المعايير الدولية لسياسات أمن المعلومات: دراسة تحليلية لمعايير المنظمة الدولية للتوحيد القياسي (آيزو27002 : ISO/IEC 27002) ومدى تطبيقها في الجامعات العربية.

إعداد

د / أحمد عبادة العربي

أستاذ علم المعلومات المساعد

جامعة طنطا – مصر

aiaamr@hotmail.com

المستخلص:

تهدف الدراسة إلى تحليل معايير آيزو 27002 لإدارة أنظمة أمن المعلومات والصادرة عن المنظمة الدولية للتوحيد القياسي(آيزو)، والتعرف على السياسات والتوجيهات التي تتضمنها المعايير ومدى التزام أفضل الجامعات العربية بها. واستخدم الباحث المنهج الوصفي التحليلي للتعرف على مكونات معايير آيزو 27002 ومدى تطبيقها في مواقع أفضل الجامعات العربية حسب تصنيف ويبومتركس لتقييم الجامعات والمعاهد CSIC -Webometrics عام 2012، بالإضافة إلى منهج تحليل المضمون لتحليل عناصر معايير 27002 الفرعية. وتم الاعتماد على قائمة مراجعة تضم عناصر معايير تقييم أمن المعلومات لتطبيقها على مواقع أفضل الجامعات العربية، وتوصل الباحث إلى أن جميع جامعات الدراسة حرصت على تطبيق معايير فرعية في (11) معيارًا أساسيًا بنسبة 28.20% من إجمالي معايير آيزو 27002، وكان معيار السياسات الأمنية هو أقل المعايير تطبيقا بنسبة 19.05% من الجامعات العربية موضوع الدراسة، وجاءت جامعة الملك عبد العزيز في المرتبة الأولى بتطبيق 95 معيارا بنسبة 71.43% من إجمالي المعايير، تليها جامعة الملك فهد للبترول والمعادن بنسبة 58.65%، ثم جامعة أم القرى بنسبة 52.63%، ثم الجامعة الأردنية بنسبة 51.88%. ووصلت نسبة الجامعات التي لم تحقق 50% من المعايير الفرعية 80.95% من إجمالي الجامعات العربية موضوع الدراسة.

تمهيد:

لقد أصبح اختراق أنظمة المعلومات و نظم الشبكات و المواقع المعلوماتية خطراً يقلق العديد من المنظمات في السنوات الأخيرة و مع مرور الزمن نجد أنه على الرغم من سبل الحماية التي تتبعها المنظمات، إلى أن هناك ارتفاعا واضحا في معدل الاختراقات مع تنوع الوسائل المستخدمة في الاختراق أما عن طبيعة الأخطار التي يمكن أن تواجهها نظم المعلومات فهي عديدة، فالبعض منها قد يكون مقصودًا كسرقة المعلومات أو إدخال الفيروسات و غيرها و هي الأشد ضررا على نظم المعلومات، و قد يصعب أحيانا التنبؤ بالدوافع العدائية للأشخاص الذين يقومون بها، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية و الكوارث الطبيعية.

نظراً لأهمية أمن المعلومات لكل المؤسسات الحكومية والخاصة، وأنه أصبح ضرورة لا غنى عنها في ظل التطور المستمر في تقنيات المعلومات وما صاحبه من تطور آخر في أساليب اختراق البيانات والمعلومات، لذا حرصت العديد من المنظمات العالمية وعلى رأسها المنظمة الدولية للتوحيد القياسي (آيزو)International Organization for Standardization (ISO) على وضع معايير لضبط أمن المعلومات بالمؤسسات والمنظمات وهي منظمة تعمل على وضع المعايير، وتضم ممثلين من عدة منظمات قومية للمعايير. بالرغم من أنها منظمة غير حكومية، ولكن قدرتها على وضع المعايير التي تتحول عادة إلى قوانين (إما عن طريق المعاهدات أو المعايير القومية) تجعلها أكثر قوة من معظم المنظمات غير الحكومية.

أهداف الدراسة:

تهدف الدراسة إلى وصف وتحليل معايير آيزو 27002 لإدارة أنظمة أمن المعلومات، والتعرف على السياسات والتوجيهات التي تتضمنها المعايير،ومدى التزام أفضل الجامعات العربية بهذه المعايير.

ولأغراض الدراسة تم تقسيم هذا الهدف الرئيس إلى عدة أهداف فرعية هي:

- التعرف على أهم المعايير والقوانين الدولية لأمن المعلومات.
- تحليل عناصر وسياسات وتوجيهات معايير آيزو 27002 لأمن المعلومات.
- تطبيق معايير آيزو 27002 على مواقع أفضل الجامعات العربية.
- تحديد مواطن القوة والضعف في سياسات أمن معلومات الجامعات العربية.
- ترتيب الجامعات العربية حسب تطبيقها لمعايير أيزو 27002 لأمن المعلومات.

