**السياسة العامة ألمن المعمومات**

**في**

**الو از ارت والمؤسسات الحكومية**

**Gaza**

Tel. +970 8 2829262/3

Fax +970 8 2829450

I

[http://www.gcc.gov.ps](http://www.gcc.gov.ps/) Email [gcc@gov.ps](mailto:gcc@gov.ps)

+970 8 2829262/3

+970 8 2829450

تمفون فاكس

**غزة**

# جدول المحتويات

**سياسة أمن المعمومات** **3**

[**مجاالت تطبيق السياسة األمنية لنظم المعمومات** **4**](#_bookmark0)

[**5............................................................................................................................................................**](#_bookmark1)

[**المسؤوليات اإلدارية** **6**](#_bookmark2)

[**اإلدا ارت العامة والدوائر** 5](#_bookmark3)

[**الجهات الخارجية** 7](#_bookmark4)

[**إدارة األزمات** 7](#_bookmark5)

[**األمن المادي** **9**](#_bookmark6)

[**البيئة** 8](#_bookmark7)

[**التعريفات**](#_bookmark1)

[**1**](#_bookmark2)

[**1.1**](#_bookmark3)

[**1.2**](#_bookmark4)

[**1.3**](#_bookmark5)

[**2**](#_bookmark6)

[**2.1**](#_bookmark7)

[**أمن المعدات** 8](#_bookmark8)

[**2.2**](#_bookmark8)

[**التحكم في الوصول المادي** 01](#_bookmark9)

[**أمن تحكم الدخول** **11**](#_bookmark10)

[**التحكم بالوصول لمبيانات** 00](#_bookmark11)

[**التحقق من الشخصية** 00](#_bookmark12)

[**الخصوصية** 00](#_bookmark13)

[**تحديد الهوية** 01](#_bookmark14)

[**إدارة امتيا ازت المستخدم** 01](#_bookmark15)

[**إدارة كممات المرور** 01](#_bookmark16)

[**الوصول إلي الشبكة** 02](#_bookmark17)

[**توثيق األحداث** 02](#_bookmark18)

[**أمن المعمومات** **15**](#_bookmark19)

[**خصوصية البيانات** 04](#_bookmark20)

[**النسخ االحتياطي** 05](#_bookmark21)

[**أمن التطبيقات** **17**](#_bookmark22)

[**تطوير وصيانة التطبيقات** 06](#_bookmark23)

[**إدارة اإلعدادات والتحكم بها** 06](#_bookmark24)

[**أمن االتصال و الشبكات** **18**](#_bookmark25)

[**حماية الشبكة** 07](#_bookmark26)

[**أمن اإلنترنت** 08](#_bookmark27)

[**أمن البريد اإللكتروني** 11](#_bookmark28)

[**الحماية ضد فيروسات الكمبيوتر والشيف ارت الخبيثة** 11](#_bookmark29)

[**إدارة البرمجيات وممفات التصحيح** 10](#_bookmark30)

[**أمن الشبكة الالسمكية** 10](#_bookmark31)

[**تقييم وتدقيق المخاطر األمنية** **23**](#_bookmark32)

[**تقييم المخاطر األمنية** 12](#_bookmark33)

[**التدقيق األمني** 12](#_bookmark34)

[**إدارة األحداث األمنية** **24**](#_bookmark35)

[**م ارقبة األحداث األمنية** 13](#_bookmark36)

[**االستجابة لمحوادث األمنية** 13](#_bookmark37)

[**3.2**](#_bookmark9)

[**3**](#_bookmark10)

[**3.1**](#_bookmark11)

[**3.2**](#_bookmark12)

[**3.3**](#_bookmark13)

[**3.4**](#_bookmark14)

[**3.5**](#_bookmark15)

[**3.6**](#_bookmark16)

[**3.7**](#_bookmark17)

[**3.8**](#_bookmark18)

[**4**](#_bookmark19)

[**4.1**](#_bookmark20)

[**4.2**](#_bookmark21)

[**5**](#_bookmark22)

[**5.1**](#_bookmark23)

[**5.2**](#_bookmark24)

[**6**](#_bookmark25)

[**6.1**](#_bookmark26)

[**6.2**](#_bookmark27)

[**6.3**](#_bookmark28)

[**6.4**](#_bookmark29)

[**6.5**](#_bookmark30)

[**6.6**](#_bookmark31)

[**7**](#_bookmark32)

[**7.1**](#_bookmark33)

[**7.2**](#_bookmark34)

[**8**](#_bookmark35)

[**8.1**](#_bookmark36)

[**8.2**](#_bookmark37)

**Gaza**

Tel. +970 8 2829262/3

Fax +970 8 2829450

II

[http://www.gcc.gov.ps](http://www.gcc.gov.ps/) Email [gcc@gov.ps](mailto:gcc@gov.ps)

+970 8 2829262/3

+970 8 2829450

تمفون فاكس

**غزة**

# المعمومات

**سياسة أمن**

### الهدف

الو از ارت والمؤسسات الحكومية الواجب

األساس لمسياسة العامة ألمن المعمومات في جميع

تشكل ىذه الوثيقة

إتباعيا، بحيث تالئم درجات الموظفين ومياميم المختمفة في اإلدا ارت والدوائر واألقسام حيت أنيا تشمل كافة

الموظفين دون استثناء.

