



وزارة رئاسة مجلس الوزراء
المركز القومي للمعلومات
الإدارة الفنية



المرجع: المنظمة الدولية للقياس والهيئة الدولية للكهروتقنية
ISO 27002

الطبعة الثانية 15-06-2005

2010م

6	1.0 ما هو أمن المعلومات؟
7	2.0 لماذا نحتاج لأمن المعلومات؟
7	3.0 كيفية وضع المتطلبات الأمنية
8	4.0 تقييم المخاطر الأمنية
8	5.0 اختيار التحكيمات
9	6.0 نقطة الانطلاق في أمن المعلومات
10	7.0 عوامل النجاح الحاسمة
10	8.0 وضع التوجيهات الخاصة بك
11	1 المدى
11	2 المصطلحات والتعاريف
11	1.2 الأصل
11	2.2 التحكم
11	3.2 التوجيهات
11	4.2 مرافق معالجة المعلومات
11	5.2 امن المعلومات
12	6.2 حدث امن المعلومات
12	7.2 حادثة امن المعلومات
12	8.2 السياسة
12	9.2 المخاطر
12	10.2 تحليل المخاطر
12	11.2 تقييم المخاطر
12	12.2 قيم المخاطر
12	13.2 إدارة المخاطر
12	14.2 معالجة المخاطر
13	15.2 جهة ثالثة
13	16.2 المهدد
13	17.2 الثغرات
13	3 هيكلية المعيار
13	1.3 الفصول
14	2.3 المجموعات الأمنية الرئيسية
15	4تقييم المخاطر ومعالجتها
15	1.4 تقييم المخاطر الأمنية
15	2.4 معالجة مخاطر الأمن
17	5 السياسة الأمنية
17	1.5 سياسة أمن المعلومات
17	1.1.5 وثيقة سياسة أمن المعلومات
18	2.1.5 مراجعة سياسة أمن المعلومات
19	6 تنظيم أمن المعلومات
19	1.6 التنظيم الداخلي
20	1.1.6 التزام الإدارة بأمن المعلومات
21	2.1.6 تنسيق أمن المعلومات
22	3.1.6 توزيع مسئوليات أمن المعلومات
23	4.1.6 عملية ترخيص مرافق معالجة المعلومات
23	5.1.6 الاتفاقات السرية
25	6.1.6 الاتصال مع الهيئات الأخرى
25	7.1.6 الاتصال مع المجموعات ذات الاهتمامات الخاصة

26	8.1.6	المراجعة المستقلة لأمن المعلومات
27	2.6	الأطراف الخارجية
28	6.2.1	تحديد المخاطر ذات الصلة بالأطراف الخارجية
31	2.2.6	المعالجة الأمنية عند التعامل مع الزبائن
32	3.2.6	معالجة القضايا الأمنية في الاتفاقات مع طرف ثالث
37	7	إدارة الوصول
37	1.7	المسئولية عن الأصول
37	1.1.7	جرد الأصول
38	2.1.7	ملكية الأصول
39	3.1.7	الاستخدام المقبول للأصول
40	2.7	تصنيف المعلومات
40	1.2.7	إرشادات التصنيف
41	2.2.7	التعامل مع المعلومات وتمييزها
42	8	أمن الموارد
42	1.8	قبل التوظيف
42	1.1.8	الأدوار والمسئوليات
43	2.1.8	معاينات وفرز المترشحين
44	3.1.8	شروط ومهام الاستخدام
46	2.8	خلال التوظيف
46	1.2.8	مسئوليات الإدارة
47	2.2.8	أمن المعلومات الواعي ، التعليم، التدريب
48	3.2.8	عملية التأديب والعقاب
48	3.8	إنهاء أو تغيير العمل
49	1.3.8	مسئوليات الإنهاء
49	2.3.8	إعادة الأصول
50	3.3.8	إزالة حق الوصول
51	9	الأمن المادي والبيئي
51	1.9	المناطق الأمانة
51	1.1.9	الحماية المادية للمحيط
53	2.1.9	تحكمات الدخول الفيزيائي
54	3.1.9	تأمين المكاتب والقاعات والمرافق
55	4.1.9	الحماية ضد التهديدات الخارجية والبيئية
55	5.1.9	العمل في المناطق الأمانة
56	6.1.9	الوصول المتاح للجمهور، وتسليم المواد ومناطق شحنها
57	2.9	سلامة المعدات
57	1.2.9	تحديد مواقع نصب المعدات وحمايتها
58	2.2.9	المرافق الداعمة
60	3.2.9	سلامة شبكة الكابلات
61	4.2.9	صيانة المعدات
62	5.2.9	أمن سلامة المعدات خارج المباني
63	6.2.9	التخلص المأمون من المعدات أو إعادة استخدامها
64	7.2.9	نقل الممتلكات
65	10	إدارة العمليات والاتصالات
65	1.10	الإجراءات التشغيلية والمسئوليات
65	1.1.10	إجراءات التشغيل الموثقة
66	2.1.10	إدارة التغيير
67	3.1.10	فصل الواجبات
68	4.1.10	الفصل بين التنمية، والاختبار، والتسهيلات التنفيذية

69	2.10	الطرف الثالث تقديم الخدمات الإدارية
69	1.2.10	تقديم الخدمة
70	2.2.10	رصد واستعراض خدمات طرف ثالث
71	3.2.10	إدارة التغييرات في خدمات طرف ثالث
72	3.10	نظام التخطيط والقبول
72	1.3.10	إدارة بناء القدرات
73	2.3.10	نظام القبول
74	4.10	الحماية من الشيفرات الخبيثة والمحمول
74	1.4.10	عناصر من الشيفرات الخبيثة
76	2.4.10	تحكم ضد رمز المحمول
77	5.10	نسخ احتياطية
77	1.5.10	المعلومات احتياطية
79	6.10	إدارة أمن الشبكة
79	1.6.10	شبكة ضوابط
80	2.6.10	الأمن من خدمات الشبكة
81	7.10	التعامل مع وسائل الإعلام
81	1.7.10	إدارة الوسائط القابلة للإزالة
84	4.7.10	الأمن من وثائق النظام
85	8.10	تبادل المعلومات
85	1.8.10	تبادل المعلومات السياسات والإجراءات
88	2.8.10	اتفاقات التبادل
89	3.8.10	البيدنية في وسائل الاعلام العابر
90	4.8.10	الرسائل الالكترونية
91	5.8.10	الأعمال ونظم المعلومات
92	1.9.10	التجارة الالكترونية
94	2.9.10	على الخط الصفقات
95	3.9.10	المعلومات المتاحة للجمهور
96	10.10	الرصد
97	1.10.10	تسجيل التدوين
98	2.10.10	استخدام نظام الرصد
101	5.10.10	خطأ تسجيل
101	6.10.10	ساعة التزامن
103	11	التحكم في الوصول
103	1.11	احتياج العمل للتحكم في الوصول
103	1.1.11	سياسة التحكم في الوصول
105	2.11	إدارة وصول المستخدم
105	1.2.11	تسجيل المستخدم
106	2.2.11	إدارة الامتيازات
107	3.2.11	إدارة كلمات مرور المستخدمين
108	4.2.11	مراجعة صلاحيات وصول المستخدمين
109	3.11	مسئوليات المستخدم:
109	1.3.11	استخدام كلمات المرور:
110	2.3.11	أجهزة المستخدمين في غيابهم
111	3.3.11	سياسة نظافة المكتب والشاشة
112	4.11	التحكم في الوصول للشبكة
112	1.4.11	سياسة استخدام خدمات الشبكة
113	2.4.11	توثيق المستخدمين للإرتباطات الخارجية
114	3.4.11	تحديد المعدات في الشبكات