تساؤلات الدراسة:

تحاول الدراسة الإجابة عن التساؤلات الآتية:

1. ما أهم المعايير الدولية لأمن المعلومات؟
2. ما المقصود بمعايير الأيزو 27000 – 27006 لأمن المعلومات؟
3. ما العناصر الأساس والسياسات التوجيهات الفرعية لمعايير الأيزو 27002 لسياسات أمن المعلومات؟
4. ما مدى التزام أفضل الجامعات العربية بتطبيق معايير الأيزو 27002؟
5. ما مواطن القوة ومواضع الضعف في سياسات أمن معلومات مواقع الجامعات العربية؟
6. ما أفضل جامعة عربية حسب تطبيق معايير أيزو 27002 لأمن المعلومات؟

منهج الدراسة وأدواتها:

اعتمدت الدراسة على المنهج الوصفي التحليلي للتعرف على مكونات معايير أيزو 27002 ومدى تطبيقها في مواقع أفضل الجامعات العربية حسب تصنيف ويبومتركس 2012، بالإضافة إلى منهج تحليل المضمون، لتحليل عناصر معايير 27002 الفرعية، من خلال إعداد قائمة مراجعة تضم عناصر تقييم أمن المعلومات لتطبيقها على مواقع أفضل الجامعات العربية.

عينة الدراسة:

تناولت الدراسة معايير الأيزو 27002 كونه أشهر معايير سياسات أمن المعلومات والذي يتكون من (12) فصلًا هي:

1. تقييم المخاطر ومعالجتها
2. السياسة الأمنية Security policy
3. تنظيم أمن المعلومات Organization of information security
4. إدارة الأصول Asset management
5. أمن الموارد البشرية Human resources security
6. الأمن المادي والبيئي Physical and environmental security
7. الاتصالات وإدارة العمليات Communications and operations management
8. التحكم في الوصول access control
9. حيازة وتطوير وصيانة أنظمة المعلومات Information systems acquisition development and maintenance
10. إدارة حوادث أمن المعلومات Information security incident management
11. إدارة استمرارية الأعمال Business continuity management

12. إدارة الامتثال أو التوافق Compliance management

تم تطبيق هذه المعايير على أفضل (20) جامعة عربية حسب تصنيف ويبومتركس لتقييم الجامعات والمعاهد Webometrics- CSIC *يناير عام 2012*، (Spanish, 2012) بالإضافة إلى جامعة طيبة والتي يعمل بها الباحث حالياً وتم اضافتها بناءً على توصية عمادة البحث العلمي بالجامعة.

الجدول رقم (1) ترتيب الجامعات العربية حسب تصنيف ويبومتركس لتقييم الجامعات والمعاهد عام 2012

م	الجامعات	الدولة	الترتيب العالمي	الترتيب العربي
1	جامعة الملك سعود	السعودية	214	1
2	جامعة الملك فهد للبترول والمعادن	السعودية	458	2
3	جامعة الملك عبد العزيز	السعودية	699	3
4	جامعة القاهرة	مصر	770	4
5	الجامعة الأمريكية في القاهرة	مصر	1043	5
6	الجامعة الأمريكية في بيروت	لبنان	1080	6
7	جامعة عين شمس	مصر	1094	7
8	جامعة الإمارات العربية المتحدة	الامارات	1157	8
9	جامعة الكويت	الكويت	1199	9
10	جامعة الملك فيصل	السعودية	1211	10
11	جامعة الخرطوم	السودان	1216	11
12	جامعة السلطان قابوس	سلطنة عمان	1261	12
13	الجامعة الأردنية	الأردن	1310	13
14	جامعة المنصورة	مصر	1373	14
15	جامعة قطر	قطر	1443	15
16	جامعة النجاح الوطنية	فلسطين	1542	16
17	جامعة أم القرى	السعودية	1592	17
18	جامعة الأردنية للعلوم والتكنولوجيا	الأردن	1594	18
19	جامعة الزقازيق	مصر	1682	19
20	جامعة الشارقة	الإمارات	1694	20
21	جامعة طيبة	السعودية	4384	62

الدراسات السابقة:

من خلال البحث في مصادر المعلومات التقليدية والالكترونية باللغتين العربية والانجليزية لا توجد دراسة واحدة (على حد علم الباحث) تناولت موضوع معيار أيزو 27002 لسياسات أمن المعلومات، وإنما تركز الدراسات على موضوع أمن المعلومات والخصوصية، وحماية الملكية الفكرية في ظل البيئة الإلكترونية وتوصل الباحث إلى عدد من السياسات والمعايير الدولية والإقليمية منها:

السياسة التي وضعها (مجلس أبو ظبي للتعليم 2010) والتي تتكون من مقدمة وأحد عشر قسمًا رئيسًا، حيث ورد في المقدمة توضيح الهدف من السياسة ونطاقها، وطريقة توزيع الأدوار والمسؤوليات، وعدد من التعريفات الإجرائية، ثم تم استعراض أقسام السياسة بالشرح والتوضيح، فتناول القسم الأول السياسة

الأمنية والقسم الثاني الأمن المؤسسي، ثم إدارة الأصول، وأمن الموظفين، والأمن المادي والبيئي، و إدارة الاتصالات والعمليات، والتحكم في الأصول، وتطوير وصيانة الأجهزة، وإدارة الحوادث وأمن المعلومات، وإدارة واستمرارية العمل، والالتزام.