لتسييل وتسريع عممية ق ارءة السياسة العامة كل حسب تخصصو ومجالو تم إضافة ىامش لنياية كل

سياسة لتحديد الفئة المستيدفة من ىذه السياسة.

اليوامش عمى ثالث مستويات كالتالي:

[ م ] موظفي الفئة العميا واألولى

وانما فقط السياسات المتعمقة بيم.

[ ت ] موظفي تكنولوجيا المعمومات وأمن المعمومات

[ ظ ] كافة الموظفين ليس إل ازما عمى كل الموظفين ق ارءة جميع السياسات

## مجاالت تطبيق السياسة األمنية لنظم المعمومات

تتناول ىذه الوثيقة اعتبا ارت األمن في المجاالت الثمانية التالية :

.0 المسؤوليات اإلدارية.

.1 األمن المادي.

.2 أمن تحكم الدخول.

.3 أمن المعمومات.

.4 أمن التطبيقات.

.5 أمن االتصال و الشبكات.

.6 تقييم وتدقيق المخاطر األمنية.

.7 إدارة األحداث األمنية.

**التعريفات**

|  |  |
| --- | --- |
| **التعريف** | **المصطمح** |
| نظام معمومات الكتروني يقوم بمعالجة البيانات الكترونيا من خالل استخدام تكنولوجيا المعمومات -- ومنيا عمى سبيل المثال ال الحصر : أنظمة الحاسوب ، الخوادم ، أجيزة الحاسوب ، وسائط التخزين ، وأجيزة  االتصاالت و موارد الشبكة. | أ. نظام المعمومات |
| األشخاص المصرح ليم فقط يمكنيم الوصول إلى المعمومات المخزنة أو  المعالجة من خالل نظم المعمومات. | ب. السرية / الخصوصية |
| األشخاص المصرح ليم فقط يمكنيم إج ارء تغيي ارت عمى المعمومات  المحفوظة أو المعالجة من خالل نظم المعمومات. | ت. سالمة المعمومات |
| نظم المعمومات ينبغي أن تكون متاحة لممستخدمين، في أي فترة زمنية  محددة. | ث. إتاحة نظم المعمومات |
| قائمة التعميمات اإلدارية التي تصف االستخدام السميم واإلدارة لمحاسوب وموارد الشبكة بغرض حماية ىذه الموارد وكذلك المعمومات المحفوظة أو المعالجة من خالل نظم المعمومات من أي تعديل أو تدمير أو وصول غير  مصرح بو . | ج. السياسة األمنية لتكنولوجيا المعمومات |
| يشير إلى فئات من المعمومات التي صنفت وفقا ألنظمة األمن. | ح. معمومات مصنفة |
| األف ارد الذين يعممون في الحكومة بغض النظر عن الفترة والوظيفة. | خ. الموظفون |
| مركز رئيسي لمعالجة البيانات يضم نظم المعمومات والمعدات ذات الصمة. وىناك عادة وحدة داخل المركز تعمل عمى استقبال الطمبات المتعمقة بالعمل  و إصدار النتائج من و إلى المستخدمين. | د. مركز البيانات |
| غرفة مخصصة الستضافة معدات الحاسوب. | ذ. غرفة الحاسوب |
| الب ارمج التي تؤدي إلى آثار غير مرغوب فييا عمى نظم المعمومات. أمثمة عمى الشيف ارت الخبيثة: فيروسات الكمبيوتر، ديدان الشبكة ، حصان طروادة | ر. الشيف ارت الخبيثة |

|  |  |
| --- | --- |
| الخ… |  |

## .1 المسؤوليات اإلدارية

### .1.1اإلدا ارت العامة والدوائر

يتم م ارجعة سياسات أمن المعمومات والمعايير و التعميمات واإلج ارءات بشكل دوري. [

] م

.0.0.0

تضمن اإلدا ارت أن الحماية األمنية تكون متكيفة ومتجاوبة مع تغي ارت البيئة والتكنولوجيا.

[ م ] تضمن اإلدا ارت وجود بند مالي في الموازنة لتغطية احتياجات ومصادر الحماية األمنية

الضرورية. [ م ] تضمن اإلدا ارت حفظ وصيانة مخزون العتاد المادي والبرمجيات وعقود الصيانة

والضمانات سارية المفعول بعناية و بشكل سميم. [ م ] يجب أن تطبق اإلدا ارت سياسة فعالة لمفصل بين الميام والواجبات لتجنب تنفيذ كل الميام

األمنية بشكل فردي. [ م ]

.0.0.1

.0.0.2

.0.0.3

.0.0.4

موارد نظم المعمومات بما

عمى

بمنح الموظفين أقل الصالحيات الالزمة

اإلدا ارت

تمتزم

.0.0.5

يضمن سير العمل. [ م ]

اإلدا ارت سرية وسالمة وتوفر المعمومات وغيرىا من الجوانب األمنية لنظم

تضمن

.0.0.6

بما يشمل أنظمة المعمومات المدارة من جيات خارجية. [

المعمومات الخاضعة لسيطرتيا

]م

أن تضمن

وعمى ىذا النحو يجب

موظف في الحكومة.

