلات الدقيقة والكاملة للنسخ الاحتياطية وإجراءات الاستعادة الموثقة في موقع بعيد
- يجب تشفير النسخ الاحتياطية والأرشيف تلقائياً عند جدوى وملائمة ذلك من الناحية الفنية
- يجب صنع نسخ احتياطية دائماً قبل إجراء أية تغييرات رئيسية

6-10 أدوات التحكم بالشبكات

يتم إدارة الشبكات والتحكم بها بالصورة الكافية بغرض الحماية من التهديدات والحفاظ على أمن الأنظمة والتطبيقات باستخدام الشبكات ومن بينها المعلومات أثناء نقلها.

- يجب الفصل بين مسئوليات إدارة وتأمين شبكات وأجهزة حاسبات المجلس بين وظائف تشغيل الشبكات وتشغيل الحاسبات، على أن يتم التنسيق بين أنشطة إدارة الشبكات وأجهزة الحاسب للحد من المخاطر داخل بيئة العمل وضمان تطبيق أدوات التحكم الأمنية بصورة متناغمة في جميع مكونات البنية التحتية التكنولوجية.
- يجب أن تحقق أدوات التحكم التشفيرية (cryptographic control) السرية والسلامة وعدم إنكار الرسائل التي تحتوي على بيانات معاملات العمل التي تتسم بالحساسية أو الأهمية.
- يجب أن يكون لحدود الشبكة أو النطاقات الداخلية المنفصلة – إذا تطلب الأمر– جدران نارية (firewalls) بغرض مراقبة والتحكم في استخدام والوصول إلى الشبكات والأنظمة المتصلة بها.
- يجب أن يراعى في تصميم وإدارة الشبكات تحقيق مستوى من التوفر والسعة والأداء معادل لأنظمة الحاسب المتصلة وكافي لتلبية متطلبات العمل المشروعة

6-11 أمن خدمات الشبكات

يتم تحديد وشمول الخصائص الأمنية ومستويات الخدمة ومتطلبات إدارة كافة خدمات الشركات (كتوفير التوصيلات وخدمات الشبكات الخاصة وشبكات القيمة المضافة والحلول الأمنية الخاصة بالخدمات المدارة كالجدران النارية وأنظمة رصد التسلل) في اتفاقيات الخدمات المتعلقة بالشبكات.

6-12 إدارة الوسائط القابلة للإزالة (Removable media)

يجب توثيق وإتباع الإجراءات الخاصة بالتحكم في الوسائط القابلة للإزالة والتعامل معها تخزينها وأمنها (كشرائط النسخ الاحتياطية والأقراص والأقراص المدمجة وأقراص الـDVD و Flash RAM والمواد المطبوعة):

- يجب الحصول على تصريح قبل إزالة الوسائط من المناطق الخاضعة للتحكم أو أخذها خارج الموقع
- يجب تخزين الوسائط التي تحمل النسخ الاحتياطية في المواقع الخارجية كالبنوك مثلاً

- في حال الحاجة إلى حفظ المعلومات بما يتجاوز العمر الافتراضي للوسائط، يجب إعادة التحقق منها ونقلها إلى وسائط جديدة بصفة دورية لتجنب تلف البيانات أو فقدها، ويجب حفظ المعلومات الحيوية المتضمنة في الأرشيف بنسخ متعددة منفصلة عن بعضها البعض (ويفضل أن يكون ذلك على وسائط مختلفة) للحد من الخسائر.

6-13 التخلص من الوسائط

يجب التخلص من وسائط التخزين (وهي تشمل الوثائق والتقارير الورقية وقوائم البرامج (program listings) ووثائق الأنظمة والأشرطة المغناطيسية والأقراص أو الأشرطة ووسائط التخزين الضوئية) بصورة أمنة عن طريق الكتابة فوقها لمرات عديدة بما يتوافق مع معايير وزارة الدفاع الأمريكية المنصوص عليها في دليل برنامج الأمن الصناعي الوطني أو تمزيق و/أو حرق تلك الوسائط بناء على درجة حساسية وتصنيف البيانات التي تحملها.

يجب حماية الحاويات الورقية وأرفف التخزين وحوامل الأشرطة وغيرها من الأدوات، التي تحمل الوسائط المقرر التخلص منها بصورة أمنة، من السرقة أو الاستخدام غير المصرح به وفقاً لمستوى المخاطرة.

6-14 إجراءات التعامل مع المعلومات

يجب وضع وإعداد الإجراءات الخاصة بالتعامل مع البيانات السرية وتخزينها بغرض حماية تلك المعلومات من الإفشاء غير المصرح به أو إساءة الاستخدام وذلك وفقاً لتصنيف المعلومات (انظر البند 3-3 "تصنيف المعلومات").

تنطبق إجراءات التعامل مع المعلومات على كافة أشكال المعلومات كبيانات الحاسب والوثائق وأنظمة الحاسب والشبكات والحاسبات والاتصالات النقالة والبريد الإلكتروني والخدمات البريدية والبريد الصوتي والاتصالات الصوتية والوسائط المتعددة وأجهزة الفاكس علاوة على وثائق مثل الشيكات والفواتير الخاصة بالمجلس.

6-15 أمن وثائق النظام

يجب تصنيف وثائق توصيف الأنظمة والشبكات وتصاميم التطبيقات والمقاييس الأمنية وعمليات التشغيل والإدارة وهياكل البيانات وعمليات إصدار تصاريح المستخدمين وغيرها حسب نظام التصنيف المتبع في المجلس وحمايتها من الدخول غير المصرح به.

يتم توفير الحماية الكافية لوثائق النظام الموجودة على شبكة الإنترانيت (Intranet) والتي يمكن وصول الموظفين إليها.

6-16 سياسات وإجراءات تبادل المعلومات

يجب حماية المعلومات المتبادلة بصورة ملائمة ضد اعتراضها ونسخها وتعديلها وتغيير مسارها وتدميرها من قبل الأطراف الخارجية وذلك وفقاً لمستوى التصنيف والمخاطر.

- يجب استخدام مرافق الاتصالات الإلكترونية وفقاً للتعليمات والإجراءات المعمول بها وسياسات الاستخدام المقبولة (انظر البند 3-5 "الاستخدام المقبول للأصول")
- يجب استخدام أساليب التشفير الملائمة بغرض حماية سرية وسلامة ومصداقية المعلومات وفقاً لسياسات تصنيف المعلومات (انظر البند 3-3 "تصنيف المعلومات").
- لا يجوز للعاملين إعطاء بياناتهم الشخصية كعناوين البريد الإلكتروني إلى الأطراف الخارجية ما لم يكن هناك سبب مشروع لذلك واعتبار الأطراف الخارجية جديرة بالثقة.

6-17 اتفاقيات تبادل المعلومات

يجب أن يحكم عملية تبادل المعلومات والبرامج بين المجلس وغيره من المؤسسات اتفاقيات تعكس درجة حساسية وقيمة المعلومات المتبادلة وتنص على أدوات التحكم اللازمة مثل:

- الفقرات الخاصة بالسرية والمسئولية القانونية في الاتفاقيات التعاقدية بغرض الحد من الآثار المترتبة على المجلس في حال حدوث إخفاقات أمنية بالأطراف الأخرى.
- اتخاذ الترتيبات المتعلقة بالضمان (Escrow arrangements) على سبيل المثال لتأمين كود المصدر في حالة إفلاس متعهدي البرامج أو فقدان الموظفين الرئيسيين أو عدم قدرة المتعهدين على تقديم المستوى اللازم من الدعم لأي سبب أخر.
- ملكية المعلومات والبرامج والمسئوليات المتعلقة بحماية البيانات والالتزام بحقوق الطبع والنشر والاعتبارات الأخرى المشابهة.

6-18 الوسائط المادية أثناء النقل

يجب مراعاة النقل الأمن لوسائط الحاسب الآلي بين مواقع المجلس والمواقع الخارجية:

- استخدام وسائل أو شركات توصيل طرود بريدية موثوق بها، مع وضع قائمة بشركات التوصيل تلك بالاتفاق مع الإدارة إضافة إلى وضع وإتباع إجراءات لتحديد والتعرف على الطرود المرسلة.

- تغليف الوسائط بالصورة الكافية لحماية محتوياتها من أي ضرر في مكوناتها المادية قد ينجم أثناء عملية النقل وذلك وفقاً لمواصفات المصنع (على سبيل المثال: حاويات مقفلة ومحكمة معدة خصيصًا لهذا الغرض).
- إتباع أدوات تحكم خاصة عند الضرورة لضمان حماية الوسائط التي تحتوي على معلومات سرية أو غيرها من المعلومات ذات الحساسية أو الأهمية الكبيرة (وذلك حسب نظام تصنيف البيانات الموضح في القسم 3-3) من الإفشاء أو التعديل غير المصرح به (على سبيل المثل من خلال التشفير أو الحاويات المقفلة أو التسليم باليد أو أساليب التغليف التي تكشف فتح الحاويات أو تقسيم الوسائط المرسلة إلى عدة أجزاء وإرسال كل منها بطريقة مختلفة).

6-19 الرسائل الإلكترونية

يجب حماية المعلومات الحساسة التي تحتويها رسائل البريد الإلكتروني بالطرق الملائمة وفقاً لمخاطر أمن المعلومات ذات الصلة وتصنيفها (على سبيل المثال: عن طريق تشفير الرسائل ورسائل البريد الإلكتروني الحساسة). .

6-20 أنظمة معلومات العمل

يجب أن يؤخذ أمن المعلومات في الاعتبار عند وضع وتطبيق أنظمة معلومات العمل الداخلية كالأنظمة الإدارية والمحاسبية على سبيل المثال.