وضع مركز أبو ظبي للأنظمة الالكترونية والمعلومات(2009) عدداً من المعايير لتمكن حكومة أبو ظبي من خلق بيئة من الثقة بين جهاتها ومواطنيها وشركائها في العمل، وتوفر الإجراءات الإدارية والوظيفية اللازمة لإدارة مخاطر المعلومات وتتكون المعايير من خمسة أقسامًا رئيسة هي: الخلفية العامة، والأهداف، ونطاق المعايير ، والالتزام والتنفيذ. وتسعى هذه المعايير للتطوير المستمر لأمن المعلومات، والخدمات المقدمة من حكومة أبو ظبي وأجهزتها المساندة.

المعايير التي وضعتها (حكومة أبو ظبي 2008) لسياسات أمن المعلومات والتي تتكون من مقدمة وسياسات أمن المعلومات والمهام والمسؤوليات وملحقين للمصطلحات والتعريفات. وتناولت مقدمة المعايير، والغاية من وضع سياسة أمن المعلومات بإمارة أبو ظبي ونطاقها، والتقيد بها وتنفيذها، والسلطات المخول لها تنفيذ والإشراف على هذه السياسة. أما معايير سياسات أمن المعلومات فتشتمل على (14) عنصرًا هي: الإستراتيجية والتخطيط، والسياسة والمعايير، وإدارة المخاطر، والتوعية والتدريب، والاتصال والتواصل الإعلامي، وإدارة الأداء، وإدارة المخزون، وأمن الموارد البشرية، وأمن المرافق، وإدارة الاتصالات، ووسائل الدخول، وحيازة نظم المعلومات، وإدارة الحوادث، وإدارة استمرارية الأعمال. أما المهام والمسؤوليات فتتكون من ثمانية عناصر هي: الأمانة العامة ومركز أبو ظبي للأنظمة الالكترونية والمعلومات ومكتب أمن المعلومات، وجهاز أبو ظبي للمحاسبة، والقيادة العامة لشرطة أبو ظبي، ومجموعة عمل أمن المعلومات، والجهات الحكومية في إمارة أبو ظبي، والمتعاقدون ومؤسسات الطرف الثالث.

معيار آيزو 27001 (2005) والذي يهدف إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل ورصد واستعراض وصيانة وتحسين وتوثيق نظام إدارة أمن المعلومات داخل المنظمة. وينطبق هذا المعيار على جميع المؤسسات والمنظمات الحكومية والتجارية، ووضع هذا المعيار ليتم تطبيقه على أربعة مراحل هي: تأسيس نظام لإدارة أمن المعلومات، والبدء في تنفيذ الخطط وتشغيلها، ومراجعة النظام بعد تنفيذه، وصيانة وتحسين النظام. ويتكون المعيار من 11 قطاعًا فرعيًا من المعايير هي: السياسة الأمنية، والتأمين التنظيمي، وإدارة الأصول، وأمن الموارد البشرية، وأمن المرافق والبيئة المحيطة، وإدارة الاتصالات والعمليات، والتحكم بالدخول، وحيازة أنظمة المعلومات، وإدارة حوادث أمن المعلومات، و إدارة استمرارية العمل، والتوافق.

معيار ITIL (2003) هو اختصار لـ The Information Technology Infrastructure Libraryويسمى أيضاً آيزو 20000. هو عبارة عن مجموعة من أفضل الممارسات في مجال إدارة خدمات تقنية المعلومات (ITSM) ، ويركز على خدمة عمليات تقنية المعلومات ويعتبر المرجع الرئيس للمستخدم، وقد تم بناؤه بواسطة مكتب المملكة المتحدة للتجارة الحكومية(OGC) وإدارة خدمة التقييم الذاتي، و يتم العمل به عن طريق وضع استبيانات على الإنترنت، ويتكون من 11 قسمًا هي: إدارة مستوى الخدمة، والإدارة المالية وإدارة بناء القدرات، وإدارة استمرارية الخدمة، و إدارة الإتاحة، وإدارة الخدمات، وإدارة الحوادث، وإدارة المشكلات، وإدارة التكوين ، وإدارة التغيير، وإدارة الإصدار.