115	4.4.11	حماية مرافق التحليل والتهيئة عن بعد
116	5.4.11	تقسيم الشبكات
117	6.4.11	التحكم في إرتباط الشبكة
118	7.4.11	التحكم في توجيه الشبكة
118	5.11	التحكم في الوصول لنظم التشغيل
119	1.5.11	إجراءات الدخول الآمن
120	2.5.11	تحديد هوية المستخدم وتوثيقه
122	3.5.11	نظام إدارة كلمات المرور
123	4.5.11	استخدام أدوات النظام المساعدة
123	5.5.11	إنهاء زمن الجلسة
124	6.5.11	تحديد زمن الارتباط
125	6.11	التحكم في الوصول للتطبيق والمعلومات
125	1.6.11	تقييد الوصول للمعلومات
126	2.6.11	عزل النظم الحساسة
127	7.11	الحوسبة المتنقلة
127	1.7.11	الحوسبة المتنقلة والاتصالات
128	2.7.11	العمل عن بعد
131	12	حيازة وتطوير وصيانة أنظمة المعلومات
131	1.12	متطلبات أمن نظم المعلومات
131	1.1.12	تحليل وتحديد مواصفات متطلبات الأمن
132	2.12	تصحيح المعالجة في التطبيقات
132	1.2.12	التحقق من صحة البيانات المدخلة
133	2.2.12	مراقبة المعالجة الداخلية
135	3.2.12	صحة الرسالة
135	4.2.12	التحقق من صحة البيانات المخرجة
136	3.12	ضوابط التشفير
136	1.3.12	السياسات بشأن استخدام ضوابط التشفير
138	2.3.12	إدارة المفاتيح
140	4.12	أمن ملفات النظام
140	1.4.12	مراقبة البرامج التشغيلية
142	2.4.12	حماية بيانات اختبار النظام
143	3.4.12	مراقبة الدخول إلى شفرة مصدر البرنامج
144	5.12	الأمن في دعم وتطوير العمليات
144	1.5.12	تغيير إجراءات المراقبة
146	2.5.12	استعراض فني للتطبيقات بعد تغييرات نظام التشغيل
146	3.5.12	تقييد التغييرات الى حزم البرمجيات
147	4.5.12	تسرب المعلومات
148	5.5.12	جهة خارجية لتطوير البرمجيات
148	6.12	إدارة الثغرات التقنية
149	1.6.12	مراقبة نقاط الضعف التقني
151	13	إدارة حوادث أمن المعلومات
151	13.1	الإبلاغ عن نقاط الضعف، والأحداث الأمنية
151	1.1.13	التبليغ عن أحداث أمن المعلومات
153	2.1.13	الإبلاغ عن الضعف في الأنظمة الأمنية
154	2.13	إدارة وتأمين حوادث المعلومات والتحسينات
154	1.2.13	المسؤوليات والإجراءات
156	2.2.13	التعلم من الحوادث الأمنية للمعلومات
158	14	إدارة استمرارية الأعمال

158	1.14	إدارة نواحي أمن المعلومات واستمرارية الأعمال
158	1.1.14	تضمين أمن المعلومات في عملية إدارة استمرارية الأعمال
160	2.1.14	تواصل الأعمال وتقييم المخاطر
160	3.1.14	وضع وتنفيذ خطط الاستمرارية المتضمنة على أمن المعلومات
162	4.1.14	الهيكل الإداري لتخطيط تواصل الأعمال
164	5.1.14	اختبار، وصيانة وإعادة تقييم خطط استمرارية الأعمال
166	15	الامتثال
166		الامتثال للمتطلبات القانونية
166	1.1.15	تعريف التشريعات المطبقة
166	2.1.15	حقوق الملكية الفكرية
168	3.1.15	حماية السجلات التنظيمية
170	4.1.15	حماية البيانات والخصوصية والمعلومات الشخصية
170	5.1.15	منع إساءة استخدام المعلومات ومرافق المعالجة
172	2.15	الامتثال للسياسات والمعايير الأمنية والفنية
173	1.2.15	الامتثال للسياسات والمعايير الأمنية
173	2.2.15	التحقق من الامتثال التقني
174	3.15	اعتبارات مراجعة نظم المعلومات
175	1.3.15	مراجعة ضوابط نظم المعلومات
175	2.3.15	حماية أدوات مراجعة نظم المعلومات

1.0 ما هو أمن المعلومات؟

2.0 لماذا نحتاج لأمن المعلومات؟

(أ)

(ب)

(

(

3.0 كيفية وضع المتطلبات الأمنية

:

(1)

(2)

(3)

4.0 تقييم المخاطر الأمنية

1.4

5.0 اختيار التحكيمات

" 4.2

7.0 عوامل النجاح الحاسمة

:

(

(

(

(

(

(

(

(

(

(

8.0 وضع التوجيهات الخاصة بك

1 المدى

2 المصطلحات والتعاريف

1.2 الأصل

2.2 التحكم

3.2 التوجيهات

4.2 مرافق معالجة المعلومات

5.2 امن المعلومات

6.2 حدث امن المعلومات

7.2 حادثة امن المعلومات

)

(

8.2 السياسة

9.2 المخطر

10.2 تحليل المخطر

11.2 تقييم المخاطر

12.2 قيم المخاطر

13.2 إدارة المخاطر

:

14.2 معالجة المخاطر

15.2 جهة ثالثة

16.2 المهدد

17.2 الثغرات

3. هيكلية المعيار

39

1.3 الفصول

.

:

(1)	(
(2)	(
(2)	(
(3)	(
(2)	(
(10)	(
(7)	(
(6)	(
(2)	(

(1) (_____
(3) (_____
: _____

2.3 المجموعات الأمنية الرئيسية

:
(_____
() (_____
:

4 تقييم المخاطر ومعالجتها

1.4 تقييم المخاطر الأمنية

()

()

)

.(

2.4 معالجة مخاطر الأمن

(

(

(

(

(

(

(

(

(

()

(3.10)

(10.10)

5 السياسة الأمنية

1.5 سياسة أمن المعلومات

:

1.1.5 وثيقة سياسة أمن المعلومات

_____:

:

(

(

(

(

:

-1

-2

-3

-4

()

()

2.1.5 مراجعة سياسة أمن المعلومات

:

(
(
(
(

(
(
(

:

(
(
(

6 تنظيم أمن المعلومات

1.6 التنظيم الداخلي

:

2.1.6 تنسيق أمن المعلومات

(

(

(

(

(

(

(

3.1.6 توزيع مسنوليات أمن المعلومات

(4)

()

:

(

(

(2.1.7) .

(

4.1.6 عملية ترخيص مرافق معالجة المعلومات

:

(

(

(

5.1.6 الاتفاقات السرية

:

() . (

(

(

(

() . (

(

(

(

(

(

(

(1.1.5) .

6.1.6 الاتصال مع الهيئات الأخرى

(...)

()

(14)

(2.13)

()

()

7.1.6 الاتصال مع المجموعات ذات الاهتمامات الخاصة

-:

(

.

(

(

.

(

(

.