مسؤولية كل

أمن المعمومات ىو

.0.0.7

حول السياسة األمنية لتكنولوجيا المعمومات وتعزيز الوعي

الموظفين

اإلدا ارت تثقيف

األمني لدييم. [ م ]

نشر وتطبيق السياسة األمنية الخاصة بتكنولوجيا المعمومات بما

اإلدا ارت

عمى

يجب

.0.0.8

يتواءم مع السياسة األمنية العامة المتبعة. [ م ]

إعالم الموظفين بأنيم في حالة مخالفة بنود السياسة األمنية المطبقة

اإلدا ارت

عمى

يجب

.0.0.01

خطورة

ويختمف مستوى ىذه اإلج ارءات التأديبية حسب

إلج ارءات تأديبية،

قد يتعرضون

المخالفة. [ م ]

في حال انتياك السياسة العامة ألمن

أنو

إعالم الموظفين المؤقتين

اإلدا ارت

عمى

يجب

.0.0.00

المعمومات قد يتعرضون إلنياء عقودىم وذلك تبعا لشدة االنتياك. [ م ]

نظم المعمومات والموارد يجب

الموظفون الذين ليم حق الوصول غير الم ارقب إلى

.0.0.01

عاتقيم،

عمى

عمم ووعي بالمسئوليات والواجبات الممقاة

عمى

اختيارىم بعناية وأن يكونوا

ويجب أن يتم إبالغيم رسميا بمستوى التخويل الممنوح ليم لموصول إلى نظم المعمومات.

[ م ] يجب تعميم وتدريب الموظفين ، لتمكينيم من االطالع عمى مسؤولياتيم وأداء واجباتيم بما

.0.0.02

يخص أمن تكنولوجيا المعمومات. [ م ]

إعالم الموظفين بمسؤولياتيم فيما يخص أمن تكنولوجيا المعمومات

اإلدا ارت

عمى

يجب

.0.0.03

إجتياز

من بداية تعيينو وطوال فترة عممو في الحكومة بشكل دوري. [ م ] الموظفون الذين يعالجون أو يتعاممون مع أنظمة معمومات مصنفة يجب عمييم

.0.0.04

معايير األمانة واالستقامة وذلك كشرط لمتعيين، ونوع الفحص ومستواه( فحص موسع ,

عادي ) يجب أن يتناسب مع مستوى حساسية المعمومات التي سوف يتعامل معيا. [ م ]

### .1.2الجهات الخارجية

.0.1.0 يجب أن يتقيد مزودو الخدمات الخارجية أو الب ارمج التجارية بسياسة أمن تكنولوجيا

المعمومات في اإلدا ارت أو أي من متطمبات أمن المعمومات التي تصدرىا الحكومة. [ م

]

المقدمة من مزودي الخدمات

أمن المعمومات

معايير

م ارقبة وم ارجعة

اإلدا ارت

عمى

يجب

.0.1.1

والب ارمج التجارية لكي تتأكد من إدارتيا بشكل صحيح. [ م ] يجب أن يخضع المستشارون الخارجيون والمتعاقدون والموظفون المنتدبون والمؤقتون الذين يعممون مع الحكومة لنفس المتطمبات و المسؤوليات الخاصة بأمن تكنولوجيا

المعمومات وتبعاتيا كموظفي الحكومة تماما. [ م ]

.0.1.2

### .1.3إدارة األزمات

خطط االستجابة لمطوارئ والكوارث المتعمقة بأنظمة المعمومات اليامة وتختبر

يجب توثيق

.0.2.0

بشكل دوري ومن ثم دمجيا مع خطة استم اررية العمل. [ م ] [ ت ]

## .2 األمن المادي

### .2.1البيئة

يجب وضع خطة قياسية ت ارعي المعايير األمنية عند اختيار مكان مركز الحاسوب ، مع

وضع مرجعيو ليذه المعايير تمزم اإلدا ارت. [ م ] [ ت ]

.1.0.0

األمن المادي

من ناحية

جيدا

يجب أن تكون مؤمنة

م اركز البيانات وغرف الحاسوب

.1.0.1

ومحمية من الكوارث والتيديدات األمنية ، سواء الطبيعية أو الناجمة عن أسباب أخرى،

من أجل تقميل حجم الخسائر ومدة التعطيل. [ م ] [ ت ]

الحساسة

األساسية أو

المعمومات

وسائط النسخ االحتياطي التي تحتوي عمى

يجب وضع

.1.0.2

عمى مسافة آمنة من الموقع الرئيسي من أجل تفادي األض ارر الناجمة عن كارثة في

الموقع الرئيسي. [ ت ] [ م ]