أما الدراسات التي تناولت موضوعات التحديات الأمنية والخصوصية، و أمن المعلومات، و الملكية الفكرية، و تقييم إدارة المخاطر، و الجريمة الالكترونية، فمنها:

دراسة (النقيب، 2010) التي تتناول التحديات الأمنية لمشاريع الرقمنة بمؤسسات المعلومات العربية ونظمها وتطبيقاتها في البيئة الرقمية المحملة على شبكات المعلومات وقابليتها للتعرض للضرر والخطر، مثل اختراقات ومخاطر نظم إدارة المحتوى الرقمي وفاعلية الآليات المطبقة لإدارة المخاطر، ومكونات نظم إدارة المحتوى الرقمي . وتمثلت عينة الدراسة في سبعة مشاريع رقمية عربية هي :

مستودع الأصول الرقمية لمكتبة الإسكندرية، و ومكتبة الوراق الرقمية، ومكتبة ببليواسلام الرقمية، ومركز توثيق التراث الحضاري والطبيعي ، ومكتبة المدينة الرقمية، ودار الكتب المصرية ومكتبة الملك فهد الوطنية. وتوصل الباحث إلى عدم كفاية إجراءات الرقابة المطبقة لمواجهة المخاطر التي تتعرض لها ثلاثة عناصر من مكونات إدارة المحتوى الرقمي بمؤسسات المعلومات العربية، نتيجة التركيز على الجوانب الفنية دون الاهتمام بالجوانب الأمنية.

تتناول دراسة (المشهداني،2010) تعريف الخصوصية وأركان جريمة المعالجة الالكترونية للبيانات الشخصية دون ترخيص والعلاقة بين حماية الأمن القومي وحماية الخصوصية، وتعرض الباحث إلى بعض صور إساءة استخدام التقنيات في انتهاك الخصوصية، مثل تعديل أو إزالة أو نقل بيانات الأفراد، كما تناولت مواد القانون الفرنسي رقم 17 لسنة 1987/ والمتعلقة بحماية البيانات الشخصية المعالجة الكترونياً . وأوصى الباحث بوضع القوانين الرادعة التي تضمن حماية الخصوصية، ووضع ضوابط تنظيمية لتداول البيانات والمعلومات الشخصية، ونشر الوعي بأهمية احترام الحق في الحياة الالكترونية الخاصة بجميع أشكالها وصورها.

دراسة (فؤاد، 2010) التي تناولت الجريمة الالكترونية من حيث تعريفها وتاريخ ظهورها وفئاتها، ومظاهر الاحتيال في عالم النشر الالكتروني من حيث النسخ غير الشرعي وسرقة المعلومات والبرامج، كما تناول الباحث قضية أمن المعلومات بين الأخلاقيات والتشريعات، وتناول كذلك واقع تشريعات أمن المعلومات في الجزائر وفق القانون رقم 05/03 لعام 2003 والذي يتعلق بحقوق الملكية الفكرية والذي يتضمن المصنفات الفنية وقواعد المعلومات وبرامج الحاسب الآلي.

تناولت دراسة (عرب 2009) الحقائق التاريخية لعلاقة تقنية المعلومات بالنظام القانوني، وملامح التنظيم القانوني الدولي والمقارن لتقنية المعلومات و اطار الحماية القانونية للمعلومات والحماية القانونية للأداء الرقمي، والمرتكزات العامة لقوانين تقنية المعلومات، والنظام القانوني لحماية المصنفات الرقمية، وموقف النظام القانوني العربي من حماية المعلومات والمصنفات الرقمية، والنظام القانوني العربي للملكية الفكرية وحماية المصنفات الرقمية، وتشريعات الملكية الفكرية في الوطن العربي، وإشكالات حماية البرمجيات وقواعد البيانات، وحماية البرمجيات بين تطبيق القانون وآثره على الدول النامية، وأوصى الباحث بوضع قواعد حماية للمعلومات والبيانات الخاصة تضبط جمعها ومعالجتها وتداولها ونقلها داخليا وخارجيا حفاظا على الخصوصية وتحقيقا لمبادئ حماية البيانات الخاصة المقررة دوليا ، ووضع تشريعات منظمة لقواعد التجارة الالكترونية من حيث متطلباتها التقنية والإدارية وقواعد حمايتها وحل مشكلات التواقيع والعقود الالكترونية، ومشكلات الإخفاق في التسليم المادي للمنتج بعد اكتمال التعاقد.

دراسة (Kuegah 2009) التي تتناول تحليل الآليات التي تستخدمها المؤسسات التي تتحول إلى الشكل الرقمي في تقييم إدارة المخاطر التي تتعرض لها في ظل البيئة الجديدة، وتوصلت الدراسة إلى أن التدمير المتعمد وغير المتعمد للبيانات وإدخال البيانات بطرق غير صحيحة من قبل العاملين، وإدخال بيانات غير سليمة بطريقة متعمدة ، وكذلك استخدام البرامج الخبيثة وعدم الاحتفاظ بنسخ احتياطية من البيانات والملفات، والحوادث الطبيعية وانقطاع التيار الكهربائي، هذه العوامل تمثل أخطر الاختراقات لنظم المعلومات.