يتعين معالجة نقاط الضعف الأمنية الواضحة/الضمنية الموجودة في الأنظمة من خلال أدوات التحكم التعويضية المناسبة مع تحديد الأشخاص الذين يسمح لهم بالوصول إلى تلك الأنظمة، ولا يجوز نقل المعلومات السرية إلا من خلال أساليب التشفير الآمنة. ويراعى إنشاء نسخة احتياطية من الأنظمة والبيانات بصورة منتظمة (انظر القسم 6-9 "النسخ الاحتياطية من المعلومات") مع اتخاذ الإجراءات اللازمة الخاصة بالاستعادة بعد الكوارث (disaster recovery) والرجوعية (resilience) (انظر القسم 6-9 "إدارة استمرارية العمل".

6-21 المعلومات المعلنة

يجب حماية سلامة المعلومات المعلنة على المواقع الإلكترونية والوسائط المكتوبة المتعلقة بها وغيرها باستخدام أدوات التحكم في أمن المعلومات كالتحكم في الوصول إليها والتوقيع الإلكتروني بناء على طبيعة متطلبات عمل المجلس والالتزامات القانونية السارية.

يتعين أن تلتزم المعلومات المقرر نشرها بواسطة موظفين نيابة عن المجلس في أي منتدى عام بالقوانين والقواعد واللوائح المعمول بها كما يجب أن يعتمد نشرها من قبل إحدى الجهات الإدارية المعنية.

6-22 سجلات التدقيق

يجب تدوين الاستثناءات الخاصة بسجلات التدقيق وغيرها من الأمور المتعلقة بالأمن والاحتفاظ بها في مكان آمن وفقاً للمعايير الأرشيفية بغرض المساعدة في التحقيق في الحوادث الأمنية وإجراء المراقبة الأمنية الروتينية. ويتعين استخدام السجلات مع جميع مستويات الأنظمة بما فيها الشبكات والتطبيقات والخوادم وقواعد البيانات وغيرها.

6-23 مراقبة استخدام الأنظمة

يجب وضع الأنظمة والإجراءات اللازمة لمراقبة استخدام مرافق معالجة البيانات بغرض ضمان عدم قيام المستخدمين بأية أنشطة غير مصرح بها أو غير ملائمة.

- يراعى في تحديد مستوى المراقبة لكل نظام على حدة عوامل مثل درجة الأهمية والحساسية.
- يجب إرسال أنواع الرسائل ذات الصلة أوتوماتيكياً إلى نظام تسجيل مركزي أمن يمكنه الربط بين المعلومات القادمة من مصادر متعددة وتحليلها وذلك بغرض المساعدة في تحديد الأحداث الأمنية الهامة لأغراض المراقبة الأمنية.
- يجب مراجعة السجلات الأمنية بصورة دورية من قبل الإدارة الأمنية (مسؤول أمن المعلومات) وعند الضرورة بواسطة الأطراف الأخرى (مثل قسم عمليات تكنولوجيا المعلومات) التي تفوضها الإدارة العليا بالقيام بذلك تحديداً، ويحق لمدير أمن المعلومات أو إدارة التدقيق الداخلي مراجعة السجلات الأمنية في أي وقت.

6-24 حماية المعلومات المتعلقة بالسجلات

يجب حماية أنظمة التسجيل وملفات التسجيل كلما أمكن ضد التعديلات غير المصرح بها والمشاكل التشغيلية مثل:

- إبطال مرافق التسجيل الأمني.
- تعديل محتويات ملف التسجيل أو تواريخ أو عدد ملفات التسجيل أو عدد مرات الدخول الشخصي.
- مسح أو إعادة تسمية ملفات التسجيل

- نفاذ مساحة ملفات التسجيل وبالتالي التخلص من السجلات أو الكتابة فوقها.

6-25 سجلات المديرين والمشغلين

يجب أن يحتفظ موظفو قسم عمليات تكنولوجيا المعلومات ومديرو النظم وغيرهم بـ"سجلات للمشغلين" بغرض تدوين الأنشطة الهامة بأنظمة الإنتاج.

6-26 تسجيل الأعطال

يجب الإبلاغ عن الأعطال (أي المشاكل المتعلقة بأنظمة تكنولوجيا المعلومات والاتصالات ومن بينها الخروقات الأمنية المؤكدة أو المشكوك بها وأعطال الأنظمة وأخطاء البرامج (PROGRAM ERRORS)/البرامج الضارة(BUGS)/الفيروسات) وذلك باستخدام الوظائف الإلكترونية المتاحة.

يجب اتخاذ الإجراءات الإصلاحية اللازمة فوراً، مع ضرورة وضع وتطبيق قواعد واضحة للتعامل مع الأعطال المبلغ عنها بما فيها مراجعة الإدارة فيما يخص:

- الاحتفاظ بسجلات للأعطال لضمان معالجة الأعطال بصورة مرضية
- اتخاذ الإجراءات الإصلاحية لضمان عدم تعطل أدوات التحكم والتفويض الكامل بالإجراءات التي تنفذ
- معلمات تهيئة أخطاء السجلات (ERROR LOGGING CONFIGURATION PARAMETERS)

6-27 تزامن التوقيت (CLOCK SYNCHRONIZATION)

بغرض تسهيل إجراء عملية التحليل أثناء التحقيق يجب أن يضبط موظفو قسم العمليات ساعات الأنظمة متزامنة على أساس أحد المراجع مثل التوقيت العالمي المنسق (UTC) مع مراقبة دقة التوقيتات. وينطبق ذلك على أجهزة التحويل (Routers and switchers) والخوادم (servers) وغيرها من أجهزة ومعدات الشبكات.

6-28 تقديم الخدمات

يجب ضمان تطبيق وتشغيل وصيانة أدوات التحكم الأمنية وتعريفات الخدمات ومستويات تقديم الخدمات المنصوص عليها في اتفاقيات تقديم الخدمات المبرمة مع الأطراف الخارجية بواسطة الغير.

- يجب أن تحدد عقود التوريد المبرمة مع الأطراف الخارجية لتوفير الخدمات المتعلقة بتكنولوجيا المعلومات المتطلبات الخاصة بأدوات التحكم في أمن المعلومات والخدمات ومستويات الخدمات.
- يتعين أن يتم من خلال المناقشات والمراجعة – والتفتيش والتدقيق – التأكد من قدرة الأطراف الخارجية على الوفاء بالمتطلبات قبل إبرام تلك العقود والتحقق من قدرتهم ونيتهم على مواصلة تقديم المستوى الكافي من الخدمة بعد إبرام العقود.
- يجب أن تنص العقود المبرمة مع الموردين على منح المجلس "حق التدقيق" بغرض التفتيش على العمليات الداخلية للغير وتقييمها فيما يتعلق بالعقد، ويشمل ذلك جوانب مثل الوثائق الخاصة بالسياسات الأمنية والإجراءات وأدوات التحكم في التغييرات وسجلات التدقيق الإلكترونية وعمليات التعرف على الحوادث الأمنية وإدارتها ومعالجتها والإبلاغ عنها.

6-29 متابعة ومراجعة خدمات الأطراف الخارجية

يجب متابعة ومراجعة الخدمات والتقارير والسجلات التي تقدمها الأطراف الخارجية بانتظام مع إجراء عمليات التدقيق بصورة دورية:

- مراقبة الخدمات التي تقدمها الأطراف الخارجية لضمان قيام الأطراف الخارجية بتأديتها وصيانتها وفقاً لنصوص العقود.
- إيكال المسؤوليات المتعلقة بإدارة عقود الموردين والعلاقات معهم إلى وظائف معينة أو فرق عمل محددة.

6-30 إدارة التغييرات التي تستحدث على خدمات الأطراف الخارجية

يتم إدارة التغييرات التي يتم إدخالها على عملية تقديم الخدمات بما فيها عمليات صيانة وتطوير السياسات والإجراءات وأدوات التحكم الخاصة بأمن المعلومات مع الأخذ في الاعتبار درجة أهمية أنظمة العمل والعمليات المشمولة.

6-31 الربط البيني

يجب اعتماد اتفاقيات الربط بين أنظمة المعلومات بواسطة المسئولين المعنيين بالمجلس.

القسم السابع

التحكم بالوصول

7. التحكم بالوصول

إن الغرض من السياسات المنصوص عليها في هذا القسم هو ضمان قدرة مستخدمي المجلس على الوصول إلى المعلومات الملائمة في أي وقت.

7-1 متطلبات العمل الخاصة بالتحكم في الوصول (ACCESS CONTROL)

يجب تحديد متطلبات العمل بوضوح واعتمادها من قبل إدارة المجلس قبل منح المستخدمين حق الوصول إلى الأصول المعلوماتية الممنوحة للمجلس.

7-2 إدارة وصول المستخدمين

يتم تخطيط وتطبيق العمليات الرسمية بهدف التحكم في منح حقوق الوصول (ACCESS RIGHTS) إلى الأصول المعلوماتية للمجلس:

- تقوم الإدارة الأمنية بعملية تنظيم تسجيل المستخدمين الذين يتطلبون الوصول إلى أنظمة المعلومات والخدمات وغيرها من الأجهزة التكنولوجية الهامة ذات المستخدمين المتعددين عن طريق استخدام إجراءات طلب الوصول إلى البيانات.
- يعتبر المديرون (أو من يقومون بإنابته) مسئولين عن إصدار القرارات بشأن وصول المستخدمين العاديين إلى أنظمة التطبيقات عن طريق السماح لهم بالقيام بأدوار المستخدمين الملائمة.
- يجب أن يفهم المستخدمون شروط السماح لهم بالوصول (يجب أن يظهروا موافقتهم على الالتزام بشروط السياسات والإجراءات الأمنية التي يفرضها المجلس).
- يكون لكل مستخدم من المستخدمين (بما فيهم المديرين administrators) هوية مستخدم مميزة تدل على الإجراءات التي يتخذونها أثناء استخدام النظام.
- تحتفظ إدارة الأمن بسجلات رسمية توثق التفويضات التي تمنحها الإدارة وحقوق الوصول الممنوحة والملغاة.
- تكون إدارة الأمن ومعها قسم عمليات تكنولوجيا المعلومات وملاك الأصول المعلوماتية والمديرين وإدارة الموارد البشرية مسئولين مجتمعين عن التحديث أو الإلغاء الفوري لحقوق الوصول في حال تغيير الموظفين للوظيفة أو تركهم العمل بالمجلس مع ضرورة مراجعة هويات المستخدمين المكررة/غير الصالحة بصورة دورية وإلغائها وحقوق الوصول.