)

(

.(1.2.13

8.1.6 المراجعة المستقلة لأمن المعلومات

)

(

)

(1.1.5

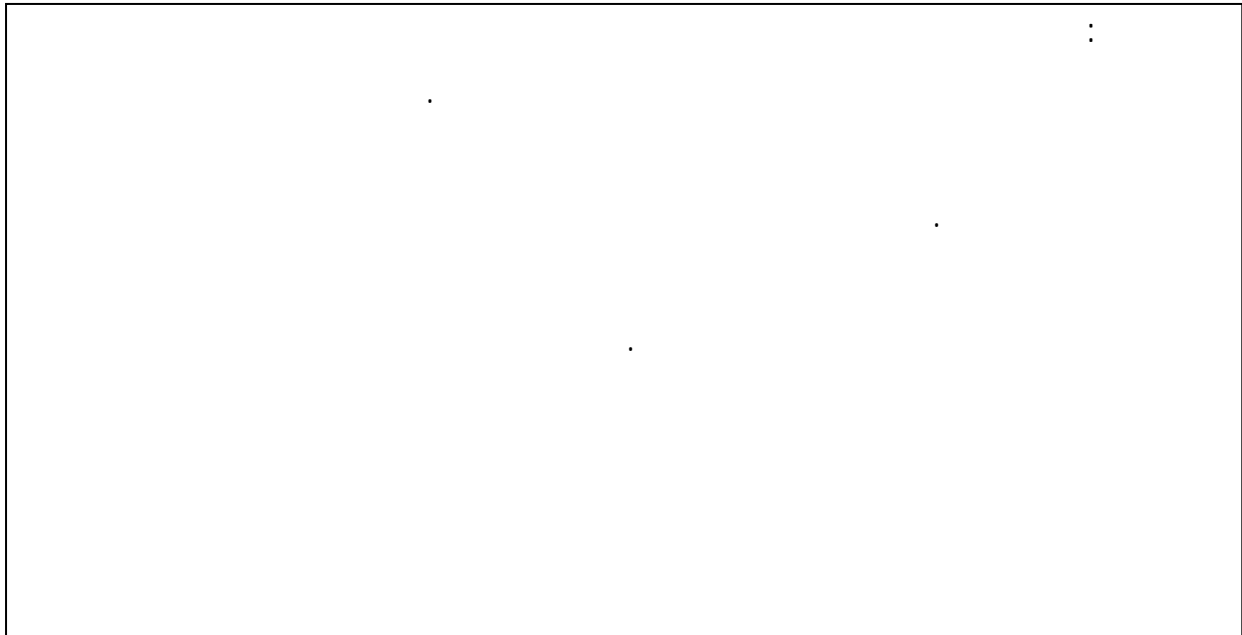
(1.2.15)

2002

ISO/9011:2002

(3.15)

2.6 الأطراف الخارجية



6.2.1 تحديد المخاطر ذات الصلة بالأطراف الخارجية

() (4).

:

(

(

- :

(1

:

(2

()

(3

)

.(

(4

(

(

(

(

(

(

(

(

(

(2.2.6 3.2.6) .

:

-:

(3.2.6 2.2.6)

(

(

()

(

:

/

(

(

:

(

(

(

2.2.6 المعالجة الأمنية عند التعامل مع الزبائن

-)
:(
-:
(
(1
(2
(3
(4
(
(
(
- :
(1
(2
(3

(1.2.6):

(

- :

(

(1

(2

(1.4.10) .

(3

(4

(5

(6

(5.1.2)

(7

(5.1.6) .

(

(

(

(

(

(

-:

(

(1

(2

(3

(4

(5

(6

(

(

. (1.2.7)

(

(

(

(

(

(

(

(

)

. (1.15

)

(2.1.15)

(

(5.1.6

(

- :

(

(1

(2

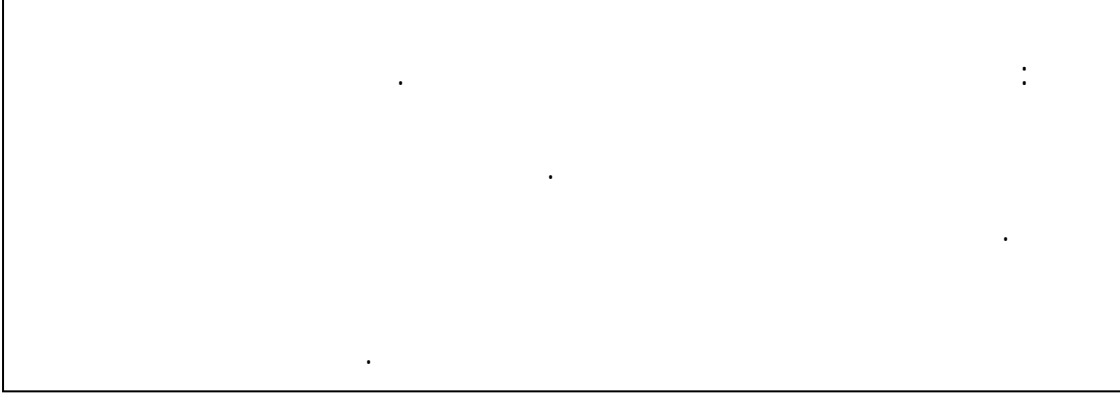
(3)

(1.2.6) .

/

7 إدارة الوصول

1.7 المسؤولية عن الأصول



1.1.7 جرد الأصول

(2.7)

(2.1.7)

:

(:

(:

(:

(:

(

(

(4) .

2.1.7 ملكية الأصول

:

(

(

:

(

(

(

(

()

3.1.7 الاستخدام المقبول للاصول

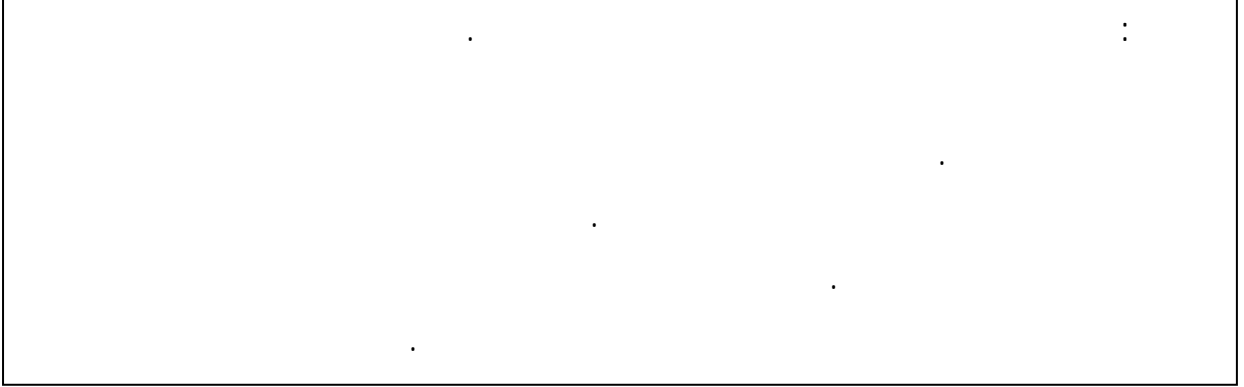
(8.10)

(1.7.11)

(

(

2.7 تصنيف المعلومات



1.2.7 إرشادات التصنيف

(2.1.7)

2.7.10

2.2.7 التعامل مع المعلومات وتمييزها

()

