السياسة العامة لأمن المعلومات

في

الوزارات والمؤسسات الحكومية

Gaza Tel. +970 8 2829262/3 Fax +970 8 2829450 http://www.gcc.gov.ps Email gcc@gov.ps
غزة تلفون +970 8 2829262/3 فاكس +970 8 2829450

جدول المحتويات

Gaza Tel. +970 8 2829262/3 Fax +970 8 2829450 http://www.gcc.gov.ps Email gcc@gov.ps
غزة تلفون +970 8 2829262/3 فاكس +970 8 2829450

سياسة أمن المعلومات

الهدف

تشكل هذه الوثيقة الأساس للسياسة العامة لأمن المعلومات في جميع الوزارات والمؤسسات الحكومية الواجب إتباعها، بحيث تلائم درجات الموظفين ومهامهم المختلفة في الإدارات والدوائر والأقسام حيث أنها تشمل كافة الموظفين دون استثناء.

لتسهيل وتسريع عملية قراءة السياسة العامة كل حسب تخصصه ومجاله تم إضافة هامش لنهاية كل سياسة لتحديد الفئة المستهدفة من هذه السياسة.

الهوامش على ثلاث مستويات كالتالي:

[م] موظفي الفئة العليا والأولى
[ت] موظفي تكنولوجيا المعلومات وأمن المعلومات
[ظ] كافة الموظفين

ليس إلزاما على كل الموظفين قراءة جميع السياسات وإنما فقط السياسات المتعلقة بهم.

مجالات تطبيق السياسة الأمنية لنظم المعلومات

تتناول هذه الوثيقة اعتبارات الأمن في المجالات الثمانية التالية :

1. المسؤوليات الإدارية.
2. الأمن المادي.
3. أمن تحكم الدخول.
4. أمن المعلومات.
5. أمن التطبيقات.
6. أمن الاتصال و الشبكات.
7. تقييم وتدقيق المخاطر الأمنية.
8. إدارة الأحداث الأمنية.

التعريفات

المصطلح	التعريف
أ. نظام المعلومات	نظام معلومات الكتروني يقوم بمعالجة البيانات الكترونيا من خلال استخدام تكنولوجيا المعلومات -- ومنها على سبيل المثال لا الحصر : أنظمة الحاسوب ، الخوادم ، أجهزة الحاسوب ، وسائط التخزين ، وأجهزة الاتصالات و موارد الشبكة.
ب. السرية / الخصوصية	الأشخاص المصرح لهم فقط يمكنهم الوصول إلى المعلومات المخزنة أو المعالجة من خلال نظم المعلومات.
ت. سلامة المعلومات	الأشخاص المصرح لهم فقط يمكنهم إجراء تغييرات على المعلومات المحفوظة أو المعالجة من خلال نظم المعلومات.
ث. إتاحة نظم المعلومات	نظم المعلومات ينبغي أن تكون متاحة للمستخدمين، في أي فترة زمنية محددة.
ج. السياسة الأمنية لتكنولوجيا المعلومات	قائمة التعليمات الإدارية التي تصف الاستخدام السليم والإدارة للحاسوب وموارد الشبكة بغرض حماية هذه الموارد وكذلك المعلومات المحفوظة أو المعالجة من خلال نظم المعلومات من أي تعديل أو تدمير أو وصول غير مصرح به .
ح. معلومات مصنفة	يشير إلى فئات من المعلومات التي صنفت وفقا لأنظمة الأمن.
خ. الموظفون	الأفراد الذين يعملون في الحكومة بغض النظر عن الفترة والوظيفة.
د. مركز البيانات	مركز رئيسي لمعالجة البيانات يضم نظم المعلومات والمعدات ذات الصلة. وهناك عادة وحدة داخل المركز تعمل على استقبال الطلبات المتعلقة بالعمل و إصدار النتائج من و إلى المستخدمين.
ذ. غرفة الحاسوب	غرفة مخصصة لاستضافة معدات الحاسوب.
ر. الشيفرات الخبيثة	البرامج التي تؤدي إلى آثار غير مرغوب فيها على نظم المعلومات. أمثلة على الشيفرات الخبيثة: فيروسات الكمبيوتر، ديدان الشبكة ، حصان طروادة

	الخ...