7-3 إدارة الامتيازات

يجب التحكم في تخصيص ومنح الامتيازات من خلال قنوات التفويض التي يجب أن تتسم بما يلي:

- تحديد الامتيازات المتعلقة بكل منتج للنظام (على سبيل المثال نظام التشغيل ونظام إدارة قواعد البيانات) وتصنيف الموظفين التي تمنح إليهم.
- تخصيص ومنح الامتيازات للأفراد على أساس ما يحتاجون إلى استخدامه وعند وجود مناسبة للاستخدام أي الحد الأدنى من المتطلبات الخاصة بأدوارهم الوظيفية عند الحاجة إليها فقط.
- إدارة المستخدم صاحب الامتيازات حسب نفس الإجراءات المتبعة مع المستخدم العادي (أي من خلال إجراءات طلب الوصول إلى البيانات)
- لا تعطي امتيازات المدير المحلي إلا إلى موظفي إدارة تكنولوجيا المعلومات بغرض أداء مهام الدعم الفني، ولا يجوز منح امتيازات المدير المحلي للمستخدمين من غير موظفي إدارة تكنولوجيا المعلومات إلا في حال كانت مطلوبة لاستخدامات معينة تخص العمل مع الحصول على موافقة من رئيس قسم أمن المعلومات.

4-7 إدارة كلمات مرور المستخدمين

تحتاج جميع الأنظمة التي تحتوي على معلومات سرية أو ليست متاحة للجمهور إجراءات كافية لإثبات الهوية (على سبيل المثال اسم المستخدم وكلمة مرور قوية) للتحقق من هوية جميع المستخدمين:

- يكون اتخاذ كلمات المرور إجبارياً (أي لا يجوز أن تكون كلمة المرور فراغ)
- يتم تغيير كلمات المرور التلقائية الخاصة بالأجهزة الجديدة
- يتم الاحتفاظ بنسخ من كلمات المرور الإدارية في مكان أمن خارج الموقع ومعها نسخاً احتياطية لأغراض الاستعادة بعد الكوارث.
- يتم وضع إجراءات رسمية للتحقق من هوية المستخدم قبل إصدار كلمة مرور بديلة.
- يستخدم موظفي إدارة النظام حسابات شخصية ولا يجوز لهم استخدام حسابات إدارة النظام للقيام بالعمليات اليومية الاعتيادية.
- يتم تغيير كلمات المرور المبدئية/المؤقتة عند استخدامها للمرة الأولى
- يطلب من جميع المستخدمين اختيار كلمات المرور الخاصة بهم بناء على تعقيد بنية كلمات المرور المعدة مسبقاً والمتطلبات المتعلقة بالتاريخ.
- يطلب من جميع المستخدمين تغيير كلمات المرور الخاصة بهم بصورة دورية
- يجب تخزين ملفات كلمات المرور بصيغة مشفرة
- يتم تشغيل الخاصية التي تسمح بتعقيد بنية كلمات المرور في الأجهزة الحساسة

- على الأقل حرف واحد كبير
- على الأقل حرف واحد صغير
- على الأقل رقم واحد
- على الأقل رمز لا ينتمي للحروف ولا الأرقام

- يجب أن تتكون كلمات المرور من 8 رموز (character) على الأقل، ويجب ألا تكون كلمة المرور الجديدة هي إحدى كلمات المرور الست الأخيرة على الأقل، ويجب تغيير كلمة السر كل 90 يوماً، والمدة الأدنى لتغيير كلمات المرور هي يومين.
- يتم إقفال الحساب بعد خمس محاولات دخول غير ناجحة خلال مدة نصف ساعة، ويجب إبلاغ مكتب المساعدة بهدف إعادة تعيين كلمة المرور.

5-7 مراجعة حقوق وصول المستخدم

تقوم الإدارة بمراجعة حقوق وصول المستخدمين بصفة دورية من خلال الإجراءات الرسمية:

- يقوم المديرون بالمراجعة الرسمية لحقوق وصول المستخدمين بصورة سنوية وبعد أي تغييرات هامة على مستوى المؤسسة أو الأنظمة أو المستوى الشخصي لجميع الموظفين:
- تقوم إدارة الأمن بمراجعة الامتيازات وحقوق الوصول السارية فيما يخص أنظمة الإنتاج مرتين سنويا على أساس الموافقات المتضمنة في الملف للتحقق من عدم منح امتيازات غير مصرح بها
- يتم إجراء مراجعات لحقوق الوصول في أي وقت بناء على طلب الإدارة أو ملاك الأصول المعلوماتية أو أمن المعلومات أو المدققين.
- يقوم المديرون بمراجعة حقوق وصول المستخدمين والامتيازات وفي حالة الضرورة إعادة اعتمادها عند انتقال الموظفين داخليا وخاصة لغرض تحديد المسؤوليات.
- يجب توثيق جميع عمليات مراجعة حقوق الوصول والامتيازات مع الاحتفاظ بالوثائق لمدة عام واحد على الأقل في نموذج قابل للتدقيق.

7-6 استخدام كلمة المرور

يتم الاحتفاظ بكلمات مرور الامتيازات الإدارية الخاصة بخوادم تكنولوجيا المعلومات والشبكات/الأجهزة الأمنية في مظروف مختوم يحفظ بدوره في خزانه مقفلة، وفيما يخص كلمات المرور (ومن بينها عبارات المرور وأراقم التعريف الشخصية وغيرها) يتعين ما يلي:

- الاحتفاظ بسريتها وعدم تبادلها (ما عدا في حالة هويات المستخدمة المشتركة/الجماعية المصرح بها)
- حفظها عن ظهر قبل وليس تدوينها
- أن تكون سهلة التذكر ولكن يصعب تخمينها (ليست مثلا كلمات من القاموس أو تعديلات في اسم المجلس أو اسم المستخدم أو اسم المشروع أو الإدارة أو الأماكن أو رموز متسلسلة بلوحة المفاتيح وغيرها)

7-7 التعامل مع الأجهزة عند عدم تواجد المستخدم

يجب أن يتأكد المستخدمون من توفر الحماية الكافية للأجهزة عند عدم تواجدهم بجانبها، ويتعين حماية الأجهزة الموجودة في أماكن عمل المستخدمين كأجهزة الحاسب الآلي والحاسب المحمول ومكاتب العمل والطابعات وأجهزة المودم وغيرها ضد وصول الأشخاص غير المصرح بهم إليها، وتقع المسئولية على المستخدم في منع ذلك الوصول غير المصرح به.

7-8 إخلاء المكتب والشاشات

يجب إخلاء أسطح المكاتب وأماكن العمل من الأوراق ووسائط التخزين الإلكترونية القابلة للإزالة (بما فيها أجهزة الحاسب الآلي وأجهزة المساعدة الرقمية الشخصية) عندما لا تكون قيد الاستخدام سواء ضمن ساعات العمل الرسمية أو خارجها، ويعتبر هذا الإجراء هاماً للغاية في حالة وجود معلومات ذات أهمية خاصة (high integrity information) والتي يجب حفظها في خزائن مقفلة لحمايتها من الوصول غير المصرح به (بما فيه التعديل والسرقة والتصوير) وذلك عندما تكون غير مستخدمة.

يجب عدم ترك أجهزة الحاسب الآلي والمحطات الطرفية (terminal) دون مراقبة خلال يوم العمل أثناء دخول أي مستخدم من حسابه إلا إذا كانت مقفلة بواسطة أحد الإجراءات المناسبة كالشاشة الحافظة المزودة بكلمة مرور (-password protected screensaver) أو قفل لوحة المفاتيح (key lock) أو قفل الرموز (token lock). يجب أن يوقف المستخدم تشغيل الجهاز تماماً (log off) في نهاية يوم العمل إلا أن أجهزة الحاسب من نوع سطح المكتب (fixed desktop) قد تترك قيد التشغيل على مدار الليل لأغراض التحديث المؤتمت للبرامج (يجب قفل أجهزة الحاسب المحمول على مدار الليل واستئناف التحديث عند إعادة ربطها بالشبكة مرة أخرى).

7-9 السياسة المتبعة بشأن خدمات الشبكات

لا يجوز منح المستخدمين حق الوصول سوى للخدمات المسموح لهم استخدامها فقط، وينطبق هذا الأمر على كافة الخدمات مثل remote desktop control و SharePoint و WebEx و Domain و E-mail و Files و Folders و Wireless و Telnet و Web Access و Security devices وغيرها.

7-10 التحقق من هوية المستخدم فيما يخص الاتصال من الخارج

يجب التحقق من هوية المستخدمين (user authentication) الراغبين في الوصول إلى شبكات المجلس عند نقطة الدخول الأولية إلى الشبكة باستخدام هويات مستخدمين مميزة وإجراءات التحقق اللازمة من هوية المستخدم (على سبيل المثال الرموز الأمنية المشفرة أو البطاقات الذكية المقرونة بكلمات مرور وأرقام التعريف الشخصية و/أو المقاييس الحيوية (biometrics).

لا يجوز سوى للموظفين المفوضين استخدام برامج التحكم عن بعد في الشبكات، ويجب إعداد قائمة بتلك البرامج مع ضرورة إنشاء أدوات تحكم خاصة لحماية سرية وسلامة البيانات التي تمر عبر الشبكات العامة وحماية الأنظمة المتصلة بها.

يحظر استخدام برامج سطح المكتب البعيد على الإنترنت (Internet-based remote desktop software) مثل WebEx إلا في حال تصريح مدير أمن المعلومات بذلك.