إذا كان

محدد و

أمني

لمستوى

تكون مطابقة

م اركز البيانات وغرف الحاسوب يجب أن

.1.0.3

نظام المعمومات الموجود يتطمب التعامل مع معمومات سرية فيجب أن يتوافق مع مستوى

أمني أعمى لضمان سرية المعمومات. [ م ] [ ت ]

### .2.2أمن المعدات

جميع نظم المعمومات يجب أن توضع في بيئة آمنة أو بحضور الموظفين المخولين لمنع

الوصول غير المسموح بو. [ ت ]

يجب عمى الموظفين الذين في عيدتيم كمبيوتر محمول ، أو المساعد الرقمي الشخصي ،

.1.1.0

.1.1.1

ىذه

عمى

أن ي ارعوا المعايير األمنية لمحفاظ

العمل

أو أجيزة الحوسبة النقالة ألغ ارض

المعدات. [ ظ ]

### .2.3التحكم في الوصول المادي

المسموح ليم بالوصول إلى م اركز البيانات

قائمة بأسماء األشخاص

يجب أن يكون ىناك

.1.2.0

وغرف الكمبيوتر وما شابو، وىذه القائمة يجب أن ت ارجع وتحدث بشكل دوري. [ م ] [ ت]

، ...

الخ

، كممات السر ،

األمان

جميع مفاتيح الوصول ، بطاقات

يجب أن يكون

.1.2.1

مؤمنة ضمن إج ارءات أمنية

لمدخول إلى أي من أنظمة الكمبيوتر والشبكات

الالزمة

محددة جيدا وصارمة. [ م ] [ ت ]

من قبل

طوال الوقت

جميع ال ازئرين لم اركز البيانات أو غرف الحاسوب

يجب م ارقبة

.1.2.2

موظف حكومي مخول . [ ت ]

كممة سر شاشة التوقف المحمية ، وقفل لوحة

الحماية التمقائية (

يجب تفعيل خاصية

.1.2.3

المفاتيح) في الخوادم ومحطات الحاسوب ، ومحطات العمل أو الحواسيب الصغيرة إذا لم

غير

بطريقة

يكن ىناك أي نشاط لمدة محددة مسبقا من الوقت لمنع الوصول إلى النظام

إذا اقتضى األمر ، قبل تركيم

دورة تسجيل الدخول واالتصال

إنياء

يجب

مشروعة.و

العمل ليوم أو أكثر. [ ظ ] [ ت ]

الباب

نظام معمومات معين قفل

عمى

كل موظف لو غرفة منفصمة وتحتوي

عمى

يجب

.1.2.4

عند مغادرة ىذه الغرفة. [ ظ ]

يجب أن توضع شاشات العرض الخاصة بطريقة ال تسمح لغير المخولين برؤيتيا[.ظ]

]ت[

.1.2.5

## .3 أمن تحكم الدخول

### .3.1التحكم بالوصول لمبيانات

] ظ [

ال يجوز الوصول إلى المعمومات إال بإذن من أصحاب المعمومات ذات الصمة.

] ت [

تمنح حقوق الوصول إلى البيانات لممستخدمين عمى أساس الحاجة. [ ظ ] [ ت ]

.2.0.0

.2.0.1

ويتم م ارجعتيا بشكل

البيانات محددة تحديدا واضحا

الوصول إلى

حقوق

تكون

يجب أن

.2.0.2

بطرق

تقيد

يجب أن

مستوى خاص فما أعمى-

المصنفة -

دوري. [ ت ] الوصول إلى نظم المعمومات

.2.0.3

التحكم المنطقي لموصول. [ ت ]

### .3.2التحقق من الشخصية

.2.1.0 ال يسمح بالوصول إلى معمومات مصنفة بدون تحقق مناسب من الشخصية. [ ظ ] [ ت ]

الم ارد

يتناسب مع حساسية المعمومات

عمى نحو

التحقق من الشخصية

يتم

يجب أن

.2.1.1

الوصول إلييا. [ ت ]

يجب م ارقبة محاوالت الدخول المتتابعة وغير الناجحة. [ ت ]

.2.1.2

### .3.3الخصوصية

بفحص جميع المعمومات المخزنة أو المرسمة عبر أنظمة المعمومات

تحتفظ اإلدارة بحقيا

.2.2.0

الحكومية مع م ارعاة القوانين المحمية لمخصوصية. [ ظ ] [ م ]

### .3.4تحديد الهوية

يجب أن يكون لكل موظف اسم مستخدم وحيد ويجب أن ال يكون ىناك اسم مستخدم

مشترك إال بإذن خاص من الموظف الحكومي المختص بأمن المعمومات. [ ظ ] [ ت ]

المستخدم مسؤول عن جميع األنشطة التي يقوم بيا من خالل اسم المستخدم الخاص بو.