1. المسؤوليات الإدارية

1.1. الإدارات العامة والدوائر

1.1.1. يتم مراجعة سياسات أمن المعلومات والمعايير و التعليمات والإجراءات بشكل دوري. [م]

1.1.2. تضمن الإدارات أن الحماية الأمنية تكون متكيفة ومتجاوبة مع تغيرات البيئة والتكنولوجيا. [م]

1.1.3. تضمن الإدارات وجود بند مالي في الموازنة لتغطية احتياجات ومصادر الحماية الأمنية الضرورية. [م]

1.1.4. تضمن الإدارات حفظ وصيانة مخزون العتاد المادي والبرمجيات وعقود الصيانة والضمانات سارية المفعول بعناية و بشكل سليم. [م]

1.1.5. يجب أن تطبق الإدارات سياسة فعالة للفصل بين المهام والواجبات لتجنب تنفيذ كل المهام الأمنية بشكل فردي. [م]

1.1.6. تلتزم الإدارات بمنح الموظفين أقل الصلاحيات اللازمة على موارد نظم المعلومات بما يضمن سير العمل. [م]

1.1.7. تضمن الإدارات سرية وسلامة وتوفر المعلومات وغيرها من الجوانب الأمنية لنظم المعلومات الخاضعة لسيطرتها بما يشمل أنظمة المعلومات المدارة من جهات خارجية. [م]

1.1.8. أمن المعلومات هو مسؤولية كل موظف في الحكومة. وعلى هذا النحو يجب أن تضمن الإدارات تثقيف الموظفين حول السياسة الأمنية لتكنولوجيا المعلومات وتعزيز الوعي الأمني لديهم. [م]

1.1.9. يجب على الإدارات نشر وتطبيق السياسة الأمنية الخاصة بتكنولوجيا المعلومات بما يتواءم مع السياسة الأمنية العامة المتبعة. [م]

1.1.10. يجب على الإدارات إعلام الموظفين بأنهم في حالة مخالفة بنود السياسة الأمنية المطبقة قد يتعرضون لإجراءات تأديبية، ويختلف مستوى هذه الإجراءات التأديبية حسب خطورة المخالفة. [م]

1.1.11. يجب على الإدارات إعلام الموظفين المؤقتين أنه في حال انتهاك السياسة العامة لأمن المعلومات قد يتعرضون لإنهاء عقودهم وذلك تبعا لشدة الانتهاك. [م]

1.1.12. الموظفون الذين لهم حق الوصول غير المراقب إلى نظم المعلومات والموارد يجب اختيارهم بعناية وأن يكونوا على علم ووعي بالمسئوليات والواجبات الملقاة على عاتقهم، ويجب أن يتم إبلاغهم رسميا بمستوى التخويل الممنوح لهم للوصول إلى نظم المعلومات. [م]

1.1.13. يجب تعليم وتدريب الموظفين ، لتمكينهم من الاطلاع على مسؤولياتهم وأداء واجباتهم بما يخص أمن تكنولوجيا المعلومات. [م]

1.1.14. يجب على الإدارات إعلام الموظفين بمسؤولياتهم فيما يخص أمن تكنولوجيا المعلومات من بداية تعيينه وطوال فترة عمله في الحكومة بشكل دوري. [م]

1.1.15. الموظفون الذين يعالجون أو يتعاملون مع أنظمة معلومات مصنفة يجب عليهم إجتياز معايير الأمانة والاستقامة وذلك كشرط للتعيين، ونوع الفحص ومستواه(فحص موسع , عادي) يجب أن يتناسب مع مستوى حساسية المعلومات التي سوف يتعامل معها. [م]

1.2 . الجهات الخارجية

1.2.1. يجب أن يتقيد مزودو الخدمات الخارجية أو البرامج التجارية بسياسة أمن تكنولوجيا المعلومات في الإدارات أو أي من متطلبات أمن المعلومات التي تصدرها الحكومة. [م]