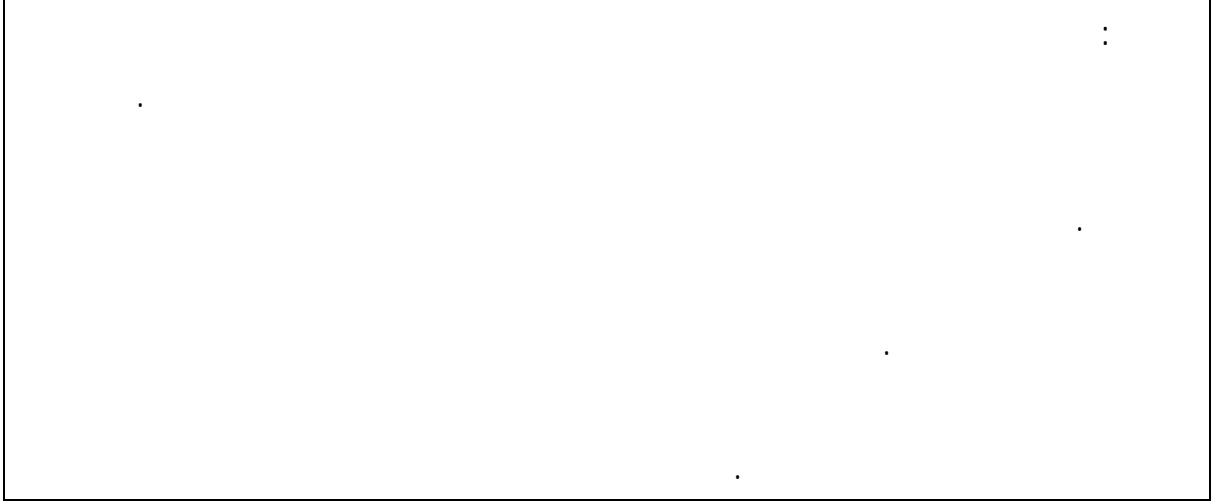
.1.2.7

)

(

8 أمن الموارد

1.8 قبل التوظيف



1.1.8 الأدوار والمسئوليات

(5-1) .

(

(

(

(

(

()

2.1.8 معاینات وفرز المترشحين

:

(

(

(

()

(

(

()

(3.2.6)

3.1.8 شروط و مهام الاستخدام

(

(

(1.1.15 2.1.15)

(

(1.2.7)

(3.7.10)

(

(

(

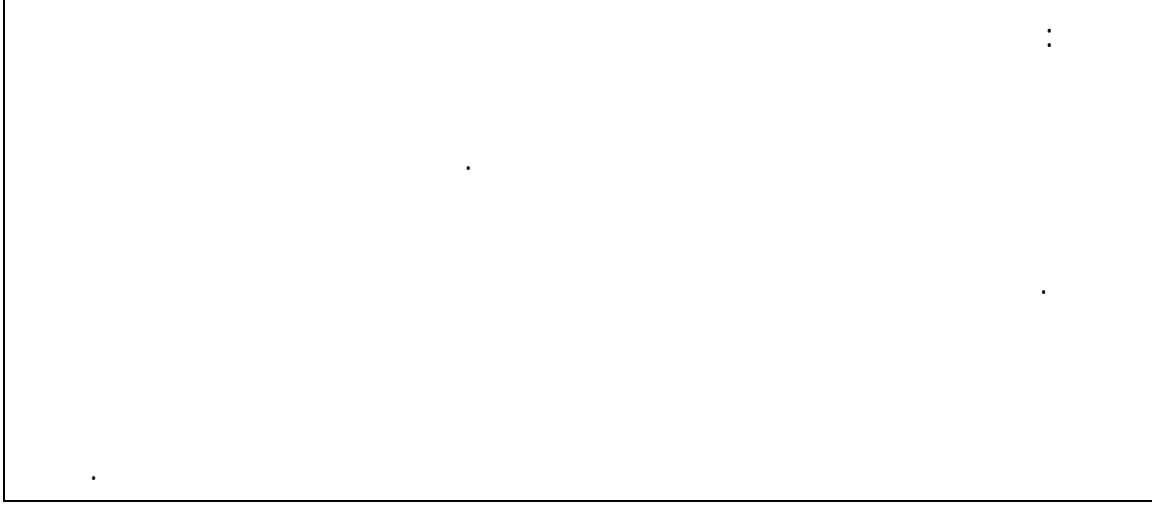
.(1.7.11 5.2.9)

(

.(3.2.8) .

.(3.8) .

2.8 خلال التوظيف



1.2.8 مسئوليات الإدارة

:

(

(

(

(

) .

(2.2.8

(

(

2.2.8 أمن المعلومات الوعي ، التعليم، التدريب

(1.13) .

3.2.8 عملية التأديب والعقاب

3.2.13)

(

3.8 إنهاء أو تغيير العمل

:

.1.8

1.3.8 مسئوليات الإنهاء

(3.1.8)

(5.1.6)

2.3.8 إعادة الأصول

(10.7).

3.3.8 إزالة حق الوصول

(4.2.11)

:

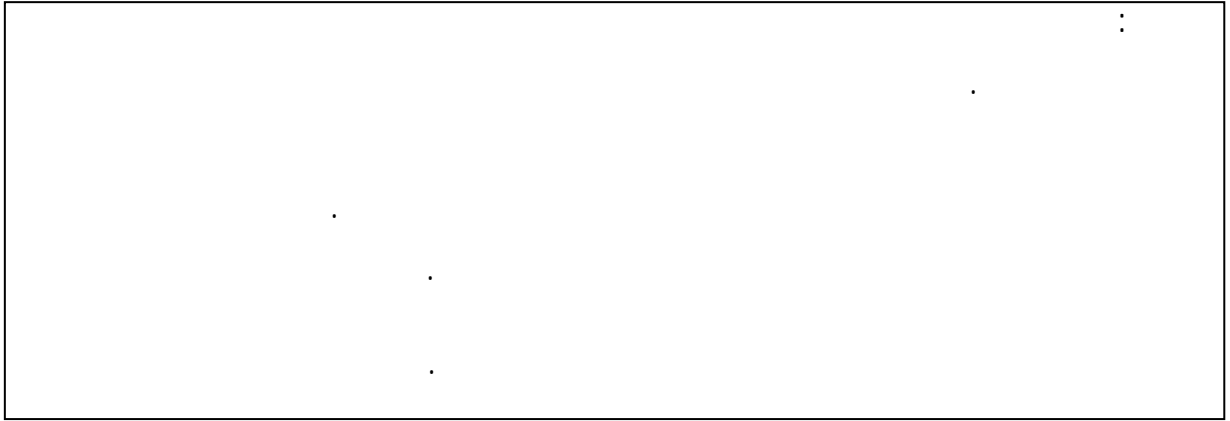
(

(

(

9 الأمن المادي والبيئي

1.9 المناطق الآمنة



1.1.9: الحماية المادية للمحيط

()
:

(

(

:)

(

(

(

(

(

(

2.1.9 تحكيمات الدخول الفيزيائي

:

(

(

:

" "

(

(

(

.(3-3-8) .

3.1.9 تأمين المكاتب والقاعات والمرافق

_____:

:

(

(

(

(

4.1.9 الحماية ضد التهديدات الخارجية والبيئية

" "

()

(

(

(

5.1.9 العمل في المناطق الآمنة

:

(

(

(

(

6.1.9 الوصول المتاح للجمهور، وتسليم المواد ومناطق شحنها

:

(

(

(

(1.2.9)

(

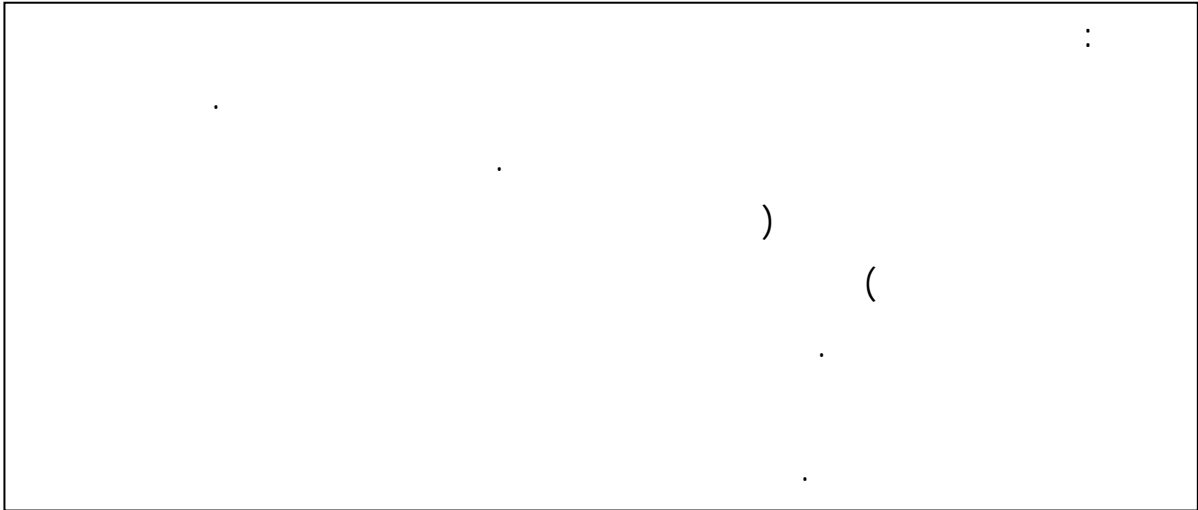
)