] ظ [

.2.3.0

.2.3.1

### .3.5إدارة امتيا ازت المستخدم

يجب تعطيل جميع الحسابات بعد فترة محددة سمفا من خموليا. [ ت ] [ م ]

يجب م ارجعة امتيا ازت المستخدم دوريا. [ ت ]

.2.4.0

.2.4.1

يجب إلغاء جميع االمتيا ازت المتعمقة

في حال انتقال او استقالة الموظف من الحكومة،

بنظم المعمومات فو ار. [ م ] [ ت ] [ ظ ]

.2.4.2

.2.4.3 يجب أن يتم تحديد وم ارقبة استخدام االمتيا ازت الخاصة بالموظفين. [ ت ]

### .3.6إدارة كممات المرور

لطول ىذه

اإلدا ارت تحديد سياسة صارمة لكممة المرور كتحديد الحد األدنى

عمى

يجب

.2.5.0

الكممة، طبيعة اختيار الكممات، مدة استخدام الكممة، باإلضافة إلى وجود إرشادات توضح

كيفية اختيارىا. [ ت ] يمنع مشاركة كممات المرور بين الموظفين أو إفشاء سريتيا إال عند الضرورة ألن ىذا

.2.5.1

يزيد من احتمالية انتياك أمن المعمومات، و إذا كان البد من مشاركة كممات المرور في

أنو

إلى

أمن المعمومات باإلضافة

اإلذن المسبق من إدارة

بعض األحيان فالبد من أخذ

يجب تغييرىا بشكل دوري و عند انتياء الحاجة لمشاركة كممة المرور البد من تغييرىا

فو ار. [ ظ ] [ ت ] عند تخزين كممات المرور يجب حمايتيا و يجب تشفير كممات المرور عند انتقاليا خالل

.2.5.2

يجب تطبيق

القدرة عمى تطبيق تقنية التشفير

وفي حال عدم

وسائل اتصال غير موثوقة،

إلى مستوى مقبول.

والوصول بيا

لمحد من تعرض نظم المعمومات لممخاطر

وسائل تحكم

] ت [

أو أي آلية أخرى لم ارقبة

أومفاتيح التشفير ،

المرور

كممات

التقاط

الموظفين

يحظر عمى

.2.5.3

الوصول ، والتي يمكن أن تؤدي إلى الوصول غير المصرح بو. [ ظ ]

ألي نظام من نظم المعمومات عند تشغيمو

االفت ارضية

المرور

جميع كممات

يجب تغيير

.2.5.4

واستخدامو بشكل رسمي. [ ظ ] [ ت ]

لمفنيين من

الكشف عنيا

عند

يجب تغير كممات المرور فو ار إذا اشتبو بأنيا مخترقة، أو

.2.5.5

] ت [ ] ظ [

أجل الصيانة والدعم.

### .3.7الوصول إلى الشبكة

يحظر إضافة أي قسم ألي نظام معمومات إال بموافقة مسبقة من دائرة أمن المعمومات مع

م ارعاة المحافظة عمى مستوى مناسب من أمن المعمومات. [ ت ]

.2.6.0

### .3.8توثيق األحداث

وتسجيل أنشطة نظم المعمومات

سياسة ذات عالقة بتوثيق

اإلدا ارت تحديد

عمى

يجب

.2.7.0

التابعة ليا وفقا الحتياجات العمل ، وتصنيف البيانات. [ م ] [ ت ]

لم ارجعة

إليو

معمومات كافية عند الرجوع

عمى

أي توثيق لألحداث يجب أن يحتوي

مستوى فعالية أمن النظام . [ ت ]

.2.7.1

األحداث،

كأداة لم ارجعة

مع استعماليا

تتناسب

لفترة

التوثيق

االحتفاظ بسجالت

يجب

.2.7.2

االطالع

ال يمكن تعديميا ، ويمكن

ويجب م ارعاة أن تكون ىذه السجالت مؤمنة بحيث

عمييا من قبل األشخاص المخولين فقط. [ ت ]

يجب عدم توثيق أي معمومات غير ضرورية. [ ت ]

.2.7.3

التشغيل،

يجب م ارجعة سجالت التوثيق بشكل دوري خاصة المتعمقة بالتطبيقات وأنظمة

وعند الشك بوجود ثغرة أمنية يجب توثيقيا وعمل تقرير عنيا. [ م ] [ ت ] [ ظ ]

يجب أن يكون ىناك ت ازمن بالتوقيت بين جميع أنظمة المعمومات. [ ت ]

.2.7.4

.2.7.5

## .4 أمن المعمومات

### .4.1خصوصية البيانات

ال يجوز الكشف عن المعمومات المتعمقة بنظم المعمومات التي يمكن أن تمس أمن تمك النظم لممستخدمين أو أي أط ارف أخرى إال عمى أساس مبدأ الحاجة لممعرفة و بأذن مسبق

من إدارة تكنولوجيا المعمومات. [ ت ]