1.2.2. يجب على الإدارات مراقبة ومراجعة معايير أمن المعلومات المقدمة من مزودي الخدمات والبرامج التجارية لكي تتأكد من إدارتها بشكل صحيح. [م]

1.2.3. يجب أن يخضع المستشارون الخارجيون والمتعاقدون والموظفون المنتدبون والمؤقتون الذين يعملون مع الحكومة لنفس المتطلبات و المسؤوليات الخاصة بأمن تكنولوجيا المعلومات وتبعاتها كموظفي الحكومة تماما. [م]

1.3 . إدارة الأزمات

1.3.1. يجب توثيق خطط الاستجابة للطوارئ والكوارث المتعلقة بأنظمة المعلومات الهامة وتختبر بشكل دوري ومن ثم دمجها مع خطة استمرارية العمل. [م] [ت]

2. الأمن المادي

2.1 . البيئة

2.1.1. يجب وضع خطة قياسية تراعي المعايير الأمنية عند اختيار مكان مركز الحاسوب ، مع وضع مرجعيه لهذه المعايير تلزم الإدارات. [م] [ت]

2.1.2. مراكز البيانات وغرف الحاسوب يجب أن تكون مؤمنة جيدا من ناحية الأمن المادي ومحمية من الكوارث والتهديدات الأمنية ، سواء الطبيعية أو الناجمة عن أسباب أخرى، من أجل تقليل حجم الخسائر ومدة التعطيل. [م] [ت]

2.1.3. يجب وضع وسائط النسخ الاحتياطي التي تحتوي على المعلومات الأساسية أو الحساسة على مسافة آمنة من الموقع الرئيسي من أجل تفادي الأضرار الناجمة عن كارثة في الموقع الرئيسي. [ت] [م]

2.1.4. مراكز البيانات وغرف الحاسوب يجب أن تكون مطابقة لمستوى أمني محدد و إذا كان نظام المعلومات الموجود يتطلب التعامل مع معلومات سرية فيجب أن يتوافق مع مستوى أمني أعلى لضمان سرية المعلومات. [م] [ت]

2.2 . أمن المعدات

2.2.1. جميع نظم المعلومات يجب أن توضع في بيئة آمنة أو بحضور الموظفين المخولين لمنع الوصول غير المسموح به. [ت]

2.2.2. يجب على الموظفين الذين في عهدتهم كمبيوتر محمول ، أو المساعد الرقمي الشخصي ، أو أجهزة الحوسبة النقالة لأغراض العمل أن يراعوا المعايير الأمنية للحفاظ على هذه المعدات. [ظ]

2.3 . التحكم في الوصول المادي

2.3.1. يجب أن يكون هناك قائمة بأسماء الأشخاص المسموح لهم بالوصول إلى مراكز البيانات وغرف الكمبيوتر وما شابه، وهذه القائمة يجب أن تراجع وتحدث بشكل دوري. [م] [ت]

2.3.2. يجب أن يكون جميع مفاتيح الوصول ، بطاقات الأمان ، كلمات السر ، الخ ... ، اللازمة للدخول إلى أي من أنظمة الكمبيوتر والشبكات مؤمنة ضمن إجراءات أمنية محددة جيدا وصارمة. [م] [ت]

2.3.3. يجب مراقبة جميع الزائرين لمراكز البيانات أو غرف الحاسوب طوال الوقت من قبل موظف حكومي مخول . [ت]

2.3.4. يجب تفعيل خاصية الحماية التلقائية (كلمة سر شاشة التوقف المحمية ، وقفل لوحة المفاتيح) في الخوادم ومحطات الحاسوب ، ومحطات العمل أو الحواسيب الصغيرة إذا لم يكن هناك أي نشاط لمدة محددة مسبقا من الوقت لمنع الوصول إلى النظام بطريقة غير مشروعة.و يجب إنهاء دورة تسجيل الدخول والاتصال إذا اقتضى الأمر ، قبل تركهم العمل ليوم أو أكثر. [ظ] [ت]

2.3.5. يجب على كل موظف له غرفة منفصلة وتحتوي على نظام معلومات معين قفل الباب عند مغادرة هذه الغرفة. [ظ]