7-11 التعرف على الأجهزة في الشبكات

يتم التعرف على المكون المادي من خلال النظام الذي يدخل إليه الجهاز، وقد تشمل تلك الأجهزة المحطات الطرفية والخطوط وعقد الاتصالات (communication nodes) وأدوات التحكم (controllers) والمعالجات عن بعد (remote processor) وأجهزة الحاسب الآلي. تتراوح أساليب التحقق من العقد المحتملة من عناوين MAC/Ethernet/IP (للمواقف منخفضة المخاطر) إلى التحقق المتبادل بالشفرة (mutual cryptographic authentication) باستخدام الرموز أو الشهادات الرقمية. يجب إعداد وتوثيق واختبار وتطبيق وتشغيل وصيانة ومراجعة الأساليب المنتقاة للوفاء بمتطلبات العمل والأمن بصورة محترفة على أن يتناسب عدد مرات ودرجة عمق المراجعة مع مستوى المخاطر الأمنية.

7-12 منفذ التشخيص عن بعد والتهيئة (configuration port)

- يتم التحكم في الوصول المادي والمنطقي لمنافذ التشخيص والتهيئة

- يتم السماح لموظفي الدعم المفوضين فقط بالوصول إلى منافذ التشخيص عن بعد والتهيئة/الإدارة أو console port وأجهزة المودم التي تسمح بامتيازات الوصول لأغراض الدعم الفني على الأجهزة مثل وذلك باستخدام إجراءات قوية للتحقق من هوية المستخدم والتحكم في الوصول.
- يتم تفعيل المنافذ ذات الامتيازات بالصورة المطلوبة فقط وعند الطلب فقط أمام أنشطة معينة مصرح بها للدعم عن بعد.
- يجب ان تكون جميع مكونات الشبكات قابلة للتعرف عليها وقصر استخدامها على وظائف العمل المعنية.
- يجب توفير الحماية المادية لكل الشبكات والخوادم بما فيها أجهزة routers وswitchers وhubs وfirewalls وfront-end processors ضد الوصول غير المصرح به عن طريق الاحتفاظ بها في غرف أو خزائن مقفلة.

7-13 الفصل بين الشبكات

يجب الفصل بين أنظمة وشبكات المجلس الداخلية وفقاً لمخاطر أمن المعلومات المعنية وتصنيفها إلى فئات (categories) أو مجموعات أو أقسام (partitions) أو مجالات (domains):

- الأنظمة التي تملكها وتديرها الأطراف الخارجية مقابل تلك التي يملكها ويديرها المجلس
- التطوير مقابل الاختبار مقابل أنظمة الإنتاج
- الشبكات السلكية مقابل اللاسلكية
- يتم الفصل عن طريق أدوات التحكم الملائمة كـ firewalls/gateways والفصل المادي والتشفير (على سبيل المثال الشبكات الافتراضية الخاصة virtual private networks) وغيرها التي تعكس المتطلبات الأمنية التي تنشأ عن احتياجات العمل ومخاطر أمن المعلومات حسب التقييم وسياسات أمن المعلومات هذه.

7-14 التحكم في اتصال الشبكات (network connection control)

يجب تقييد قدرة المستخدمين على الاتصال بالشبكات المتشارك بها وخاصة تلك التي تمتد عبر حدود المؤسسة.

7-15 التحكم في توجيه الشبكات (network routing control)

إضافة إلى الجدران النارية فإن أدوات التحكم الأخرى في توجيه حركة السير (مثل إجراءات التحقق من عنوان المصدر والوجهة ومدى عنوان بروتوكولات الإنترنت الداخلي المعين وترجمة عنوان الشبكة) يجب أن تستخدم في التحكم في المعلومات المتدفقة داخل أو بين الشبكات عندما يكون ذلك هاماً لأغراض العمل بهدف معالجة متطلبات التحكم الناشئة عن عمليات تقييم المخاطر الأمنية وأيضاً بغرض الالتزام بالسياسات الأمنية هذه.

7-16 إجراءات تسجيل الدخول الآمن

يجب أن تستخدم أنظمة المجلس إجراءات تسجيل دخول آمنة كلما أمكن ذلك:

- يجب أن يتوفر بأجهزة الحاسب الآلي أداة تسجيل الدخول عن طريق control-alt-delete
- قبل تسجيل دخول المستخدم بجب أن يظهر الجهاز إخطاراً قياسياً يحذر من دخول المستخدمين غير المصرح بهم.
- تعتبر كلمات المرور وأرقام التعريف الشخصية والرموز الخاصة (private keys) وغيرها سرية (حسب تصنيف البيانات المذكور في القسم 3-3) وعليه فإنه يحظر إظهارها على الشاشة أو إرسالها غير مشفرة عبر الشبكات أو تخزينها غير مشفرة.
- في حال إدخال بيانات مستخدم أو كلمات مرور أو أرقام تعريف شخصية أو رموز غير صالحة أو غيرها فإن النظام لا يوضح أي العناصر غير صحيحة
- يسمح النظام بعدد معين من محاولات تسجيل الدخول أو الاتصال غير الناجحة وعندها يتم تجميد اسم المستخدم لمدة معينة

7-17 التعرف على المستخدم والتحقق منه (user identification and authentication)

يجب أن يكون لكل مستخدم معرف مميز (هوية مستخدم) لاستخدامه الشخصي بغرض متابعة الأنشطة التي يقوم بها الشخص في النظام، على أن تلتزم هويات المستخدمين بمعايير اختيار الأسماء ويجب ألا تشير إلى حقوق الوصول الخاصة بالمستخدم أي ألا تحتوي على كلمات مثل المدير أو المشرف أو صاحب الامتيازات.

في حال تعذر استخدام هوية مستخدم مميزة لكل فرد، يجوز مشاركة مجموعة من المستخدمين في هوية مستخدم واحدة لأغراض معينة، على أن يوافق على صراحة مدير أمن المعلومات وملاك الأصول المعلوماتية المعنيين على أي هوية مستخدم يتشاركها المستخدمون، ويكون شخص معين مسئولاً بصفة شخصية عن كل حساب مشترك.

7-18 نظام إدارة كلمات المرور

يجب أن تكون أنظمة إدارة كلمات المرور تفاعلية وتؤمن كلمات مرور لا يسهل اكتشافها (انظر القسم 7-4 "إدارة كلمات المرور").

7-19 استخدام مرافق النظام

يجب التحكم في استخدام مرافق النظام، مع مراعاة أدوات التحكم التالية:

- الحماية عن طريق كلمة المرور الخاصة بمرافق النظام
- فصل مرافق النظام عن برامج التطبيقات
- قصر استخدام مرافق النظام على عدد صغير من الأشخاص المصرح بهم
- تسجيل بيانات أي استخدام لمرافق النظام
- يتم إزالة أو تعطيل مرافق النظام وبرامجه غير الضرورية وخاصة فيما يتعلق بأنظمة الإنتاج الهامة

7-20 إنهاء الجلسات غير النشطة

يجب إنهاء الجلسات غير النشطة بعد فترة معنية من الوقت (الحد الأقصى 15 دقيقة).

7-21 تحديد زمن الاتصال

يجب تهيئة الأنظمة الهامة بغرض تقييد زمن الاتصال أو الوصول إلى الأنظمة الهامة وفقاً للمتطلبات التي يضعها ويعتمدها ملاك الأصول المعلوماتية، ويكون ذلك عن طريق تقييد زمن الاتصال بساعات العمل الاعتيادية في المكتب شريطة عدم وجود حاجة للتشغيل خارج ساعات العمل.

7-22 تقييد الوصول إلى المعلومات

يجب ان يكون لجميع أنظمة التطبيقات التي تعمل عبر المؤسسة إجراءات مناسبة ونشطة للتحكم في الوصول بغرض ضمان سلامة وأمن البيانات ومنع/تقييد الوصول غير المصرح به إلى التطبيقات أو أي أجزاء منها.

7-23 عزل الأنظمة الحساسة

يجب أن يكون للأنظمة الحساسة بيئة حاسب آلي مخصصة لها.

7-24 أجهزة الحاسب والاتصال النقالة

يجب تطبيق أدوات تحكم مناسبة عند استخدام مرافق تكنولوجية نقالة كأجهزة الحاسب المحمول laptop/notebook وأجهزة المساعدة الرقمية الشخصية التي وأجهزة الهاتف النقال التي يوفرها المجلس بغرض حماية الأصول المعلوماتية للمجلس (كالأجهزة والبرامج والبيانات).

- يحظر ترك الأجهزة النقالة دون مراقبة في السيارات أو غرف الفنادق أو قاعات المؤتمرات وغيرها ويجب تطبيق أدوات التحكم في الوصول المنطقي (logical control) (انظر القسم 5-10 أمن المعدات والأجهزة خارج المبني)
- يكون الموظفون المتنقلون مسئولين عن إنشاء نسخ احتياطية منتظمة للبيانات عن طريق التزامن مع برامج تشغيل الشبكات (network drive) أو وسائط إنشاء النسخ الاحتياطية المحلية غير المتصلة بالإنترنت إضافة إلى حماية جميع وسائط النسخ الاحتياطية من السرقة والضياع والتلف (انظر القسم 6-9 "النسخ الاحتياطية من المعلومات) والقسم 6-12 (إدارة الوسائط القابلة للإزالة).
- تعتبر إدارة تكنولوجيا المعلومات مسئولة عن صيانة أنظمة التشغيل وبرامج التطبيقات ويشمل ذلك سد الثغرات الأمنية (patching) في الحال بغرض معالجة نقاط الضعف الأمنية والجدران النارية الشخصية والبرامج الضارة (انظر 6-7 "الحماية من الفيروسات") على الأجهزة النقالة، ويجب على المستخدمين عدم التدخل في هذه الإجراءات الأمنية الفنية عن طريق تعطيلها أو إعادة تهيئتها على سبيل المثال.
- تعتبر مقاهي الإنترنت مواقع غير آمنة نسبياً لذلك يجب على الموظفين المتنقلين الذين يستخدمون أجهزة حاسبات المجلس في مقاهي الإنترنت الحذر بشان إفشاء كلمات المرور وغيرها من المعلومات الحساسة.
- يحظر على موظفي المجلس وغيرهم الاتصال بشبكة المجلس الداخلية باستخدام أجهزتهم الخاصة.
- يجب إعادة الأجهزة النقالة التي أصبح الموظفون في غنى عنها أو أصبحت معيبة إلى إدارة تكنولوجيا المعلومات

7-25 العمل من خارج المجلس

لا يجوز للموظفين الذين يعملون من خارج المجلس (المنزل) الالتزام باستخدام أجهزة الحاسب التي يمتلكها ويشرف على تشغيلها المجلس فقط. ولا يجوز استخدام أجهزة حاسبات المجلس سوى من قبل الموظفين المصرح لهم أو الأطراف الخارجية الذين يعملون بموجب عقد مبرم مع المجلس على أن يتم استخدامها فقط فيما يتعلق بعمل المجلس. ويحظر تماماً استخدام تلك الأجهزة بواسطة الأشخاص غير المصرح بهم (بمن فيهم أفراد العائلة والأصدقاء).