.3.0.0

الموظفين عدم اإلفصاح ألي شخص عن أي معمومات تتعمق باألف ارد أو

عمى

يجب

.3.0.1

األقسام أو الطرق المحددة المستخدمة لمعرفة نقاط الضعف لنظام معين أو أي أنظمة خاصة قد تعرضت لإلتالف بسبب الج ارئم أو التجاو ازت الحاسوبية باستثناء أولئك الذين يتعاممون مع الحدث ويتحممون مسئولية األمن لتمك األنظمة أو المحققين المخولين

بالتحقيق بتمك الج ارئم. [ ظ ]

الموظفين أن ال يفصحوا لألشخاص غير المصرح ليم عن طبيعة وموقع

عمى

يجب

.3.0.2

أنظمة المعمومات وال عن أنظمة الرقابة المستخدمة أو الطرق التي تنفذ بيا. [ ظ ]

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

.3.0.3

تخزين

عمى

وعدم االقتصار

كافة

اإلدا ارت االلت ازم بأمن أنظمة المعمومات

عمى

يجب

.3.0.4

ونقل ومعالجة واتالف المعمومات المصنفة. [ ظ [] ت [] م ]

.3.0.5 يجب م ارعاة الخصوصية عند التعامل مع البيانات الشخصية لمموظفين[. ظ [] ت [] م ]

### .4.2النسخ االحتياطي

أن تفحص بشكل دوري وتنفذ بشكل

عمى

يجب توثيق آليات النسخ االحتياطي واالسترداد

سميم. [ ت ]

.3.1.0

يجب أن يتم تنفيذ النسخ االحتياطي عمى فت ارت منتظمة. [ ت ]

يجب أن يتم م ارجعة نشاطات النسخ االحتياطي بشكل منتظم. [ ت ]

.3.1.1

.3.1.2

أن تكون محمية

عمى

يجب حفظ نسخ النسخ االحتياطي في مكان بعيد عن موقع النظام

.3.1.3

بشكل جيد، كما أن الوسائل المستخدمة في النسخ االحتياطي أثناء النقل يجب أن تكون

أو االستخدام الخاطئ أو اإلتالف. [

محمية من األشخاص غير المصرح ليم بالوصول

[ت

## .5 أمن التطبيقات

### .5.1تطوير وصيانة التطبيقات

فريق تطوير التطبيقات امتالك الخطط األمنية وتنفيذ التدابير األمنية والضوابط

يجب عمى

.4.0.0

المناسبة لمنظام قيد التطوير وفقا لممتطمبات األمنية لمنظام. [ ت ]

أن تقيد وفق معاير الحاجة

عمى

يجب أن تصان الوثائق وقوائم التطبيقات بشكل سميم

لممعرفة. [ ت ]

.4.0.1

.4.0.2 يجب م ارجعة وفحص وسائل الرقابة األمنية قبل تنفيذىا. [ ت ]

سالمة التطبيقات في ظل ضوابط أمنية مالئمة مثل آلية التحكم في

عمى

يجب الحفاظ

.4.0.3

اإلصدار والفصل بين بيئات التطوير واالختبار والتشغيل. [ ت ]

ال يجب السماح لفريق تطوير التطبيق بالوصول إلى البيانات إال لمضرورة. [ ت ]

.4.0.4

### .5.2إدارة اإلعدادات والتحكم بها.

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

يجب األخذ بعين االعتبار التغي ارت الواقعة عمى آليات الحماية األمنية الحالية. [ ت ]

.4.1.0

.4.1.1

م ارقبة وم ارجعة تركيب جميع المعدات والبرمجيات الحاسوبية. [ ت ]

يجب

.4.1.2

يجب أن تكفل اإلدا ارت إبالغ الفريق بشكل رسمي بأثر التغيي ارت األمنية و استخدام نظم

المعمومات. [ ت ] [ ظ ]

.4.1.3

## .6 أمن االتصال و الشبكات

### .6.1حماية الشبكة

واعدادات أنظمة الشبكة الداخمية دون موافقة الجية المعنية. [ ت ]

يمنع نشر عناوين

.5.0.0

أخرى

أو شبكة عامة

حكومية

شبكة

المتصمة مع

جميع الشبكات الداخمية

يجب حماية

.5.0.1

النظم

إلى

لمنع الوصول غير المصرح بو عن بعد

فعالة

بشكل صحيح. [ ت ] يجب أن تكون التدابير األمنية

والبيانات. [ ت ]

.5.0.2

يمنع الموظفون الموصولة أجيزتيم بالشبكة الداخمية من االتصال بأي شبكة خارجية بأي

شكل من األشكال إال بموافقة الجية المختصة. [ ظ ]

.5.0.3

الشبكة الحكومية

بو إلى

معمومات غير مصرح

لمموظفين ربط أي جياز نظم

ال يجوز

.5.0.4

دون الحصول عمى موافقة الجية المختصة. [ ظ ]

وادارة أنظمة االتصال والمعمومات بشكل دوري. [ ت ]