2.3.6. يجب أن توضع شاشات العرض الخاصة بطريقة لا تسمح لغير المخولين برؤيتها.[ظ] [ت]

3. أمن تحكم الدخول

3.1. التحكم بالوصول للبيانات

3.1.1. لا يجوز الوصول إلى المعلومات إلا بإذن من أصحاب المعلومات ذات الصلة. [ظ] [ت]

3.1.2. تمنح حقوق الوصول إلى البيانات للمستخدمين على أساس الحاجة. [ظ] [ت]

3.1.3. يجب أن تكون حقوق الوصول إلى البيانات محددة تحديدا واضحا ويتم مراجعتها بشكل دوري. [ت]

3.1.4. الوصول إلى نظم المعلومات المصنفة – مستوى خاص فما أعلى– يجب أن تقيد بطرق التحكم المنطقي للوصول. [ت]

3.2. التحقق من الشخصية

3.2.1. لا يسمح بالوصول إلى معلومات مصنفة بدون تحقق مناسب من الشخصية. [ظ] [ت]

3.2.2. يجب أن يتم التحقق من الشخصية على نحو يتناسب مع حساسية المعلومات المراد الوصول إليها. [ت]

3.2.3. يجب مراقبة محاولات الدخول المتتابعة وغير الناجحة. [ت]

3.3. الخصوصية

3.3.1. تحتفظ الإدارة بحقها بفحص جميع المعلومات المخزنة أو المرسلة عبر أنظمة المعلومات الحكومية مع مراعاة القوانين المحلية للخصوصية. [ظ] [م]

3.4. تحديد الهوية

3.4.1. يجب أن يكون لكل موظف اسم مستخدم وحيد ويجب أن لا يكون هناك اسم مستخدم مشترك إلا بإذن خاص من الموظف الحكومي المختص بأمن المعلومات. [ظ] [ت]

3.4.2. المستخدم مسؤول عن جميع الأنشطة التي يقوم بها من خلال اسم المستخدم الخاص به. [ظ]

3.5. إدارة امتيازات المستخدم

3.5.1. يجب تعطيل جميع الحسابات بعد فترة محددة سلفا من خمولها. [ت] [م]

3.5.2. يجب مراجعة امتيازات المستخدم دوريا. [ت]

3.5.3. في حال انتقال او استقالة الموظف من الحكومة، يجب إلغاء جميع الامتيازات المتعلقة بنظم المعلومات فورا. [م] [ت] [ظ]

3.5.4. يجب أن يتم تحديد ومراقبة استخدام الامتيازات الخاصة بالموظفين. [ت]

3.6. إدارة كلمات المرور

3.6.1. يجب على الإدارات تحديد سياسة صارمة لكلمة المرور كتحديد الحد الأدنى لطول هذه الكلمة، طبيعة اختيار الكلمات، مدة استخدام الكلمة، بالإضافة إلى وجود إرشادات توضح كيفية اختيارها. [ت]

3.6.2. يمنع مشاركة كلمات المرور بين الموظفين أو إفشاء سريتها إلا عند الضرورة لأن هذا يزيد من احتمالية انتهاك أمن المعلومات، و إذا كان لابد من مشاركة كلمات المرور في بعض الأحيان فلابد من أخذ الإذن المسبق من إدارة أمن المعلومات بالإضافة إلى أنه

يجب تغييرها بشكل دوري و عند انتهاء الحاجة لمشاركة كلمة المرور لابد من تغييرها فورا. [ظ] [ت]

3.6.3. عند تخزين كلمات المرور يجب حمايتها و يجب تشفير كلمات المرور عند انتقالها خلال وسائل اتصال غير موثوقة، وفي حال عدم القدرة على تطبيق تقنية التشفير يجب تطبيق وسائل تحكم للحد من تعرض نظم المعلومات للمخاطر والوصول بها إلى مستوى مقبول. [ت]

3.6.4. يحظر على الموظفين التقاط كلمات المرور أومفاتيح التشفير ، أو أي آلية أخرى لمراقبة الوصول ، والتي يمكن أن تؤدي إلى الوصول غير المصرح به. [ظ]