إن الأجهزة المستخدمة في العمل من المنزل تم تهيئتها مسبقاً بواسطة إدارة تكنولوجيا المعلومات وهي مزودة بأدوات التحكم الملائمة في الوصول المنطقي وأجهزة الشبكات والنسخ الاحتياطية من البيانات والحماية من الفيروسات.

القسم الثامن

تطوير وصيانة الأنظمة

8. تطوير وصيانة الأنظمة

إن الغرض من السياسات المنصوص عليها في هذا القسم هو ضمان حماية أنظمة المجلس من سوء الاستخدام والأضرار.

8-1 المتطلبات الأمنية للأنظمة

يتم إجراء تخطيط للأنظمة وتحديد للمتطلبات قبل اختيار ونشر وتطبيق أي نظام من أنظمة المجلس، كما يجب تحديد المتطلبات الأمنية قبل تطوير أنظمة المجلس:

- يجب مراعات متطلبات أمن المعلومات في مرحلة مبكرة من عملية تطوير الأنظمة المتعلقة بالعمل واقتراحات الميزانية وطلبات العمل وغيرها، بغرض الحد من التكاليف الأمنية الإجمالية وضمان تخصيص الموارد الكافية لاستكمال المهام الأمنية اللازمة، وينطبق ذلك على البرامج المخصصة المطورة داخلياً أو خارجياً أو الحزم التجارية الجاهزة سواء في حالة الأنظمة الجديدة أو إدخال التغييرات على الأنظمة القائمة.
- تقوم لجنة أمن المعلومات بمراجعة الأحوال المتعلقة بالعمل خلال مراحل عملية التطوير
- يتم تحديد ملاك الأصول المعلوماتية في اقرب وقت

بمجرد اعتماد مشاريع تطوير أو تغيير الأنظمة يكون مديرو المشاريع الذين يعملون بالتعاون مع المختصين بأمن المعلومات مسئولين عن الالتزام بتطبيق أساليب إعداد البرامج المعتمدة من المجلس وتوفيرها بما يشمل المهام الأمنية المحدد التالية:

- إجراء عمليات تقييم لمخاطر أمن المعلومات عالية الأهمية، وعند الضرورة، إعداد تحليل مفصل للمخاطر بهدف توضيح متطلبات التحكم الأمنية بما يتناسب مع قيمة الأصول المعلوماتية والآثار المحتملة للحوادث الأمنية.
- تطوير أدوات التحكم الفنية والإجرائية والإدارية المتعلقة بأمن المعلومات والتي تتألف من مزيج من أدوات التحكم الوقائية والتعقبية والعلاجية.
- تقييم/اختبار الأنظمة على أساس مواصفات المتطلبات التي تشمل العناصر الأمنية واستكمال أي تعديل لازم لتحقيق الالتزام ، على أنه يتم إجراء عملية الاختبار والتقييم تلك بالتوافق التام مع إجراءات الاختبار والتقييم الأمني التي وضعتها حكومة أبوظبي.
- يمكن للمجلس اعتماد وتصديق الخدمات المصنفة على أنها "منخفضة" (LOW) بنفسه
- أما الخدمات المصنفة على أنها "متوسطة" (MODERATE) فتقرر الجهة المخولة بالاعتماد إما اعتمادها بنفسها إو إحالتها إلى مركز أبوظبي للأنظمة الإلكترونية والمعلومات من أجل اعتمادها.

- يجب أن تحصل الخدمات المصنفة على أنها "عالية" (HIGH) على اعتماد من مركز أبوظبي للأنظمة الإلكترونية والمعلومات للتحقق من تقرير تقييم المخاطر وخطة أمن المعلومات ذات الصلة.
- بصورة عامة يجب أن تمر كافة الخدمات بعملية للاعتماد والتصديق قبل تطبيقها. في حال وجود حالة عملية معتمدة من قبل الإدارة العليا وتتضمن المبررات الكافية لتشغيل الخدمة في وقت قصير، يحب أن يتحقق المجلس من استكمال عملية الاعتماد والتصديق في غضون فترة معقولة من تشغيل الخدمة، علماً بأن تلك الفترة المعقولة تتراوح بين 6 شهور و12 شهراً.
- الانتهاء من الاختبار العملي وفقاً لتوقيع مالك الأصول المعلوماتية.

8-2 التحقق من صحة البيانات المدخلة

يجب أن تشمل أنظمة التطبيقات أدوات التحكم الفنية والإجرائية المناسبة لضمان سلامة البيانات المدخلة (صحتها واكتمالها ودقتها) بصورة يدوية أو أوتوماتيكية، وكلما زادت حساسية التطبيق كلما تشددت قواعد التحقق من البيانات المدخلة:

- يجب إجراء عمليات التحقق فيما يخص بيانات معاملات العمل والبيانات الأساسية standing data (على سبيل المثال أسماء الطلبة وعناوينهم وحدود الائتمان وأرقام العملاء)وجداول المعلمات (على سبيل المثال: الأسعار وسعر تغيير العملات ومعدلات الضرائب) عند إدخال البيانات إلى النظام أو بعدها بمدة قصيرة.
- قد يشمل التحقق من البيانات المدخلة يدوياً إجراءات يدوية لمراجعة صحة واكتمال مصادر الوثائق وغيرها عن طريق الموظفين المسئولين عن إدخال البيانات عن طريق المراجعة من قبل نظرائهم الموظفين أو المديرين.
- يمكن التحقق من البيانات المدخلة يدوياً أو أوتوماتيكياً عن طريق وظائف التحقق الأوتوماتيكي أو المنهجي.
- القيم الخارجة عن المدى (out-of-range values) (مثل المجموعات التسلسلات زائدة الطول excessively long strings).
- الرموز غير الصالحة (كعلامات التنصيص أو غيرها من الفواصل الموجودة في البيانات المدخلة المستخدمة في إنشاء SQL queries).
- البيانات المفقودة أو غير الكاملة (كالحقول الرئيسية غير المدخلة أو القيم المفقودة المتسلسلة)
- تجاوز الحد الأعلى أو الأدنى للحجم (مثلا في حال طلب 10 عناصر بيانات أو رسائل وإدخال 9 أو 11)
- بيانات تحكم غير مصرح بها أو غير منسجمة (مثلا توقيع رقمي غير صالح أو مفقودة أو عدم مطابقة إجمالي الأعمدة وإجمالي الصفوف)

- البيانات المشكوك بها (implausible data) وهي تعني تقنيات العمل المنطقية والمعاملات للتعرف على قيم بيانات غير صالحة أو مشكوك بها أو بنيتها أو زمنها أو حجمها وغيرها.
- الحزم غير الصالحة (مثلا تنسيق أو تاريخ خاطيء للملف أو عدد غير متوقع للسجلات أو خروج عن التسلسل وغيرها)

8-3 التحكم في المعالجة الداخلية

وفقاً للتصاميم الأمنية يجب أن تشمل أنظمة التطبيقات أدوات التحكم اللازمة لضمان سلامة عمليات المعالجة الداخلية مثل:

- تسجيل معلومات التدقيق الداخلي المعني في ملفات سجلات آمنة لأغراض التحليل اللاحق عليها.
- أدوات التحكم المرجعية في سلامة قواعد البيانات (مثلا التحكم في التغييرات في القيم في الحقول الرئيسية المستخدمة في ربط جداول البيانات ذات الصلة).
- التحكم في عمليات التشغيل (run-to-run) والبرامج (program-to-program) كمراجعة الأرصدة الافتتاحية في مقابل الأرصدة الختامية السابقة وإجمالي تحديث الملفات والأرقام التسلسلية للمعاملات وغيرها.
- نقطة مراجعة المعاملات (checkpoint) والرجوع عنها (rollback) بغرض الرجوع عن المعاملات غير الصالحة
- عمليات التحقق من سلامة ومصداقية البرامج والسجلات و/أو الملفات التي تتم أثناء التشغيل أو الدورية عن طريق المقارنة بين مختلف القيم/التوقيعات الإلكترونية من ناحية والقيم الموثوقة المخزنة من ناحية أخرى إضافة إلى الكشف عن البرامج الإلكترونية الضارة.
- عمليات المراجعة المتعلقة بتأخير عمليات المعالجة والصفوف الطويلة وأحجام المعالجة الزائدة والذاكرة الزائدة أو مرافق وحدة المعالجة المركزية أو غيرها من الأعراض المحتملة لأخطاء المعالجة والفجوات اللانهائية (INFINITE LOOPS) وغيرها التي تستلزم تطبيق أساليب ملائمة للتعامل مع الأخطاء والإجراءات الاستثنائية.

8-4 سلامة الرسائل

يجب استخدام أساليب التحقق من الرسائل كالتوقيع الرقمي وأكواد التشفير لضمان سلامة محتويات الرسائل الحساسة ورسائل البريد الإلكتروني.