يجب أن يتم م ارجعة إعدادات

.5.0.5

المعايير األمنية لطرفي

عمى

يجب أن ال تؤثر عممية االتصال مع أي شبكة أخرى

االتصال. [ ت ]

.5.0.6

.5.0.7 يمنع توصيل الموارد الحاسوبية الخاصة الممموكة لمموظفين بالشبكة الداخمية لمحكومة من

دون إذن مسبق من دائرة أمن الشبكات، وتكفل اإلدا ارت استخدام ىذه الموارد الشخصية

بمعايير مطابقة لسياسة أمن تكنولوجيا المعمومات. [ ظ ]

نقميا من خالل اتصال خارجي غير

عند

تشفير المعمومات المصنفة تصنيفا خاصا

يجب

.5.0.8

آمن. [ ت ] [ ظ ]

داخل الشبكة المحمية

عالي السرية عند نقميا

تشفير المعمومات المصنفة تصنيفا

يجب

.5.0.01

عمى أن تكون آلية التشفير متوافقة مع سياسة أمن تكنولوجيا المعمومات . [ ت ] [ ظ ]

### .6.2أمن اإلنترنت

.5.1.0 يجب أن تكون جميع طرق الوصول إلى اإلنترنت إما عن طريق مركزية لبوابات اإلنترنت

بما يتماشى مع المعايير األمنية. في

بالدائرة

بوابة اإلنترنت الخاصة

أو من خالل

الظروف التي ال يكون ىذا ممكنا، أو بالنظر إلى طريقة االستخدام، قد ينظر في السماح لإلدا ارت الوصول إلى اإلنترنت من خالل أجيزة قائمة بذاتيا، شريطة أن تكون ىناك

موافقة، مع وجود آلية مناسبة لمرقابة. [ ت ]

بعض المواقع غير الخاصة بالعمل.

من حجب

الفائدة

اإلدا ارت أن تنظر في

عمى

ينبغي

.5.1.1

مع األخذ بعين االعتبار أن عدم فمترة بعض المواقع ال يعني السماح لمموظف بتصفح تمك

المواقع. [ م ] [ ت ] [ ظ ]

باالستخدام المقبول

في ما يتعمق

كل قسم لممستخدمين سياستو

يوضح

يجب أن

.5.1.2

لإلنترنت[.م]

جميع الب ارمج والممفات التي تم تحميميا من شبكة

والتحقق من

الفحص

يتم

يجب أن

.5.1.3

اإلنترنت باستخدام البرمجيات المضادة لمفيروسات. [ ت ] [ ظ ]

تحميمو من شبكة اإلنترنت ما لم يكن من مصدر

أي برنامج تم

ال يجوز لمموظفين تنفيذ

موثوق بو. [ ظ ]

.5.1.4

### .6.3أمن البريد اإللكتروني

كل إدارة أن توضح سياستيا لمموظفين بشكل واضح فيما يتعمق باالستخدام

يجب عمى

.5.2.0

المقبول لمبريد االلكتروني. [ م ]

مسئولي األنظمة إنشاء عممية منيجية لمتسجيل واالحتفاظ وحذف رسائل البريد

يجب عمى

.5.2.1

االلكتروني والسجالت المرفقة بيا. [ ت ] يجب فحص الرسائل الصادرة والواردة لمبريد االلكتروني من الفيروسات وأي ممفات

مشبوىة. [ ت ] [ ظ ]

.5.2.2

المواقع الحكومية من التعديل أو

عمى

يجب حماية عناوين البريد الداخمية أو التي تحتوي

الوصول غير المصرح بو. [ ت ]

.5.2.3

يجب نقل البريد االلكتروني الذي يحتوي عمى معمومات سرية عبر نظام معموماتي مصرح بو ومصدق عميو من مسئول األمن الحكومي. كما ويجب نقل البريد االلكتروني الذي

يحتوي عمى معمومات مصنفة تصنيفا عالي السرية كما ىو موضح في .6.1.10 [ ظ ]

يمنع فتح أو إعادة توجيو رسائل البريد اإللكتروني المرسمة من مصادر مشبوىة. [ ظ ]

.5.2.4

.5.2.5

### .6.4الحماية ضد فيروسات الكمبيوتر والشيف ارت الخبيثة

جميع الخوادم واألجيزة

عمى

يجب أن تكون البرمجيات المضادة لمفيروسات مفعمة دائما

.5.3.0

األجيزة التي تتصل عن بعد بالشبكة الحكومية الداخمية.