3.6.5. يجب تغيير جميع كلمات المرور الافتراضية لأي نظام من نظم المعلومات عند تشغيله واستخدامه بشكل رسمي. [ظ] [ت]

3.6.6. يجب تغير كلمات المرور فورا إذا اشتبه بأنها مخترقة، أو عند الكشف عنها للفنيين من أجل الصيانة والدعم. [ظ] [ت]

3.7. الوصول إلى الشبكة

3.7.1. يحظر إضافة أي قسم لأي نظام معلومات إلا بموافقة مسبقة من دائرة أمن المعلومات مع مراعاة المحافظة على مستوى مناسب من أمن المعلومات. [ت]

3.8. توثيق الأحداث

3.8.1. يجب على الإدارات تحديد سياسة ذات علاقة بتوثيق وتسجيل أنشطة نظم المعلومات التابعة لها وفقا لاحتياجات العمل ، وتصنيف البيانات. [م] [ت]

3.8.2. أي توثيق للأحداث يجب أن يحتوي على معلومات كافية عند الرجوع إليه لمراجعة مستوى فعالية أمن النظام . [ت]

3.8.3. يجب الاحتفاظ بسجلات التوثيق لفترة تتناسب مع استعمالها كأداة لمراجعة الأحداث، ويجب مراعاة أن تكون هذه السجلات مؤمنة بحيث لا يمكن تعديلها ، ويمكن الاطلاع عليها من قبل الأشخاص المخولين فقط. [ت]

3.8.4. يجب عدم توثيق أي معلومات غير ضرورية. [ت]

3.8.5. يجب مراجعة سجلات التوثيق بشكل دوري خاصة المتعلقة بالتطبيقات وأنظمة التشغيل، وعند الشك بوجود ثغرة أمنية يجب توثيقها وعمل تقرير عنها. [م] [ت] [ظ]

3.8.6. يجب أن يكون هناك تزامن بالتوقيت بين جميع أنظمة المعلومات. [ت]

4. أمن المعلومات

4.1 . خصوصية البيانات

4.1.1. لا يجوز الكشف عن المعلومات المتعلقة بنظم المعلومات التي يمكن أن تمس أمن تلك النظم للمستخدمين أو أي أطراف أخرى إلا على أساس مبدأ الحاجة للمعرفة و بأذن مسبق من إدارة تكنولوجيا المعلومات. [ت]

4.1.2. يجب على الموظفين عدم الإفصاح لأي شخص عن أي معلومات تتعلق بالأفراد أو الأقسام أو الطرق المحددة المستخدمة لمعرفة نقاط الضعف لنظام معين أو أي أنظمة خاصة قد تعرضت للإتلاف بسبب الجرائم أو التجاوزات الحاسوبية باستثناء أولئك الذين يتعاملون مع الحدث ويتحملون مسئولية الأمن لتلك الأنظمة أو المحققين المخولين بالتحقيق بتلك الجرائم. [ظ]

4.1.3. يجب على الموظفين أن لا يفصحوا للأشخاص غير المصرح لهم عن طبيعة وموقع أنظمة المعلومات ولا عن أنظمة الرقابة المستخدمة أو الطرق التي تنفذ بها. [ظ]

4.1.4. يجب تشفير جميع المعلومات التي تصنف تصنيفا خاصا. [ظ] [ت]

4.1.5. يجب على الإدارات الالتزام بأمن أنظمة المعلومات كافة وعدم الاقتصار على تخزين ونقل ومعالجة وإتلاف المعلومات المصنفة. [ظ][ت][م]

4.1.6. يجب مراعاة الخصوصية عند التعامل مع البيانات الشخصية للموظفين.[ظ][ت][م]

4.2 . النسخ الاحتياطي

4.2.1. يجب توثيق آليات النسخ الاحتياطي والاسترداد على أن تفحص بشكل دوري وتنفذ بشكل سليم. [ت]

4.2.2. يجب أن يتم تنفيذ النسخ الاحتياطي على فترات منتظمة. [ت]

4.2.3. يجب أن يتم مراجعة نشاطات النسخ الاحتياطي بشكل منتظم. [ت]