(

(1.1.7

(

2.9 سلامة المعدات



1.2.9 تحديد مواقع نصب المعدات وحمايتها

:

(

(

(

: ()
()

(

(

(

()

()

(

(

2.2.9 المرافق الداعمة

/

(UPS)

.(UPS)

.()

3.2.9 سلامة شبكة الكابلات

:

:

-1

-2

-3

-4

-5

-6

4.2.9 صيانة المعدات

:

5.2.9 أمن سلامة المعدات خارج المباني

:

(ISO/IEC18028)

(1-7-11)

6.2.9 التخلص المأمون من المعدات أو إعادة استخدامها

(2-7-10)

7.2.9 نقل الممتلكات

_____:

10 إدارة العمليات والاتصالات

1.10 الإجراءات التشغيلية والمسؤوليات

_____:

1.1.10 إجراءات التشغيل الموثقة

.

:

(

(10.5) (

(

(

)

(11.5.4

(

(

(10.7.3 10.7.2)

(

(10.10)

2.1.10 إدارة التغيير

(
(
(
(
(
(
(

(12.5.1)

3.1.10 فصل الواجبات

4.1.10 الفصل بين التنمية، والاختبار، والتسهيلات التنفيذية

:

(

(

(

(

(

(12.4.2)

(

)

(12.4.2)

2.10 الطرف الثالث تقديم الخدمات الإدارية

:

1.2.10 تقديم الخدمة

)

(

(14.1).

2.2.10 رصد واستعراض خدمات طرف ثالث

:

(

(

(

(

(

(6.2.3)

/

3.2.10 إدارة التغييرات في خدمات طرف ثالث

:

:

(

2.3.10 نظام القبول

()

:

(

(

(

(

(14.1)

(

(

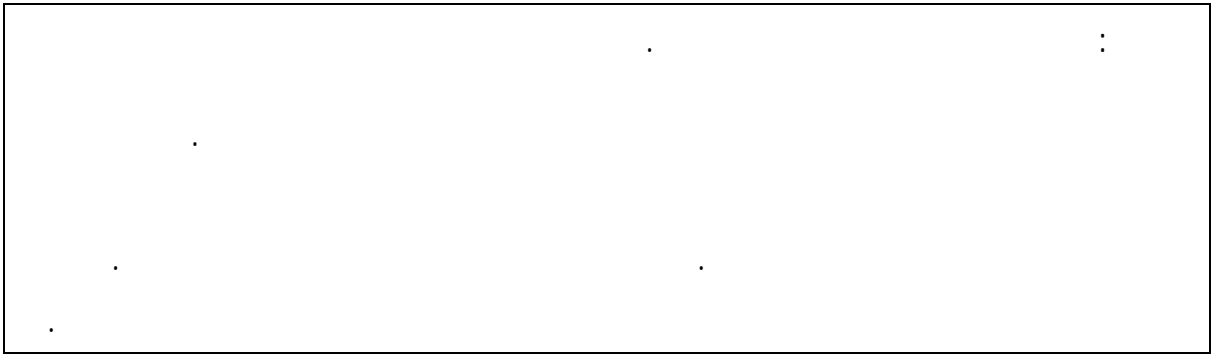
(

(

(

(

4.10 الحماية من الشيفرات الخبيثة والمحمول



1.4.10 عناصر من الشيفرات الخبيثة

(15.1.2)

:

(

(

(

(

:

(1

(2

(3

(

)

(13.2 13.1

(14)

(

(

/

(

2.4.10 تحكم ضد رمز المحمول

:

(

(

(

(

(

(

5.10 نسخ احتياطية

	:
	(14.1)

1.5.10 المعلومات احتياطية

:

(

(

() (

(

(

(9)

(

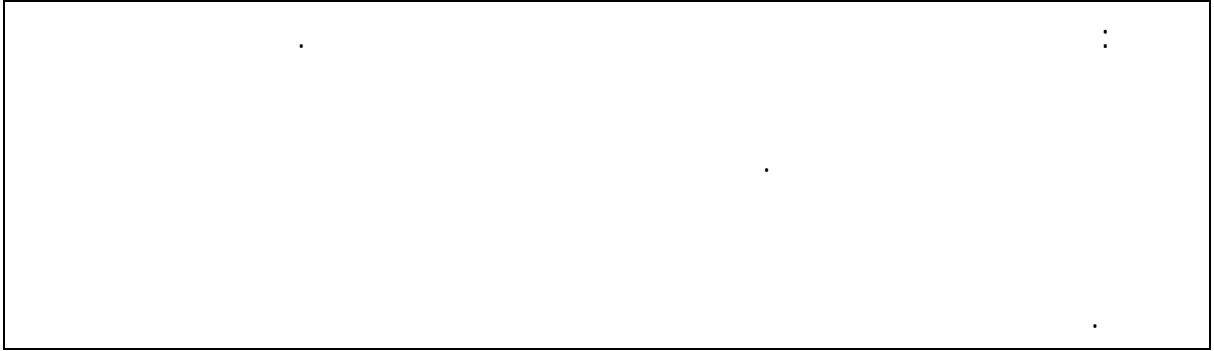
(

(

(14) .

(15.1.3) .

6.10 إدارة أمن الشبكة



1.6.10 شبكة ضوابط

(
(10.1.3)

(12.3 11.4)

(

(

(

(

/

18028

2.6.10 الأمن من خدمات الشبكة

:

(

(

(

7.10 التعامل مع وسائل الإعلام

	:
	.
	/ ()

1.7.10 إدارة الوسائط القابلة للإزالة

:

(

--

.

(

(

(

()

(

(

2.7.10 التلخيص من وسائل الاعلام

:

(

(

(

(

(

.(

9.2.6)

3.7.10 إجراءات التعامل مع المعلومات

:

(7.2)

(

(

(

(

(

(

(

(

(

/

4.7.10 الأمن من وثائق النظام

:

(

(

(

8.10 تبادل المعلومات

:	
(15).)

1.8.10 تبادل المعلومات السياسات والإجراءات

:

(

(

(10.4.1)

)

(
(
(7.1.3

(

(

)

(
(12.3

(

(

(

(

:

(1

(2

(3

(

:

(

(1

(2

(3

(

(

(15)

(10.3 14) .
(11) .

2.8.10 اتفاقات التبادل

:

(
(
(
(
(
(
(
(
(

(15.1.2 15.1.4)

(

(

(

(12.3) .

(10.8.3)

3.8.10 البدنية في وسائل الاعلام العابر

:

(

(

(

()

(

(

:

(1

(2

()

(3

(4

.