8-5 التحقق من المخرجات (OUTPUT DATA)

يجب مراجعة البيانات الصادرة عن أنظمة الإنتاج كلما أمكن ذلك للتأكد من اكتمال عملية المعالجة بصورة سليمة ودقيقة باستخدام أدوات تحكم مثل:

- تسوية إجمالي المدخلات والمخرجات من البيانات على سبيل المثال أن يتساوى إجمالي حزمة المدخلات مع إجمالي خدمة المخرجات أو الأرصدة
- التحقق من صحة قيم المخرجات، على سبيل المثال، تصحيح المدى والنوع
- التحقق من الاكتمال، على سبيل المثال، معالجة جميع سجلات المدخلات دون أخطاء وفراغ الملف
- استعادة النسخ الاحتياطية، على سبيل المثال، نقطة المراجعة (CHECKPOINT) والرجوع في المعالجة (rollback processes) لعكس عملية تشغيل برنامج غير صالح
- تدوين المعلومات ذات الصلة (شاملة نجاح/فشل عملية التحقق) في سجلات التطبيق وسجلات التدقيق وغيرها

8-6 السياسة المتعلقة باستخدام أدوات التحكم في التشفير

يجب استخدام التشفير لحماية المعلومات ذات السرية العالية و/أو متطلبات سلامة، مع مراعاة المتطلبات والشروط التالية عند استخدام أدوات التشفير بالمجلس:

- متطلبات التعامل مع المعلومات الحساسة عند نقلها بالوسائط والأجهزة النقالة أو القابلة للإزالة أو عبر خطوط الاتصال.
- آثار استخدام المعلومات المشفرة على أدوات التحكم الأخر (على سبيل المثال: الكشف عن الفيروسات)

بناء على درجة الحماية/مستوى الثقة الذي يتطلبه العمل، يجب التحقق من التوقيع الإلكتروني من خلال التشفير باستخدام المفاتيح العامة المعنية بالتوقيع نشرها على شهادات إلكترونية صالحة تصدرها سلطات التصديق التي يختارها المجلس (على سبيل المثال DigCert).

8-7 التحكم في برامج التشغيل (operational software)

يتم إتباع الإجراءات التالية بغرض التحكم في تثبيت البرامج على أنظمة التشغيل:

- يجب التحكم في استخدام البرامج على أنظمة الإنتاج بغرض الحد من المخاطر المتعلقة بتلف أنظمة التشغيل. ولا يجوز سوى لأمناء المكتبات المعينين تحديث مكتبات برامج الإنتاج، على أن يتم التصريح بتلك التحديثات وتسجيلها.

- يجب أن تمنع أدوات التحكم بأنظمة التشغيل الوصول المباشر غير المصرح به إلى برنامج التطبيقات وملفات البيانات (ومن بينها مرافق التطبيقات/الأدوات وتهيئة التطبيقات/وملفات المعلمات وبدء تشغيل التطبيقات/وبيانات الإغلاق وملفات تسجيل بيانات التطبيقات) بواسطة مستخدمين آخرين.
- يتم الاحتفاظ بالنسخ السابقة من البرامج تحت إدارة التهيئة كإجراء احترازي.
- يجب صيانة البرامج التي يوفرها الموردين والمستخدمة في الإنتاج وخاصة فيما يخص الثغرات الأمنية.
- يتم السماح بالوصول المباشر المقتصر على القراءة إلى برامج التطبيقات وملفات البيانات للقيام بأنشطة إدارة الأنظمة الروتينية كإنشاء النسخ الاحتياطية والأداء ومراقبة السعة/الطاقة والمراقبة الأمنية، ولا يسمح بالوصول المباشر إلا من خلال إجراءات التحكم في التغييرات.

8-8 حماية بيانات اختبار النظام

يجب تأمين البيانات المتعلقة بالاختبارات وفقاً للفئات المصنفة إليها، ولا يجوز استخدام بيانات الإنتاج لأغراض التطوير أو الاختبار ما لم ينتهي وضعها الحساس. يجب أن تخضع أنظمة الاختبار لأدوات التحكم في الوصول المطبقة على أنظمة التشغيل.

8-9 التحكم في الوصول لكود مصدر البرنامج

يتم تقييد الوصول إلى كود مصدر البرنامج (program source code):

- يتم الاحتفاظ بكود مصدر البرنامج والمعلومات المتعلقة به (كالمخططات والمواصفات وقوائم البرامج وخطط الاختبارات والتقارير) وفقاً لإجراءات التحكم في التغيير في مكتبات منفصلة لأغراض التطوير والاختبار وبيئات الإنتاج على إن يكون ذلك بواسطة أمناء المكتبات المعينين.
- لا يجوز تضمين سوى الأكواد التي مرت باختبار اختبار قبول الإنتاج في مكتبات الإنتاج (production libraries).
- يقوم أمناء المكتبات المعينين مباشرة بتحديث وتسجيل الأكواد المحفوظة ضمن مكتبات مصادر البرامج وإصدار أو تجميع الأكواد من المكتبات.
- يتم أرشفة النسخ القديمة من برامج المصدر.
- يتم الاحتفاظ بكود المصدر (source codes) التي تملكها الأطراف الخارجية في حساب ضمان (escrow) في حال اعتماد المجلس بصورة جوهرية على القدرة على صيانة/تحديث الكود وخاصة في حال وجود أية شكوك بشأن جدية أو -قدرات الموردين.

8-10 إجراءات التحكم في التغيير

يتم التحكم في التغييرات عن طريق استخدام إجراءات رسمية للتحكم في التغييرات (انظر أيضاً القسم 6–2 "التحكم في التغييرات") كما يلي:

- لا يتم تطبيق التغييرات إلا بعد الموافقة الرسمية عليها من قبل المالك (أو من ينوبه).
- يتم تقييم الآثار المحتملة للتغييرات المطلوبة وخاصة فيما يخص:
  - أدوات التحكم الأمنية الحالية
  - الأنظمة والتطبيقات الأخرى المتأثرة وربما تتطلب تحديث
  - تحديث الوثائق

- يجب إبلاغ بيانات التغييرات إلى جميع الموظفين المختصين للسماح بإجراء المراجعات اللازمة قبل التنفيذ.
- يتم توثيق الإجراءات والمسئوليات المتعلقة بالتغييرات في الأنظمة بغرض إبطال و/أو الاستعادة بعد التغييرات غير الناجحة
- يتم الاحتفاظ بسجل لسلطات التفويض (من يحق له تفويض ماذا)
- يتم الاحتفاظ بسجل للتدقيق بكافة طلبات التغييرات

8–11 المراجعة الفنية للتطبيقات بعد إدخال التغييرات على أنظمة التشغيل

يجب تطبيق التغييرات التي تجري على أنظمة التشغيل من خلال إجراءات التحكم في التغييرات المعمول بها، وهي تشمل عملية التحقق اللاحقة على التركيب (انظر القسم 8–10 "إجراءات التحكم في التغييرات")، ويجب اختبار أنظمة التطبيقات قبل البدء في تطبيق التغييرات الهامة التي تجري على أنظمة التشغيل (كتحديث البرامج أو سد الثغرات الأمنية) وذلك بغرض الحد من مخاطر الآثار العكسية على أمن التطبيقات والقدرات الإنتاجية.

8–12 القيود المتعلقة بتغيير حزم البرامج

يتم استخدام حزم البرامج التي يوفرها الموردون دون إجراء أية تعديلات جوهرية كلما أمكن، وفي حال تطلب الأمر إدخال تعديلات على حزم البرامج التي يوفرها الموردون، يجب مراعاة ما يلي:

- الحصول على الموافقة المسبقة من مالك الأصول المعلوماتية والمورد
- تقييم المخاطر المتعلقة بالتعديل وآثاره المحتملة وخاصة في حال مسئولية المجلس عن صيانة البرامج في المستقبل نتيجة للتغييرات
- اختبار والتحكم في التغييرات بصورة كاملة
- توثيق كافة التغييرات بصورة كاملة بحيث يمكن إعادة تطبيقها عند الضرورة بعد التحديثات المستقبلية التي يجريها الموردون

8–13 تسرب المعلومات

يتم العمل على منع أية فرصة لتسرب المعلومات:

- يجب شراء البرامج من مصادر موثوق بها أو تطويرها بواسطة مختصين أكفاء وموثوق بهم
- في حال تقييم مخاطر التهديد الأمني على أنها كبيرة يجب تدقيق كود المصدر ضد التهديدات مثل وظائف backdoors و covert channels و trojan horse كجزء من اختبار قبول المنتج.
- يجب التحكم في الوصول إلى كود المصدر والبرامج التنفيذية (executable programs) فيما يخص جميع برامج الإنتاج (انظر القسم 8–9 "التحكم في الوصول إلى كود مصدر البرامج).
- يجب تهيئة أنظمة منع/رصد المتسللين والجدران النارية بغرض التعرف على الاتصالات غير المصرح بها وحجبها

8–14 تطوير البرامج عن طريق التعهيد

يجب أن تنص عقود تعهيد تطوير البرامج على ما يلي:

- المتطلبات الخاصة بجودة الكود ودقة العمل قيد التنفيذ ومدى الاختبارات السابقة واللاحقة على التسليم
- الالتزام بالدليل والمعايير والإرشادات المتعلقة بسياسة أمن المعلومات وغيرها من الوثائق ذات الصلة ويشمل ذلك جوانب مثل تحليل المخاطر والمواصفات الأمنية الموثقة وضمان الجودة والتحكم في التغييرات وعمليات التحقق من التركيب والترخيص وحساب الضمان وحقوق الملكية الفكرية.
- حق المجلس في التدقيق على عمليات التطوير والاختبار

8–15 التحكم في نقاط الضعف الفنية

يجب توفير المعلومات اللازمة بشأن نقاط الضعف الفنية بأنظمة المعلومات في الوقت المناسب، مع تقييم درجة تعرض المجلس لنقاط الضعف تلك واتخاذ الإجراءات اللازمة لقبول أو معالجة المخاطر ذات الصلة. يجب اتخاذ الإجراءات اللازمة للاستجابة للتعرف على نقاط الضعف الفنية المحتملة في الوقت المناسب:

- يتولى قسم عمليات تكنولوجيا المعلومات، بالتعاون مع قسم أمن المعلومات، مسئولية مراقبة نقاط الضعف وتقييم المخاطر وسد الثغرات وتتبع الأرصدة والتنسيق.
- يكون قسم أمن المعلومات مسئول عن توفير مصادر المعلومات الكافية عن نقاط الضعف الفنية بما يشمل متعهدي تكنولوجيا المعلومات والأطراف الخارجية الجديرة بالثقة مثل Qualys وCERT.