تناولت دراسة (Wan 2008) العوامل التي تؤثر على نظام أمن المعلومات في المكتبات الرقمية من حيث إعدادات الشبكة، والبيئة المحيطة، و الفيروسات، والقرصنة. وتوصلت الدراسة إلى أن تطبيق الجانب غير التقني في إدارة المخاطر، غير المرتبط بالجوانب الفنية، يساعد على تقليص المخاطر الداخلية، وأن وجود سياسة لأمن المعلومات مكتوبة ومعلنة تساعد على حماية أمن النظام، وأوصت الدراسة بضرورة اعتماد إجراءات رقابية تمنع خرق القوانين والتنظيمات واللوائح الداخلية، وأن تراجع هذه التنظيمات بصفة دورية لتجنب سوء استخدام موارد النظام

دراسة (علوي 2007) والتي تناولت مفهوم الملكية الفكرية وأنواعها (حقوق الطبع – العلامات التجارية – براءات الاختراع) ثم تناولت المصنفات الرقمية مثل برامج الحاسب الآلي وقواعد المعلومات والدوائر المتكاملة. كما تناولت بالتحليل كيفية حماية الإنتاج الفكري الرقمي من منظور أعضاء هيئة التدريس بجامعة منتوري بالجزائر. وتوصلت الباحثة إلى أن 66.53% من مجتمع الدراسة يطالبون بإصدار تشريعات جديدة لحماية الإنتاج الفكري الرقمي ، وطالب 48.63% من العينة بضرورة التنسيق بين الدول العربية في مجالات حماية الإنتاج الفكري الرقمي ، كما طالب 35.8% من العينة بتبني التشريعات الدولية للملكية الفكرية وتطبيقها في الدول العربية.

تناولت دراسة (الهادي، 2006) موضوع أمن المعلومات في ظل الحكومة الإلكترونية، والتي تبدأ بمقدمة عامة حول تكنولوجيا المعلومات ، ثم تناولت خدمات نظم المعلومات في البيئة الرقمية، وأمن المعلومات في البيئة الرقمية، ثم ناقشت متطلبات الأمن الطبيعي لنظم المعلومات، وعرضت لبعض الاعتبارات والأبعاد المتعلقة بأمن المعلومات، والأضرار الناجمة عن قصور أمن المعلومات كما حددت الدراسة الأبعاد والمكونات الأساس لأمن المعلومات ومنها سياسة وتنظيم أمن المعلومات وتصنيف الأصول وأمن الأفراد والأمن البيئي والرقابة على الأصول، أوصت الدراسة بإقامة أطر سياسية وتنظيمية وقانونية لمواجهة الأمور المتعلقة بمخاطر الأمن كالقرصنة وإدارة أسماء النطاق وحماية المواطنين وتوسيع هذه الحماية في البيئة الرقمية، وتنظيم حملات عامة لنشر الوعي تهدف إلي تحسين معرفة الجمهور وتفهمهم بأهمية أمن المعلومات وحقوق الملكية الفكرية وحماية البرمجيات، وتعزيز المبادرات التي تضمن التوازن العادل بين حقوق الملكية الفكرية ومصالح مستخدمي المعلومات في مجالات البرمجيات والتجارة الإلكترونية والحكومة الإلكترونية، وتحديد وتخصيص المخاطر والمسؤولية القانونية المتصلة بفشل أمن المعلومات، وما يرتبط بها من جزاءات وعقوبات إدارية وجنائية ترتبط بسوء الاستخدام أو تعمد الضرر، كما أوصت الدراسة كذلك بإصدار القوانين والتشريعات التي تحدد صحة العقود والوثائق المنشأة والمنفذة من قبل نظم المعلومات.

تناولت دراسة (عرب، 2006) عرضاً أولياً لمحتويات القوانين المقارنة في حقل جرائم الكمبيوتر والانترنت والاتجاهات العامة للقانون المقارن بشأن جرائم الحاسوب، والإطار القانوني لجرائم الكمبيوتر والانترنت في الولايات المتحدة الأمريكية، وتقييم الإطار التشريعي الأمريكي لجرائم الكمبيوتر والانترنت، والإطار القانوني الأوروبي لجرائم الكمبيوتر والانترنت، واتفاقية بودابست 2001 للجرائم الالكترونية ، والتدابير المتعين اتخاذها على المستوى العربي، وواقع مكافحة جرائم الكمبيوتر واتجاهاتها التشريعية في البيئة العربية، ومدي توافر التشريعات الكافية في البيئة العربية لمواجهة جرائم الكمبيوتر والانترنت، وأوصى الباحث بإنهاء حالة التشابك والتخبط والقصور في المعالجات التشريعية المتصلة بالعصر الرقمي والعمل على هذا الموضوع بصورة شمولية لوضع أدوات تشريعية ملائمة في مختلف فروع قانون تكنولوجيا المعلومات وفي مقدمتها الجرائم الالكترونية.

المعايير الدولية لأمن المعلومات:

معايير المنظمة الدولية للتوحيد القياسي:

أنشئت المنظمة الدولية للتوحيد القياسي عام 1947م وهي منظمة غير حكومية تتعاون مع كل من اللجنة الدولية الكهروتقنية والاتحاد الدولي للاتصالات.