4.8.10 الرسائل الالكترونية

:

(

(

(

(

(

(

()

5.8.10 الأعمال ونظم المعلومات

:

(

(

(

(

(7.2)

(

(

(6.3 6.2)

(

(

(10.5.1)

(

.(14)

(

:

/

9.10

:

1.9.10 التجارة الالكترونية

(

()

(6.4.11)

(12.3)

2.9.10 على الخط الصفقات

:

(

:

(

(1

(2

(3

(

(

(

)

(

(

/

/

/

3.9.10 المعلومات المتاحة للجمهور

(12.3).

(15.1.4)

:

(

(

(

(

10.10 الرصد

	:
	.



1.10.10 تسجيل التدوين

:

(

(

(

(

(

(

(

(

(

(

(

(

.

(15.1.4).

(10.1.3).

2.10.10 استخدام نظام الرصد

:

:

((

(1

(2

(3

(4

(5

:

/

(1

(2

/

/

(3

:

(

(1

(2

(3

(4

(1

(2

(3

(4

(

:

(

(

(

()

(

(

.13.1.1

3.10.10 سجل حماية المعلومات

:

(
(
(

(13.2.3)

/

(
4.10.10 مدير ومشغل الجذوع

:

()
()
()
()
()

5.10.10 خطأ تسجيل

:

(

(

6.10.10 ساعة التزامن

()

() /

11 التحكم في الوصول

1.11 احتياج العمل للتحكم في الوصول

_____ :

1.1.11 سياسة التحكم في الوصول

:

(

(

(2.7) .

(

(

(

(1.15) .

(

(

(

(1.2.11)

(

(4.2.11)

(

(3.3.8)

(

:

(

"

"

(

"

(2.7)

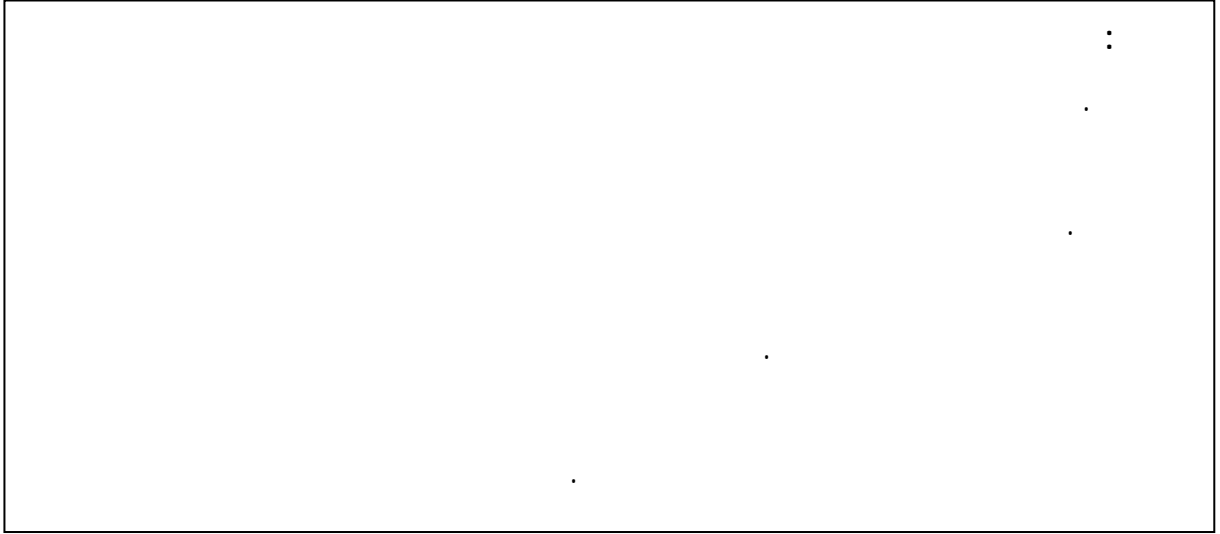
(

(

(

(6.11 1.4.10 3.11 3.1.6)

2.11 إدارة وصول المستخدم



1.2.11 تسجيل المستخدم

:

(

(

(

(1.11 3.1.10) .

(

(

(

(

(

(4.2.11).

(

2.2.11 إدارة الامتيازات

:

(..... :)

(

(

(1.1.11).

.(

(

(

(

(

3.2.11 إدارة كلمات مرور المستخدمين

(

(

(

(

(

(

(

(

4.2.11 مراجعة صلاحيات وصول المستخدمين

:

6

()

(1.2.11).

(

(2.2.11)

(

3

(

(

3.11 مسئوليات المستخدم:

:

1.3.11 استخدام كلمات المرور:

(

(

(

(

(1

(2

....

(3

(4

(

(

(

(

(

2.3.11 أجهزة المستخدمين في غيابهم

:

(

(

(

3.3.11 سياسة نظافة المكتب والشاشة

(2.7)

(1.15)

:

(

(

(

)

(

(

(

4.11 التحكم في الوصول للشبكة

	:
	:
	(
	(
	(

1.4.11 سياسة استخدام خدمات الشبكة

:
.
.
.
)
.(

(
(
(
(

(1.11).

2.4.11 توثيق المستخدمين للإرتباطات الخارجية

()

3.4.11 تحديد المعدات في الشبكات

(2.4.11) .

4.4.11 حماية مرافئ التحليل والتهينة عن بعد

/

5.4.11 تقسيم الشبكات

()
(7.4.11 6.4.11)
(1.11)

/

(1.10)

(7.4.11 6.4.11)

6.4.11 التحكم في ارتباط الشبكة

(1.11).

(1.1.11).

:

(

(

(

(

7.4.11 التحكم في توجيه الشبكة.

)

(1.11).

5.11 التحكم في الوصول لنظم التشغيل

	:
	:
	(
	(
	(

(

(

(

1.5.11 إجراءات الدخول الآمن

:

(

(

.

(

(

(

(1

(2

(3

(4

(5

(

(

(1

(2

(

(

2.5.11 تحديد هوية المستخدم وتوثيقه

() .

(1.3.11 3.5.11)

4.5.11 استخدام أدوات النظام المساعدة

:

(

(

(

(

(

(

(

(

(

5.5.11 إنتهاء زمن الجلسة

6.5.11 تحديد زمن الارتباط

(

(

(

(

2.6.11 عزل النظم الحساسة

(

(

.

:

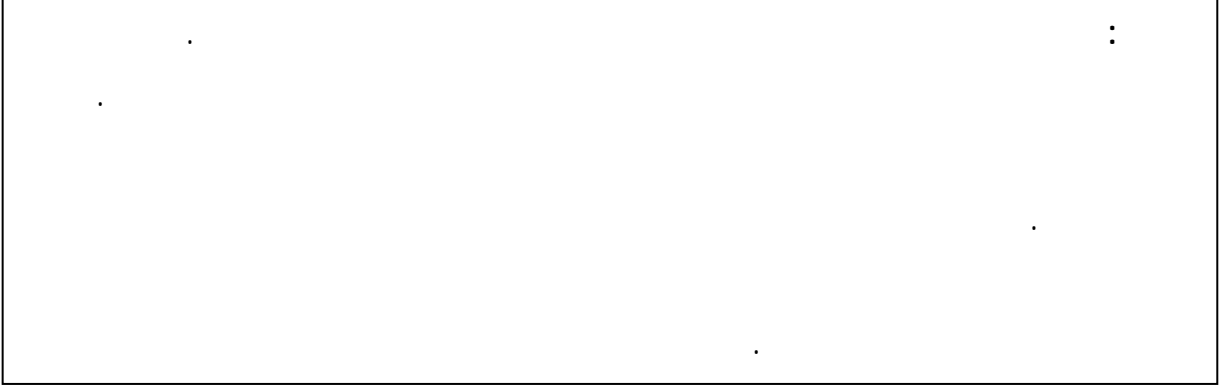
(

(

() .()

(5.4.11).