بناء على المخاطر ودرجة الأهمية فإنه يجب الالتزام بإجراءات إدارة التغييرات العادية والتغييرات الطارئة أو الاستجابة لحوادث أمن المعلومات (انظر القسم 9–1 "الإبلاغ عن حوادث أمن المعلومات").

القسم التاسع

إدارة الحوادث المتعلقة

بأمن المعلومات

9. إدارة الحوادث المتعلقة بأمن المعلومات

يجب وضع وتطبيق خطة لإدارة أمن المعلومات لضمان الإبلاغ عن حوادث ونقاط الضعف المتعلقة بأمن المعلومات بصورة تسمح بالوقت الكافي لاتخاذ الإجراءات العلاجية.

9-1 الإبلاغ عن حوادث أمن المعلومات

يجب أن يقوم الموظفون بإبلاغ مكتب الدعم الفني IT Helpdesk التابع لإدارة تكنولوجيا المعلومات عن الحوادث المتعلقة بأمن المعلومات في أقرب وقت ممكن بعد حدوثها، ولهذا الغرض يتعين توعية الموظفين بالإجراءات السليمة لرصد وعلاج والحوادث الأمنية كجزء من عمليات التدريب التعريفي القياسي بأمن المعلومات والتوعية الأمنية (انظر القسم 4-5 "التوعية بشأن أمن المعلومات"). تشمل حوادث أمن المعلومات على سبيل المثال:

- عدم الالتزام بأحكام دليل سياسات أمن المعلومات أو مخالفة القوانين واللوائح المعمول بها بشأن مخاطر تكنولوجيا المعلومات والتحكم بها وإدارتها.
- الأنشطة غير الطبيعية لنظام تكنولوجيا المعلومات كالأعطال ورسائل الأخطاء والفيروسات والتحذيرات والتنبيهات والتأخير والنتائج غير المتوقعة
- ضياع أو فقد خدمات أو أجهزة أو مرافق تكنولوجيا المعلومات وتشمل السرقة والتلف والأعطال والتحميل الزائد والحوادث والأخطاء البشرية والمواقف الأخرى التي تسبب انقطاع الخدمات.
- التغييرات غير القابلة للتحكم بها أو غير المصرح بها التي تجري على الأنظمة
- اكتشاف حقوق وصول غير سليمة/غير مصرح بها
- إساءة استخدام الأنظمة
- انتهاك السرية (مثلا الإفشاء غير المصرح به أو الوصول للمعلومات الحساسة)
- اختراق الشبكات أو الأنظمة أو الوصول للبيانات والسياسات

يقوم مكتب دعم تكنولوجيا المعلومات بالبدء في عمليات الاستجابة للحوادث ومشاركتها وإبلاغها إلى الأطراف ذات الصلة والتي تشمل واحداً أو أكثر مما يلي:

- المديرون المحليون/مديرو الخطوط
- أمن المعلومات وتكنولوجيا المعلومات
- لجنة أمن المعلومات ومدير أمن المعلومات ومسئول أمن المعلومات
- رجال الأمن

- ملاك الأصول المعلوماتية
- الموارد البشرية
- الشؤون القانونية
- التدقيق الداخلي
- المديرون التنفيذيون

بعد معالجة الحوادث الأمنية المبلغ عنها يقوم مكتب دعم تكنولوجيا المعلومات بإغلاق السجلات عن طريق إخطار الطرف المبلغ بالنتائج.

9-2 الإبلاغ عن نقاط الضعف الأمنية

يقوم الموظفون برصد والإبلاغ بشأن أية نقاط ضعف أو تهديدات أمنية مرصودة أو مشكوك بها أنظمة تكنولوجيا المعلومات أو الخدمات إلى مديريهم و/أو مكتب دعم تكنولوجيا المعلومات في اقرب وقت ممكن.

يحظر على الموظفين القيام بأنفسهم بمحاولة "استكشاف" أو "تقييم" أو "تأكيد" أو "إثبات" نقاط الضعف المشكوك بها والتي يمكنها أن تؤدي إلى (أ) التسبب بخروقات أمنية خطيرة، (ب) التدخل في أنشطة التحليل القانوني، و/أو (ج) اعتبارها إساءة استخدام متعمد للنظام ويترتب عليها اتخاذ إجراءات تأديبية أو قانونية. وبالمثل لا يجوز للموظفين محاولة إصلاح أية أعطال بالبرامج إلا في حالة ورود تعليمات صريحة إليهم من مكتب الدعم الفني لتكنولوجيا المعلومات بالقيام بذلك.

9-3 المسئوليات والإجراءات

يجب أن تضمن مسئوليات وإجراءات إدارة الحوادث الاستجابة السريعة والفعالة والمنظمة لجميع أنواع حوادث امن المعلومات.

تشمل إجراءات الاستجابة لحوادث امن المعلومات ما يلي:

- تحليل الحوادث الأمنية المبلغ عنها ونقاط الضعف ومراقبة الأنظمة والإنذارات وجوانب الضعف بغرض التعرف على الحوادث الأمنية وترتيبها حسب الأولوية سواء الحوادث الفعلية أو الوشيكة.
- الاحتواء (على سبيل المثال فصل الأنظمة المتضررة عن الشبكات حتى إجراء المزيد من التحليل)
- تحليل وتحديد أسباب الحوادث ("ماذا حدث بالضبط؟ ومن فعل ذلك؟ وما هي الأصول التكنولوجية المتضمنة؟ وما هي أدوات لتحكم الغائبة أو الفاشلة؟ وما هي الأضرار التي لحقت بالعمل؟")

- تطبيق الدروس المستفادة من الحوادث واستغلالها في تطوير القدرة على إدارة المخاطر الأمنية المتعلقة بالمعلومات.
- جمع وتأمين ملفات التسجيل وسجلات التدقيق وغيرها من الأدلة القانونية

9-4 التعلم من خلال التعامل مع حوادث أمن المعلومات

يتم إحصاء ومراقبة أنواع وأحجام وتكاليف حوادث امن المعلومات (إن وجدت) للتعرف على الحوادث المتكررة أو عالية التأثير أو الأعطال، وربما يبين ذلك الحاجة إلى مزيد من أدوات التحكم وإجراء بعض التغييرات على دليل سياسة أمن المعلومات هذا.

يجوز استخدام بيانات حوادث أمن المعلومات بغرض التوعية الأمنية مع مراعاة السرية (على سبيل المثال إزالة بيانات الأشخاص المتورطين أو غيرها من المعلومات الحساسة).

9-5 جمع الأدلة

في حال وصول الحوادث غلى الحد الذي يستوجب اتخاذ إجراءات قانونية يتم جمع والاحتفاظ بالأدلة القانونية بغرض الالتزام بقواعد جمع الأدلة وفقاً لشروط اللوائح والنظم/القضاء.

القسم العاشر

إدارة استمرارية العمل

10. إدارة استمرارية العمل

إن الغرض من وضع السياسات المنصوص عليها بهذا القسم هو ضمان مراعاة استمرارية العمل، على أن يتم وضع وتطبيق خطط عمليات العمل الطارئة وعملية إتاحة واستعادة تكنولوجيا المعلومات بغرض تعظيم القدرة على استمرارية العمل بالمستوي العملي المطلوب مع الحد من التكاليف في المرحلة الانتقالية التي تقع بين انقطاع واستعادة خدمات تكنولوجيا المعلومات.

10-1 إدخال أمن المعلومات ضمن عملية إدارة استمرارية العمل

يجب إدارة استمرارية العمل (business continuity) بصورة متناغمة عبر أقسام المجلس ومعالجة مسألة اعتماد العمل على العمليات الجوهرية عن طريق ضمان توافر أنظمة تكنولوجيا المعلومات المساندة، وهذا يعني ضرورة إنشاء ومد إدارة استمرارية العمل لتشمل جميع أجزاء المجلس.

10-2 استمرارية العمل وتقييم المخاطر

تشمل عمليات إدارة استمرارية العمل ما يلي:

- تحديد وترتيب أولوية أنشطة العمل الجوهرية من خلال إجراء تحليل منظم عبر المؤسسة لتحليل الآثار تشمل كبار المديرين وملاك الأصول المعلوماتية وقسم إدارة المخاطر وإدارة أمن المعلومات.
- توضيح المخاطر المترتبة على فشل الأنظمة والتي تصيب أنشطة العمل الجوهرية فيما يخص احتمالية وزمن الآثار وغيرها بغرض وضع وتوثيق متطلبات الإتاحة.
- وضع مواصفات ومخططات أدوات التحكم وتطويرها واختبارها وصيانتها لضمان المرونة (الاتصالات المتكررة والاستعادة بعد الكوارث وغيرها).

10-3 تطوير وتطبيق خطط لضمان استمرارية العمل تشمل أمن المعلومات

يجب تطوير وتطبيق خطط لصيانة و/أو استعادة العمليات في غضون الحدود الزمنية المطلوبة بعد انقطاع، أو فشل، أنشطة العمل الجوهرية.