من أهم المعايير التي أصدرتها الآيزو، مجموعة معايير أمن المعلومات والتي تسمى "مواصفات نظم إدارة أمن المعلومات" (آيزو 27000) والتي تتكون من ستة معايير فرعية هي:

- 27001 الأسس والمفردات
- 27002 قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات
- 27003 دليل تنفيذ إدارة أمن المعلومات
- 27004 قياس فعالية نظم إدارة أمن المعلومات

- 27005 إدارة مخاطر أمن المعلومات
- 27006 دليل لعملية المصادقة على نظام إدارة امن المعلومات

معيار 27002

هو أحد سلسلة معايير أيزو27000 الصادرة عن المنظمة العالمة للتوحيد القياسي، والذي يهدف إلى إنشاء نظام إدارة أمن المعلومات، ويستخدم في المؤسسات لتحديد الأهداف والمطالب الأمنية، والتوافق مع التشريعات والقوانين، ووضع إجراءات جديدة لإدارة أمن المعلومات وتحديد المسؤوليات والضوابط وإدارة أصول المؤسسة.

بنية معيار 27002:

يتكون معيار 27002 من (12) فصلًا، تشتمل على (39) معيارًا رئيسًا، والتي تضم (133) معيارًا فرعيًا كما في الجدول التالي:

الجدول رقم(2) المعايير الرئيسة والفرعية لمعيار 27002 لسياسات أمن المعلومات

الفصول	عناوين الفصول	عدد المعايير الرئيسة	عدد المعايير الفرعية
الفصل الأول	تقييم المخاطر ومعالجتها	مقدمة نظرية	
الفصل الثاني	السياسات الأمنية	1	2
الفصل الثالث	تنظيم أمن المعلومات	2	11
الفصل الرابع	إدارة الأصول	2	5
الفصل الخامس	أمن الموارد البشرية	4	21
الفصل السادس	الأمن المادي والبيئي	2	13
الفصل السابع	إدارة العمليات / الاتصالات	10	32
الفصل الثامن	التحكم في الوصول	7	25
الفصل التاسع	حيازة وتطوير وصيانة أنظمة المعلومات	6	16
الفصل العاشر	إدارة حوادث أمن المعلومات	2	5
الفصل الحادي عشر	إدارة استمرار العمل	1	5
الفصل الثاني عشر	الامتثال والتوافق	3	10
الإجمالي	**12**	**39**	**133**

كل معيار من معايير 27002 الرئيسة يتكون من أربعة عناصر رئيسة هي:

- أهداف المعيار (توضح أهداف المعيار الرئيس داخل المؤسسة)
- الضوابط (عدد من الضوابط التي تحقق أهداف المعيار داخل المؤسسة)
- توجيهات التطبيق (معلومات مفصلة تدعم تطبيق الضوابط)
- معلومات أخرى (معلومات إضافية قد تكون من المفيد أخذها في الاعتبار مثل المعلومات القانونية أو الإحالة إلى معايير أخرى ذات الصلة).

وفيما يلي عرض تحليلي لمعايير 27002 وهدف وضوابط وتوصيات كل منها على حده.

الفصل الأول: تقييم المخاطر ومعالجتها:

هذا الفصل عبارة عن مقدمة عن تقييم المخاطر الأمنية، من حيث كيفية تقدير حجم المخاطر (تحليل المخاطر) وتحديد أثرها، ويهدف إلى تقييم المخاطر الأمنية بشكل دوري لمعالجة الثغرات في المتطلبات الأمنية مثل: الأصول، والثغرات الأمنية، والآثار المرتبة على هذه المخاطر.

ومن أهم الضوابط التي وردت في هذا الفصل هي ضوابط " معالجة مخاطر الأمن" ومنها:

- تطبيق ضوابط لتقليص المخاطر.
- التوافق مع اللوائح والقوانين المحلية والدولية.
- ضوابط التشغيل.
- الموازنة بين تطبيق وتشغيل الضوابط والضرر المتوقع حدوثه من الثغرات الأمنية.

الفصل الثاني: السياسة الأمنية

يتكون هذا الفصل من معيار رئيس واحد هو" سياسة أمن المعلومات " ويهدف هذا المعيار إلى توجيه إدارة المؤسسة ودعمها في طريقة تعاملها مع أمن المعلومات والتوافق مع القوانين واللوائح ذات الصلة، ويشتمل على معيارين فرعيين هما:

1. الوثيقة العامة لسياسة أمن المعلومات.
2. المراجعة لسياسة أمن المعلومات.