7.11 الحوسبة المتنقلة



1.7.11 الحوسبة المتنقلة والاتصالات

... ..

.

(4-10) .

(5.2.9).

:

(

(

2.7.11 العمل عن بعد

:

(

(

(

(

.()

(

(

()

(

(

(

:

(

(

(

(

(

(

(

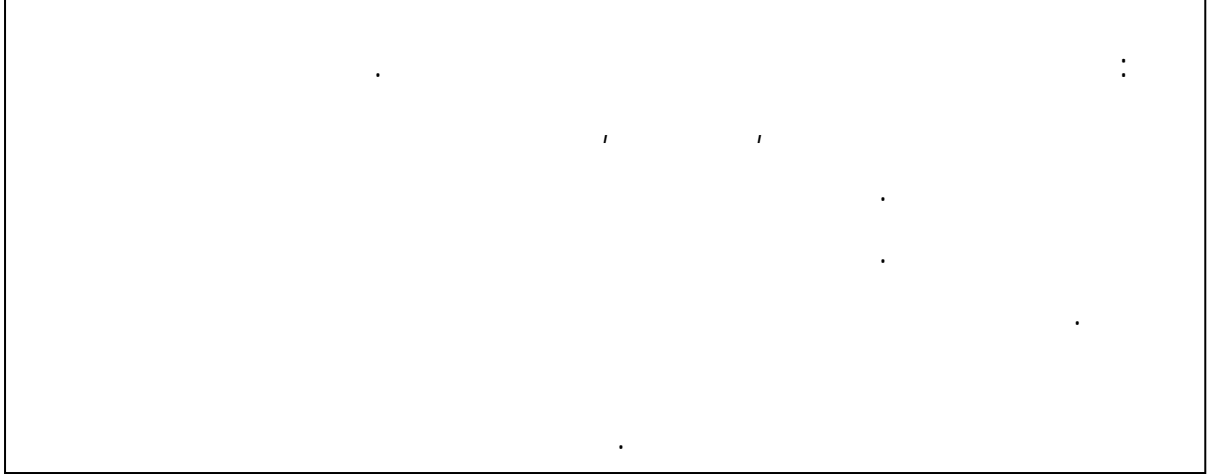
(

(

(

12 حيازة وتطوير وصيانة أنظمة المعلومات

1.12 متطلبات أمن نظم المعلومات

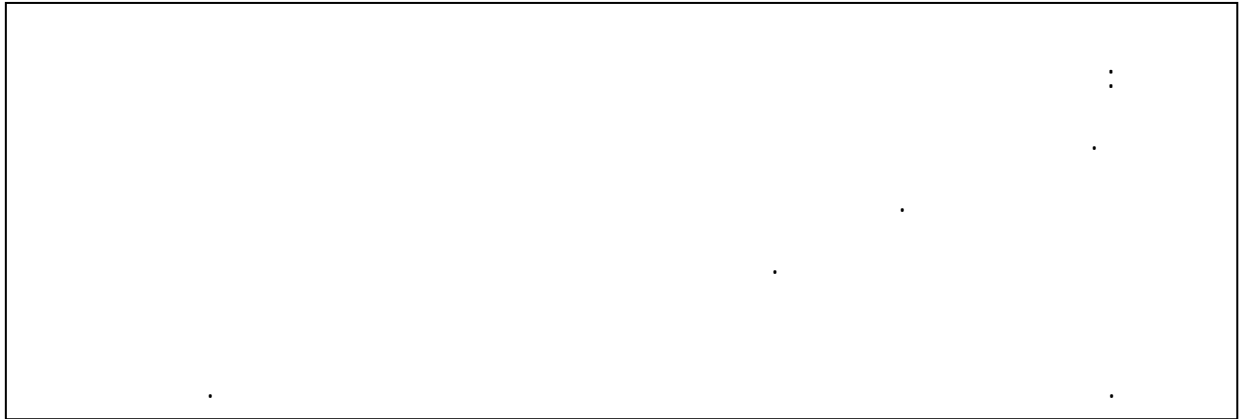


1.1.12 تحليل وتحديد مواصفات متطلبات الأمن

15408

3-13335

2.12 تصحيح المعالجة في التطبيقات



1.2.12 التحقق من صحة البيانات المدخلة

)

)

(

:

.(

(

:

(1

(2

(3

(4

(5

(

(

(

(

(

(

2.2.12 مراقبة المعالجة الداخلية

(

(

(

(

:

(

(

:

(1

(2

(3

(

(

(

(

(

(

3.2.12 صحة الرسالة

4.2.12 التحقق من صحة البيانات المخرجة

:

(

(

(

(

(

(

3.12 ضوابط التشفير

:

1.3.12 السياسات بشأن استخدام ضوابط التشفير

(

(

(

(

(

(1

(2

)

(

.(

)

(

.(

:

: (

: / (

: (

JTC1 SC27

IEEE P1363

2.3.12 إدارة المفتاح

:

(

(

(

(

(

(

) (. (((((

11770

:

:

(

(

(

(

(

(

(

(

2.4.12 حماية بيانات اختبار النظام

(

(

(

(

3.4.12 مراقبة الدخول إلى شفرة مصدر البرنامج

)

(

:

(

(

(

(

(

(

(

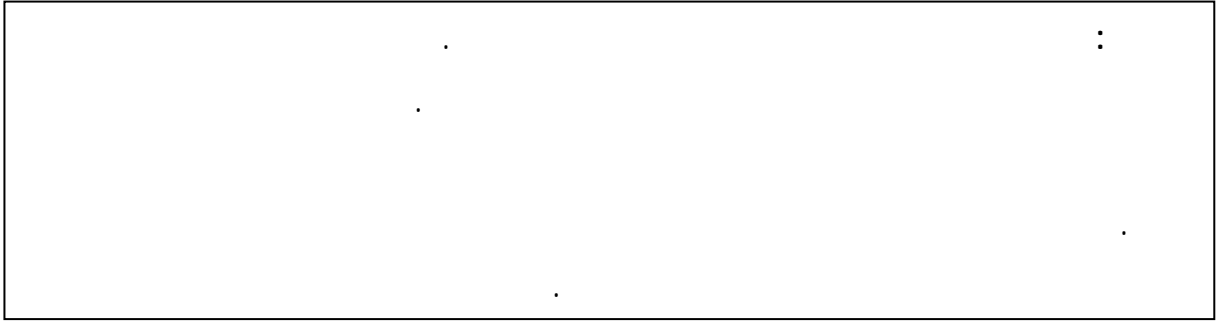
()

12207

10007

5.12 الأمن في دعم وتطوير العمليات

:



1.5.12 تغيير إجراءات المراقبة

:

(

(

(

(

(

(

(

(

(

(

(

2.5.12 استعراض فني للتطبيقات بعد تغييرات نظام التشغيل

:

(

(

(

(

3.5.12 تقييد التغييرات الى حزم البرمجيات

:

(

(

(

(

4.5.12 تسرب المعلومات

)

:(

(

(

(

(

(

5.5.12 جهة خارجية لتطوير البرمجيات

(

(

(

(

(

(

6.12 إدارة الثغرات التقنية

:

معايير

1.6.12 مراقبة نقاط الضعف التقني

()

·
·
·

(

(

(

(

/

(

(

.)

)

(

:

(1

(2

(3

(4

(

(

(

13 إدارة حوادث أمن المعلومات

13.1 الإبلاغ عن نقاط الضعف، والأحداث الأمنية

:

.

.