4.2.4. يجب حفظ نسخ النسخ الاحتياطي في مكان بعيد عن موقع النظام على أن تكون محمية بشكل جيد، كما أن الوسائل المستخدمة في النسخ الاحتياطي أثناء النقل يجب أن تكون محمية من الأشخاص غير المصرح لهم بالوصول أو الاستخدام الخاطئ أو الإتلاف. [ت]

عام التعليم الفلسطيني

5. أمن التطبيقات

5.1. تطوير وصيانة التطبيقات

5.1.1. يجب على فريق تطوير التطبيقات امتلاك الخطط الأمنية وتنفيذ التدابير الأمنية والضوابط المناسبة للنظام قيد التطوير وفقا للمتطلبات الأمنية للنظام. [ت]

5.1.2. يجب أن تصان الوثائق وقوائم التطبيقات بشكل سليم على أن تقيد وفق معايير الحاجة للمعرفة. [ت]

5.1.3. يجب مراجعة وفحص وسائل الرقابة الأمنية قبل تنفيذها. [ت]

5.1.4. يجب الحفاظ على سلامة التطبيقات في ظل ضوابط أمنية ملائمة مثل آلية التحكم في الإصدار والفصل بين بيئات التطوير والاختبار والتشغيل. [ت]

5.1.5. لا يجب السماح لفريق تطوير التطبيق بالوصول إلى البيانات إلا للضرورة. [ت]

5.2. إدارة الإعدادات والتحكم بها.

5.2.1. يجب توثيق آليات رقابة التغيير، لطلب وقبول التغيير في البرنامج أو النظام. [ت]

5.2.2. يجب الأخذ بعين الاعتبار التغيرات الواقعة على آليات الحماية الأمنية الحالية. [ت]

5.2.3. يجب مراقبة ومراجعة تركيب جميع المعدات والبرمجيات الحاسوبية. [ت]

5.2.4. يجب أن تكفل الإدارات إبلاغ الفريق بشكل رسمي بأثر التغييرات الأمنية و استخدام نظم المعلومات. [ت] [ظ]

6. أمن الاتصال و الشبكات

6.1 . حماية الشبكة

6.1.1. يمنع نشر عناوين وإعدادات أنظمة الشبكة الداخلية دون موافقة الجهة المعنية. [ت]

6.1.2. يجب حماية جميع الشبكات الداخلية المتصلة مع شبكة حكومية أو شبكة عامة أخرى بشكل صحيح. [ت]

6.1.3. يجب أن تكون التدابير الأمنية فعالة لمنع الوصول غير المصرح به عن بعد إلى النظم والبيانات. [ت]

6.1.4. يمنع الموظفون الموصولة أجهزتهم بالشبكة الداخلية من الاتصال بأي شبكة خارجية بأي شكل من الأشكال إلا بموافقة الجهة المختصة. [ظ]

6.1.5. لا يجوز للموظفين ربط أي جهاز نظم معلومات غير مصرح به إلى الشبكة الحكومية دون الحصول على موافقة الجهة المختصة. [ظ]

6.1.6. يجب أن يتم مراجعة إعدادات وإدارة أنظمة الاتصال والمعلومات بشكل دوري. [ت]

6.1.7. يجب أن لا تؤثر عملية الاتصال مع أي شبكة أخرى على المعايير الأمنية لطرفي الاتصال. [ت]

6.1.8. يمنع توصيل الموارد الحاسوبية الخاصة المملوكة للموظفين بالشبكة الداخلية للحكومة من دون إذن مسبق من دائرة أمن الشبكات، وتكفل الإدارات استخدام هذه الموارد الشخصية بمعايير مطابقة لسياسة أمن تكنولوجيا المعلومات. [ظ]

6.1.9. يجب تشفير المعلومات المصنفة تصنيفا خاصا عند نقلها من خلال اتصال خارجي غير آمن. [ت] [ظ]

6.1.10. يجب تشفير المعلومات المصنفة تصنيفا عالي السرية عند نقلها داخل الشبكة المحلية على أن تكون آلية التشفير متوافقة مع سياسة أمن تكنولوجيا المعلومات . [ت] [ظ]