10-4 إطار خطط استمرارية العمل

يتم الاحتفاظ بإطار واحد لخطط استمرارية العمل لضمان تناغم جميع الخطط مع بعضها البعض حتى يمكن الوفاء بمتطلبات أمن المعلومات بالصورة السليمة وترتيب الأولويات فيما يخص الاختبار والصيانة.

يختص كل خطة من خطط استمرارية العمل بوصف الأسلوب العام الذي يضمن توفر المعلومات والأنظمة وعمليات وشروط التصعيد (escalation) إضافة إلى الشخص المسئول عن تنفيذ كل مكون من مكونات الخطة.

تشمل خصائص إطار خطط استمرارية العمل ما يلي:

- وصف شروط تفعيل الخطط والعمليات اللاحقة على ذلك
- وصف إجراءات الطوارئ وأنواع الاستجابة المتعلقة بإدارة الأزمات الواجب اتخاذها عقب وقوع أي حادث
- إجراءات الرجوع
- إجراءات التشغيل المؤقتة
- إجراءات الاستئناف
- الجداول الزمنية للصيانة التي تحدد طريقة وتوقيت اختبار وصيانة الخطط
- أنشطة التوعية والتثقيف والتدريب
- الأدوار والمسؤوليات
- الأصول والموارد الجوهرية اللازمة لتفعيل إجراءات الطوارئ والرجوع والاستئناف

10-5 اختبار خطط ضمان استمرارية العمل وصيانتها وإعادة تقييمها

يجب اختبار وتحديث خطط استمرارية العمل بصورة دورية لضمان تحديثها وفعاليتها.

القسم الحادي عشر

الالتزامات القانونية

11. الالتزامات القانونية

إن الغرض من وضع السياسات المنصوص عليها بهذا القسم هو ضمان الالتزام القانوني والالتزام بسياسات أمن المعلومات بالمجلس مع الأخذ في الاعتبار أية قوانين أو تشريعات أو لوائح أو التزامات تعاقدية تخص أمن المعلومات.

11-1 التعرف على التشريعات الملزمة

يتعين على ملاك الأصول المعلوماتية طلب مشورة إدارة الشؤون القانونية والالتزام القانوني بشأن الالتزامات القانونية والتنظيمية والتعاقدية، على أن يتم تحديد وتوثيق الالتزامات القانونية والتعاقدية الخاصة بكل نظام معلومات بصورة واضحة.

تشمل الالتزامات العامة الخاصة بالمجلس فيما يخص استخدام تكنولوجيا المعلومات ما يلي:

- حقوق الملكية الفكرية التي تسري على حقوق الطبع والنشر والعلامات التجارية وبراءات الاختراع والتصاميم المسجلة وغيرها (انظر القسم 11.2 "حقوق الطبع والنشر الخاصة بالبرامج").
- القوانين واللوائح المتعلقة بحماية سجلات المجلس والحفاظ على سلامة البيانات وتوفرها وغيرها، وخاصة فيما يخص دقة التقارير المالية ومواعيدها الزمنية ومنها على سبيل المثال التقارير السنوية والضرائب (انظر 11-3 "حماية سجلات المجلس").
- حماية البيانات وقوانين الخصوصية التي تحمي حقوق الأفراد (انظر القسم 11-4 "حماية البيانات وخصوصية المعلومات الشخصية").
- القوانين المتعلقة الأشكال المختلفة لإساءة استعمال أجهزة الحاسب الآلي والاحتيال والتسويق الإلكتروني/الرسائل المتطفلة وغيرها (انظر القسم 11-5 "منع إساءة استخدام مرافق معالجة المعلومات")
- القوانين المتعلقة باستخدام وتصدير الشفرات القوية (انظر القسم 11-6 "اللوائح الحاكمة للتشفير").
- اتفاقات السرية/عدم الإفشاء وأحكام العقود المتنوعة (على سبيل المثال: سريان التوقيعات الرقمية).
- القوانين واللوائح الخاصة بمراقبة أفعال الموظفين والغير

11-2 حقوق الطبع والنشر الخاصة بالبرامج

لا يمكن تثبيت البرامج إلا إذا كان لدى المجلس العدد الكافي من التراخيص، ويجب على مجموعات العمل المختصة بتكنولوجيا المعلومات التحقق من البرامج المثبتة للتأكد من امتثالها لاتفاقيات تراخيص البرامج، وفي حال تثبيت المستخدمين لبرامج إضافية لازمة لاستكمال تأدية مهام وظائفهم، يجب اعتماد ورصد تلك البرامج من قبل إدارة المجلس. ويحظر على المستخدمين استغلال أو إنشاء/توزيع نسخ غير مصرح بها من المواد/البرامج المحمية بحقوق الطبع والنشر أو المرخصة.

لا يجوز نسخ المواد المحمية بحقوق الطبع والنشر دون موافقة المالك. وفي هذا الشأن يلتزم المجلس بالقانون الاتحادي لدولة الإمارات المتحدة رقم 7 لعام 2002 بشأن حقوق الطبع والنشر وما يتعلق بها من حقوق.

11-3 حماية سجلات المجلس

يجب أن تقوم الإدارة بحماية سجلات المجلس الهامة وفقاً لعملية تصنيف المعلومات (انظر القسم 3-3 "تصنيف المعلومات") وذلك ضد الضياع والتدمير والتزوير إلى الدرجة اللازمة للحد من المخاطر التي يمكن أن تهدد المجلس وفقاً لسياسة أمن المعلومات الخاصة بالمجلس. ويتم تصنيف السجلات إلى فئات مثل سجلات المحاسبة وسجلات قواعد البيانات وسجلات المعاملات وسجلات التدقيق والإجراءات التشغيلية، ويحدد لكل منها التفاصيل المتعلقة بفترة الاحتفاظ بها ونوع وسائط التخزين مثل الأوراق والوسائط المغنطيسية والضوئية وأجهزة تخزين البيانات (المايكروفيش).

11-4 حماية البيانات وخصوصية المعلومات الشخصية

استحدثت العديد من الدول تشريعات تضع أدوات للتحكم في معالجة وبث المعلومات الشخصية (بصفة عامة المعلومات المتعلقة بأشخاص أحياء ويمكن التعرف عليهم باستخدام تلك المعلومات)، وقد تفرض هذه الأدوات واجبات على الأشخاص الذين يقومون بجمع ومعالجة ونشر المعلومات الشخصية، وربما تضع قيوداً على القدرة على نقل المعلومات الشخصية إلى بلدان أخرى.

- يحظر استخدام المعلومات الشخصية سوى لأغراض محددة وقانونية
- يجب أن تكون المعلومات الشخصية كافية وذات علاقة وليست زائدة
- يحظر الاحتفاظ بالمعلومات الشخصية لفترة أطول من اللازم

- يجب أن تشمل الأنظمة والعمليات المتعلقة بمعالجة وتخزين والإبلاغ بالبيانات الشخصية أدوات تحكم ملائمة في أمن المعلومات وخاصة حماية سرية البيانات وسلامتها (مع تطبيق متطلبات سرية عالية مع المعلومات شديدة الحساسية كسجلات الامتحانات والميول الجنسية والدين وغيرها).

يكون ملاك الأصول المعلوماتية، بالتشاور مع مسئول أمن المعلومات، مسئولاً عن التأكد من الامتثال لالتزامات حماية البيانات.

11-5 منع إساءة استخدام مرافق معالجة البيانات

يتم التصريح وصول الموظفين إلى مرافق وأنظمة تكنولوجيا المعلومات بالمجلس لأغراض العمل، ولا يصح استخدام تلك المرافق في غير أغراض العمل أو لأغراض غير مصرح بها.

11-6 اللوائح الحاكمة للتشفير

يجب استخدام أدوات التحكم في التشفير بما يضمن الالتزام بالاتفاقات والقوانين واللوائح ذات الصلة.

11-7 الالتزام القانوني للسياسات والمعايير الأمنية

يقوم المديرون بالعمل على التحقق من الالتزام بجميع إجراءات أمن المعلومات ضمن سلطتهم بالصورة السليمة:

- يجب أن يرعى ملاك الأصول المعلوماتية أنشطة المراجعة الدورية للتحقق من امتثال أنظمة التطبيقات لدليل سياسة أمن المعلومات هذا والمعايير ذات الصلة إضافة إلى المتطلبات الأمنية.
- بالإضافة إلى أنشطة المراجعة الدورية المشار إليها، يجب أن يقوم المدققون الداخليون والخارجيون بمراجعة الالتزام القانوني بسياسات ومعايري وتعليمات المجلس وغيرها من الممارسات الجيدة فيما يخص أمن المعلومات من وقت لأخر وفقاً للجدول الزمني لأعمال التدقيق المتعلقة بالمخاطر، وبالمثل يجب أن تقوم إدارة المجلس من جهتها بتعهيد أنشطة مراجعة أمن المعلومات للمقيمين الأكفاء سواء كانوا داخليين أو من الأطراف الخارجية في أي وقت، على سبيل المثال لمعالجة الأسباب الجذرية للحوادث الأمنية.

11-8 مراجعة الالتزامات الفنية

يجب مراجعة أنظمة تكنولوجيا المعلومات الخاصة بالمجلس بصورة دورية لضمان الالتزام بالمعايير والسياسات الأمنية الفنية والذي يشمل فحص أنظمة التشغيل لضمان تطبيق أدوات التحكم بالأجهزة والبرامج بالصورة السليمة.

11-9 تدقيق أدوات التحكم بأنظمة المعلومات

يجب مراجعة والتدقيق في أنظمة وعمليات وأدوات التحكم في تكنولوجيا المعلومات بواسطة مدققين مستقلين وأكفاء وفقاً لمعايير وإجراءات التدقيق المعمول بها.

11-10 حماية أدوات التدقيق في أنظمة المعلومات

يجب حماية أدوات التدقيق والبرامج والبيانات ذات الصلة بالتدقيق من الوصول غير المصرح به بغرض منع أية إساءة استخدام أو تهديد.