وأيضا عمى

في الشبكة المحمية،

]ظ[ ]ت[

الشيف ارت

الخاصة بيا من الفيروسات و

اإلدا ارت حماية أنظمة المعمومات

عمى

يجب

.5.3.1

الخبيثة، كما ويجب تحديث ب ارمج مضادات الفيروسات بشكل دوري وكمما كان ذلك

ضروريا. [ ت ] [ ظ ]

فحصيا

بعد

األصل إال

المصادر مجيولة

وسائط التخزين والممفات من

يمنع استخدام

.5.3.2

الشيف ارت

فيروسات الكمبيوتر أو

وتنظيفيا من الفيروسات و الشيف ارت الخبيثة. [ ظ ] يمنع المستخدمون من كتابة أو تشغيل أو نسخ أو نشر

الخبيثة. [ ظ ]

.5.3.3

األجيزة

الالسمكية أو

االتصال

مناسبة لحماية أجيزة

تدابير

أن تنفذ

اإلدا ارت

عمى

يجب

.5.3.4

الحاسوبية المتنقمة من الفيروسات و الشيف ارت الخبيثة. [ ت ] [ ظ ]

### .6.5إدارة البرمجيات وممفات التصحيح

عمى أجيزة الكمبيوتر والشبكات [. ظ ]

يجب فقط تشغيل البرمجيات موثوقة المصدر

.5.4.0

إذن مسبق

أنظمة المعمومات الحكومية بدون

عمى

المصرح بيا

يمنع تشغيل الب ارمج غير

.5.4.1

من مسئول الدائرة. [ ت ] [ ظ ]

اإلدا ارت حماية أنظمة المعمومات من نقاط الضعف المعروفة عن طريق

عمى

يجب

.5.4.2

أنظمة المعمومات أو تنفيذ

منتجات

مزودي

بيا من

تطبيق أحدث الرقع األمنية الموصى

تدابير أمنية تعويضية. [ ت ] [ ظ ]

يجب إج ارء تقييم لممخاطر وعمل اختبار قبل تطبيق تصحيحات نظم األمان، لتقميل اآلثار

السمبية وغير المرغوب بيا عمى أنظمة المعمومات. [ ت ] [ ظ ]

.5.4.3

### .6.6أمن الشبكة الالسمكية

يجب عمى اإلدا ارت توثيق وم ارقبة والتحكم في الشبكات الالسمكية المتصمة بشبكة الحكومة

الداخمية. [ ت ]

.5.5.0

الدخول واستخدام التشفير لحماية البيانات

توثيق

السميمة من

الضوابط األمنية

إتباع

يجب

.5.5.1

المنقولة عبر الشبكات الالسمكية المتصمة مع شبكة الحكومة الداخمية. [ ت ] [ ظ ]

## .7 تقييم وتدقيق المخاطر األمنية

### .7.1تقييم المخاطر األمنية

.6.0.0 يجب أن يتم تقييم المخاطر األمنية لنظم المعمومات والتطبيقات مرة واحدة كل عامين عمى

أن يتم انجاز تقييم المخاطر األمنية قبل التحسينات والتغيي ارت الرئيسية

عمى

األقل،

المرتبطة بتمك النظم والتطبيقات. [ ت ]

يجب أن يكون استعمال البرمجيات المستخدمة لتحميل تقييم المخاطر األمنية مقيدة

ومضبوطة. [ ت ]

.6.0.1

### .7.2التدقيق األمني

يجب أن يتم تقييم نظم المعمومات دوريا من قبل مدققين من طرف مستقل وموثوق بو،

وذلك لتحديد الحد األدنى من الضوابط الالزمة لتقميل المخاطر األمنية إلى مستوى مقبول.

] ت [

يجب أن يتم م ارجعة مدى االمتثال لسياسات أمن الشبكات والحاسوب بشكل دوري. [ ت ]

يجب أن يتم تقييد وضبط استعمال البرمجيات المستخدمة لتحميل التدقيق األمني. [ ت ]

.6.1.0

.6.1.1

.6.1.2

## .8 إدارة األحداث األمنية

### .8.1م ارقبة األحداث األمنية

اإلدا ارت إنشاء آلية لتحديد الحوادث وم ارقبتيا بيدف احتواء ومنع الحوادث

يجب عمى

.7.0.0

األمنية. [ م ] يجب أن تكفل اإلدا ارت أن سجالت النظام ومعمومات الدعم األخرى محفوظة لغرض

إثبات و تتبع الحوادث األمنية فقط. [ ت ]

.7.0.1

### .8.2االستجابة لمحوادث األمنية

أن تنشئ و توثق وتحفظ خطوات معالجة الحوادث األمنية ألنظمة

اإلدا ارت

يجب عمى

.7.1.0

المعمومات التابعة ليا. [ ت ]

يجب عمى الموظفين معرفة و إتباع خطوات معالجة الحوادث األمنية الموثقة. . [ م ]

.7.1.1

والتنبييات

جميع أعطال الشبكة أو أنظمة البرمجيات ، والتحذي ارت

يجب اإلبالغ فو ار عن

.7.1.2

ومشاكل أمن الشبكة

، وما شابو ذلك ،

بيا ألمن المعمومات

المشتبو

ومناطق الضعف

المحتممة، إلى الطرف المسؤول وفقا إلج ارءات التعامل مع األحداث األمنية. [ ت ] [ ظ ] يجب إج ارء خطوات فورية في حالة وجود احتمال اخت ارق النظام وفقا لخطوات معالجة

الحوادث األمنية الموثقة. [ ت ]

.7.1.3