6.2 . أمن الإنترنت

6.2.1. يجب أن تكون جميع طرق الوصول إلى الإنترنت إما عن طريق مركزية لبوابات الإنترنت أو من خلال بوابة الإنترنت الخاصة بالدائرة بما يتماشى مع المعايير الأمنية. في الظروف التي لا يكون هذا ممكنا، أو بالنظر إلى طريقة الاستخدام، قد ينظر في السماح للإدارات الوصول إلى الإنترنت من خلال أجهزة قائمة بذاتها، شريطة أن تكون هناك موافقة، مع وجود آلية مناسبة للرقابة. [ت]

6.2.2. ينبغي على الإدارات أن تنظر في الفائدة من حجب بعض المواقع غير الخاصة بالعمل. مع الأخذ بعين الاعتبار أن عدم فلترة بعض المواقع لا يعني السماح للموظف بتصفح تلك المواقع. [م] [ت] [ظ]

6.2.3. يجب أن يوضح كل قسم للمستخدمين سياسته في ما يتعلق بالاستخدام المقبول للإنترنت.[م]

6.2.4. يجب أن يتم الفحص والتحقق من جميع البرامج والملفات التي تم تحميلها من شبكة الإنترنت باستخدام البرمجيات المضادة للفيروسات. [ت] [ظ]

6.2.5. لا يجوز للموظفين تنفيذ أي برنامج تم تحميله من شبكة الإنترنت ما لم يكن من مصدر موثوق به. [ظ]

6.3 . أمن البريد الإلكتروني

6.3.1. يجب على كل إدارة أن توضح سياستها للموظفين بشكل واضح فيما يتعلق بالاستخدام المقبول للبريد الالكتروني. [م]

6.3.2. يجب على مسئولي الأنظمة إنشاء عملية منهجية للتسجيل والاحتفاظ وحذف رسائل البريد الالكتروني والسجلات المرفقة بها. [ت]

6.3.3. يجب فحص الرسائل الصادرة والواردة للبريد الالكتروني من الفيروسات وأي ملفات مشبوهة. [ت] [ظ]

6.3.4. يجب حماية عناوين البريد الداخلية أو التي تحتوي على المواقع الحكومية من التعديل أو الوصول غير المصرح به. [ت]

6.3.5. يجب نقل البريد الالكتروني الذي يحتوي على معلومات سرية عبر نظام معلوماتي مصرح به ومصدق عليه من مسئول الأمن الحكومي. كما ويجب نقل البريد الالكتروني الذي يحتوي على معلومات مصنفة تصنيفا عالي السرية كما هو موضح في 6.1.10. [ظ]

6.3.6. يمنع فتح أو إعادة توجيه رسائل البريد الإلكتروني المرسلة من مصادر مشبوهة. [ظ]

6.4 . الحماية ضد فيروسات الكمبيوتر والشيفرات الخبيثة

6.4.1. يجب أن تكون البرمجيات المضادة للفيروسات مفعلة دائما على جميع الخوادم والأجهزة في الشبكة المحلية، وأيضا على الأجهزة التي تتصل عن بعد بالشبكة الحكومية الداخلية. [ت] [ظ]

6.4.2. يجب على الإدارات حماية أنظمة المعلومات الخاصة بها من الفيروسات و الشيفرات الخبيثة، كما ويجب تحديث برامج مضادات الفيروسات بشكل دوري وكلما كان ذلك ضروريا. [ت] [ظ]

6.4.3. يمنع استخدام وسائط التخزين والملفات من المصادر مجهولة الأصل إلا بعد فحصها وتنظيفها من الفيروسات و الشيفرات الخبيثة. [ظ]

6.4.4. يمنع المستخدمون من كتابة أو تشغيل أو نسخ أو نشر فيروسات الكمبيوتر أو الشيفرات الخبيثة. [ظ]

6.4.5. يجب على الإدارات أن تنفذ تدابير مناسبة لحماية أجهزة الاتصال اللاسلكية أو الأجهزة الحاسوبية المتنقلة من الفيروسات و الشيفرات الخبيثة. [ت] [ظ]