ومن أهم توجيهات التطبيق التي وردت تحت هذين المعيارين:

- إجازة وثيقة أمن المعلومات من الإدارة العليا للمؤسسة وتعميمها على كل المنسوبين والجهات الخارجية ذات العلاقة.
- ضرورة أن تنص وثيقة سياسة أمن المعلومات على موافقة الإدارة العليا وأن تضع رؤية المنظمة في إدارة أمن المعلومات.
- إذا تم توزيع وثيقة أمن المعلومات خارج المنظمة يجب الانتباه إلى عدم احتوائها على معلومات حساسة عن المنظمة.

الفصل الثالث: تنظيم أمن المعلومات:

يهدف هذا الفصل إلى تنظيم وإدارة أمن المعلومات داخل المنظمة، من حيث موافقة الإدارة العليا على وثيقة أمن المعلومات وتحديد الأدوار والمسؤوليات وتنسيق ومراجعة تطبيق الأمن في جميع إدارات المنظمة.

ويتكون هذا الفصل من معيارين رئيسيين هما تنظيم أمن المعلومات داخليا، وأمن المعلومات والأطراف الخارجية، ويتكون المعيار الأول من (8) معايير فرعية ويتكون المعيار الثاني من (3) معايير فرعيين يوضحها الشكل رقم(1):

الشكل رقم (1) المعايير الفرعية بمعيار تنظيم أمن المعلومات.

التنظيم الداخلي لأمن المعلومات

- التزام الإدارة العليا بأمن المعلومات.
- التنسيق بين الإدارات العليا بأمن المعلومات.
- تحديد المسؤوليات.
- ترخيص مراجعة أمن المعلومات.
- الاتفاقيات السرية.
- التواصل مع الجهات المختصة.
- التواصل مع الجهات ذات العلاقة.
- المراجعة الدورية لأمن المعلومات.

الأطراف الخارجية

- تحديد المخاطر ذات الصلة بالأطراف الخارجية.
- المعالجة الأمنية عند التعامل مع العملاء.
- المعالجة الأمنية عند التعامل مع الأطراف الخارجية

1/3 التنظيم الداخلي لأمن المعلومات.

عرضت المعايير مجموعة من توجيهات التطبيق تخص هذا المعيار الفرعي وهي:

- الصياغة والمراجعة والموافقة على وثيقة سياسة أمن المعلومات.
- توفير الموارد المادية والبشرية اللازمة لتحقيق أمن المعلومات.
- تحديد المسؤوليات والمهام في جميع وحدات المنظمة.
- التعاون بين المدراء والمراجعين وأفراد الأمن والشؤون القانونية وتقنية المعلومات في تنفيذ وثيقة أمن المعلومات.
- تعيين وتحديد الجهة المسؤولة عن أي أصل موجود وعن أي عملية أمنية وأن تكون عملية التعيين والتحديد محددة وموثقة.
- الترخيص الإداري لمرافق أمن المعلومات.
- فحص الأجهزة والبرمجيات للتأكد من أنها متوافقة تشغيليا مع مكونات النظم الأخرى.
- وضع ضوابط لاستخدام الحاسبات المحمولة عند اتصالها بشبكة المؤسسة، لعدم التسبب في إحداث ثغرات أمنية.
- مراجعة الاتفاقيات السرية الخاصة بعدم الكشف عن المعلومات بصفة منتظمة.
- وضع تعريف محدد للمعلومات التي يجب حمايتها.
- تحديد الجهات المختصة ذات العلاقة بأمن معلومات المؤسسة مثل " وحدات الإطفاء – الإسعاف – طوارئ الكهرباء والمياه والاتصالات..."
- المشاركة وتبادل المعلومات حول التقنيات الحديثة والمنتجات والتهديدات والثغرات الأمنية.
- عقد اتفاقيات للتعاون في مجالات القضايا الأمنية مع الجهات ذات العلاقة.
- مراجعة وتقييم كفاءة أمن المعلومات وتحسين الأداء من خلال أفراد متخصصين في المراجعات الأمنية.

2/3 الأطراف الخارجية:

يهدف هذا المعيار إلى الحفاظ على أمن المعلومات بالمنظمة وعلى مرافق معالجة المعلومات التي يمكن الوصول إليها أو تلك التي تعالج أو تدار من أطراف خارجية والتحكم والسيطرة على دخول هذه الأطراف، وأخذ الاحتياطات الأمنية اللازمة لإتاحة المعلومات ومرافقها للأطراف الخارجية.