1.1.13 التبليغ عن أحداث أمن المعلومات

:

(

(

(

:

)

(1

.(

(2

(

alarm4

:

(

(

(

(

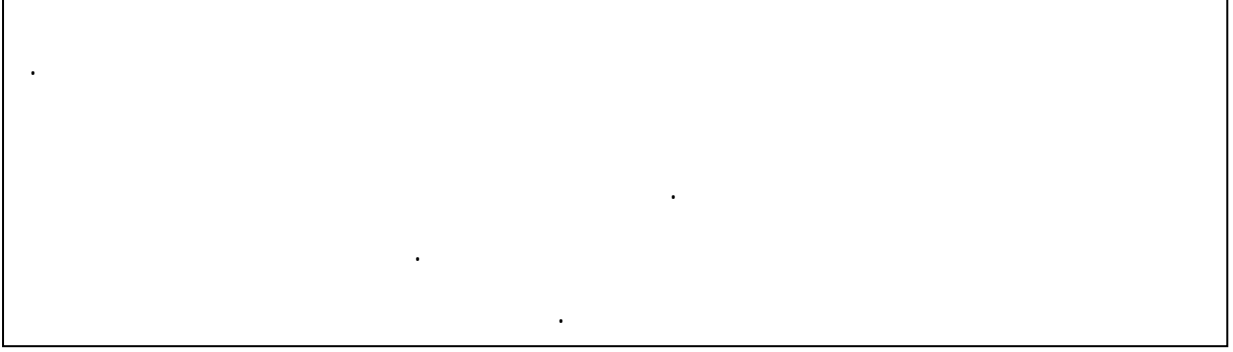
(

(

(

2.1.13 الإبلاغ عن الضعف في الأنظمة الأمنية

2.13 إدارة وتأمين حوادث المعلومات والتحسينات



1.2.13 المسؤوليات والإجراءات

:

(

:

(1

(2

(3

(4

(5

(6

(

(1

(2

(3

(4

(5

(

:

(1

(2

(3

(

:

(1

(2

(3

(4

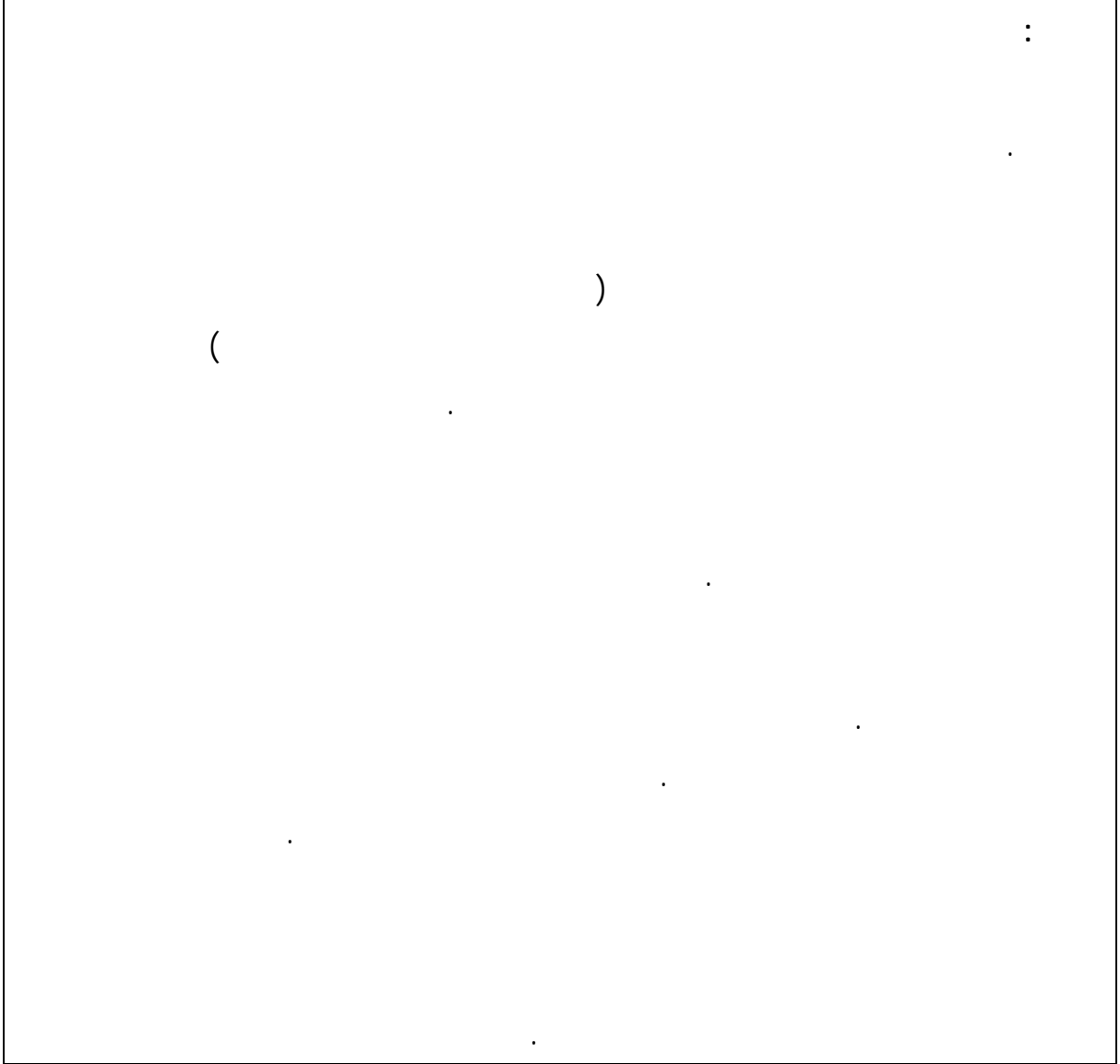
2.2.13 التعلم من الحوادث الأمنية للمعلومات

3.2.13 جمع الأدلة

()

14 إدارة استمرارية الأعمال

1.14 إدارة نواحي أمن المعلومات واستمرارية الأعمال



1.1.14 تضمين أمن المعلومات في عملية إدارة استمرارية الأعمال

:

(

:(2-1-14)

(2-17)

(

)

(

(

(

)

(

(

(

(

(

(3-1-14)

(

(5-1-14)

(

.(1-1-6)

2.1.14 تواصل الأعمال وتقييم المخاطر

)

:

(

3.1.14 وضع وتنفيذ خطط الاستمرارية المتضمنة على أمن المعلومات

:

(

(

(

(

(

(

(

:

.

.

.

(3-1-14)

4.1.14 الهيكل الإطاري لتخطيط تواصل الأعمال:

:

)

(

(

(

(

(

(

(

(

(

(

() ()

:

(

(

(

(

(

(

() (

() (

:

(

(

(

(

(

(

(

(

(

(

(

)

(

(

(

)

(

3.1.15 حماية السجلات التنظيمية

(12.3)

()

:

(

(

(

(

.

.1-15489

4.1.15 حماية البيانات والخصوصية والمعلومات الشخصية

() .

5.1.15 منع إساءة استخدام المعلومات ومرافق المعالجة

(6.1.4)

/ ()

(11.5.1).

)

/

(

6.1.15 لائحة ضوابط التشفير

:

/

(

/

(

(

(

2.15 الامتثال للسياسات والمعايير الأمنية والفنية

:

1.2.15 الامتثال للسياسات والمعايير الأمنية

(

(

(

(

(6.1.8)

.10.10

2.2.15 التحقق من الامتثال التقني

)

/

(

3.15 اعتبارات مراجعة نظم المعلومات

/	:
---	---

1.3.15 مراجعة ضوابط نظم المعلومات

:

(

(

(

(

(

(

(

(

(

2.3.15 حماية أدوات مراجعة نظم المعلومات

() 9.1.2) 6.2.1 .