6.5 . إدارة البرمجيات وملفات التصحيح

6.5.1. يجب فقط تشغيل البرمجيات موثوقة المصدر على أجهزة الكمبيوتر والشبكات .[ظ]

6.5.2. يمنع تشغيل البرامج غير المصرح بها على أنظمة المعلومات الحكومية بدون إذن مسبق من مسئول الدائرة. [ت] [ظ]

6.5.3. يجب على الإدارات حماية أنظمة المعلومات من نقاط الضعف المعروفة عن طريق تطبيق أحدث الرقع الأمنية الموصى بها من مزودي منتجات أنظمة المعلومات أو تنفيذ تدابير أمنية تعويضية. [ت] [ظ]

6.5.4. يجب إجراء تقييم للمخاطر وعمل اختبار قبل تطبيق تصحيحات نظم الأمان، لتقليل الآثار السلبية وغير المرغوب بها على أنظمة المعلومات. [ت] [ظ]

6.6 . أمن الشبكة اللاسلكية

6.6.1. يجب على الإدارات توثيق ومراقبة والتحكم في الشبكات اللاسلكية المتصلة بشبكة الحكومة الداخلية. [ت]

6.6.2. يجب إتباع الضوابط الأمنية السليمة من توثيق الدخول واستخدام التشفير لحماية البيانات المنقولة عبر الشبكات اللاسلكية المتصلة مع شبكة الحكومة الداخلية. [ت] [ظ]

7. تقييم وتدقيق المخاطر الأمنية

7.1. تقييم المخاطر الأمنية

7.1.1. يجب أن يتم تقييم المخاطر الأمنية لنظم المعلومات والتطبيقات مرة واحدة كل عامين على الأقل، على أن يتم انجاز تقييم المخاطر الأمنية قبل التحسينات والتغييرات الرئيسية المرتبطة بتلك النظم والتطبيقات. [ت]

7.1.2. يجب أن يكون استعمال البرمجيات المستخدمة لتحليل تقييم المخاطر الأمنية مقيدة ومضبوطة. [ت]

7.2. التدقيق الأمني

7.2.1. يجب أن يتم تقييم نظم المعلومات دوريا من قبل مدققين من طرف مستقل وموثوق به، وذلك لتحديد الحد الأدنى من الضوابط اللازمة لتقليل المخاطر الأمنية إلى مستوى مقبول. [ت]

7.2.2. يجب أن يتم مراجعة مدى الامتثال لسياسات أمن الشبكات والحاسوب بشكل دوري. [ت]

7.2.3. يجب أن يتم تقييد وضبط استعمال البرمجيات المستخدمة لتحليل التدقيق الأمني. [ت]

8. إدارة الأحداث الأمنية

8.1 . مراقبة الأحداث الأمنية

8.1.1. يجب على الإدارات إنشاء آلية لتحديد الحوادث ومراقبتها بهدف احتواء ومنع الحوادث الأمنية. [م]

8.1.2. يجب أن تكفل الإدارات أن سجلات النظام ومعلومات الدعم الأخرى محفوظة لغرض إثبات و تتبع الحوادث الأمنية فقط. [ت]

8.2 . الاستجابة للحوادث الأمنية

8.2.1. يجب على الإدارات أن تنشئ و توثق وتحفظ خطوات معالجة الحوادث الأمنية لأنظمة المعلومات التابعة لها. [ت]

8.2.2. يجب على الموظفين معرفة و إتباع خطوات معالجة الحوادث الأمنية الموثقة. . [م]

8.2.3. يجب الإبلاغ فورا عن جميع أعطال الشبكة أو أنظمة البرمجيات ، والتحذيرات والتنبيهات ومناطق الضعف المشتبه بها لأمن المعلومات ، وما شابه ذلك ، ومشاكل أمن الشبكة المحتملة، إلى الطرف المسؤول وفقا لإجراءات التعامل مع الأحداث الأمنية. [ت] [ظ]

8.2.4. يجب إجراء خطوات فورية في حالة وجود احتمال اختراق النظام وفقا لخطوات معالجة الحوادث الأمنية الموثقة. [ت]