ومن أهم التوجيهات التي وردت تحت هذه المعايير الفرعية ما يلي:

- حصر وتحديد الأطراف الخارجية (مقدمي خدمات الانترنت – مزودي الشبكات وخدمات الهاتف - الصيانة والدعم الفني – إدارة الخدمات الأمنية – الاستضافة الخارجية للمواقع – المستشارون – مراجعي الحسابات – الموردين – الموظفين المؤقتين...)
- تحديد مرافق معالجة المعلومات المتاحة للأطراف الخارجية.
- تحديد نوع الوصول المتاح للأطراف الخارجية.
- تحديد قيمة وحساسية المعلومات المتاحة للأطراف الخارجية.
- وضع ضوابط لحماية المعلومات التي لا ينبغي أن تصل إلى الأطراف الخارجية.
- تحديد المرافق التي تستخدمها الأطراف الخارجية عند تخزين ومعالجة وتوصيل المعلومات.
- تحديد المتطلبات القانونية والتنظيمية التي ينبغي أن تؤخذ في الاعتبار عند التعاقد مع الأطراف الخارجية.
- وضع قيود على نسخ المعلومات أو الكشف عنها عن طريق الأطراف الخارجية

الفصل الرابع: إدارة الأصول

يتكون هذا الفصل من معيارين يشتملان على خمسة معايير فرعية، ويهدف إلى تحقيق الحماية المناسبة لأصول المنظمة وتصنيفها من حيث القيمة والمتطلبات القانونية والحساسية.

1/4المسؤولية تجاه الأصول

يهدف هذا المعيار إلى حصر كل أصول المنظمة وتسمية مالكيها وصيانتها وإنشاء سجلات لتوثيقها وحفظها ويتكون هذا المعيار من ثلاثة معايير فرعية هي:

1. تصنيف وجرد الأصول.
2. تحديد ملكية الأصول.
3. الاستخدام الأمثل للأصول.

ومن أهم التوجيهات التي وردت تحت هذه المعايير ما يلي:

- تحديد أنواع الأصول (المعلومات – الأصول البرامجية – الأصول المادية – خدمات المعلومات – الأفراد – سمعة وصورة المنظمة الذهنية)
- تحديد كل الأصول بوضوح وإنشاء سجل لحفظها.
- تحديد مستوى الحماية المناسبة لأهمية الأصل المعلوماتي.
- تحديد ملكية كل أصل من أصول المنظمة بوضوح.
- تحديد وتوثيق وتطبيق الاستخدام الأمثل للمعلومات وللأصول ومرافق المعلومات.
- وضع ضوابط لاستخدام الانترنت والبريد الالكتروني والهاتف المحمول.

2/4 تصنيف المعلومات

يهدف هذا المعيار إلى ضمان أن المعلومات تلقى مستوى مناسبًا من الحماية، وتحديد درجة حساسية معلومات المنظمة.

ويتكون من معيارين فرعين هما:

1. المبادئ التوجيهية لتصنيف المعلومات.
2. التعامل مع المعلومات وتميزها.

ومن أهم التوجيهات التي وردت تحت هذين المعيارين ما يلي:

- تصنيف المعلومات حسب قيمتها وحساسيتها.
- مراجعة تصنيف المعلومات على فترات زمنية حيث يمكن تحويل المعلومات من سرية إلى عامة بعد فترة زمنية معينة.
- التداول الآمن للمعلومات المصنفة.
- وضع ضوابط لاشتمال تصنيفات المعلومات على كل من المعلومات المطبوعة والالكترونية.

الفصل الخامس:أمن الموارد البشرية

يهدف هذا الفصل إلى ضمان أن كل الموظفين والمتعاقدين والأطراف الخارجية، قد حددت مسئولياتهم وأنهم مناسبون للأدوار المنوطة بهم، وأنهم على علم بقضايا ومهددات أمن المعلومات، وتوفير قدر مناسب من الوعي والتدريب والتعليم في إجراءات الأمن وفي الاستخدام السليم لمرافق معالجة المعلومات لكافة العاملين، وتقرير آلية رسمية للعقاب لمعالجة الثغرات الأمنية، وأن يتم إنهاء عمل الموظفين أو نقلهم بطريقة منظمة.

ويتكون هذا الفصل من ثلاثة معايير رئيسة كما في الشكل رقم (2):

الشكل رقم (2) المعايير الفرعية بمعيار أمن الموارد البشرية.

1/5 إجراءات سابقة للتوظيف.

يهدف هذا المعيار إلى تعريف وتوثيق المهام والمسؤوليات الأمنية للعاملين، وأن تخضع عمليات الفرز والاختيار والتوظيف إلى معايير متقنة، مع الأخذ في الاعتبار كل القوانين ذات الصلة.
وفيما يلي أهم توجيهات التطبيق التي وردت تحت هذه المعايير الفرعية:

- توفير مرجعيات شخصية كافية عن المتقدمين لشغل الوظائف.
- التأكد من اكتمال ودقة السير الذاتية للمتقدمين.
- التأكد من المؤهلات الأكاديمية والمهنية
- تحديد المسؤوليات القانونية للعاملين
- تحديد مسؤوليات إدارة الأصول والخدمات.

2/5 إجراءات أثناء أداء الوظيفة

يهدف هذا المعيار إلى أن كافة منسوبي المنظمة لديهم القدرة على التعامل مع قضايا أمن المعلومات، وتحديد المسؤوليات الإدارية وتوزيع الاختصاصات لتقليص الأخطاء البشرية قدر الإمكان.
ومن أهم توجيهات التطبيق التي وردت تحت هذا المعيار ما يلي:

- التأكد من أن كل الموظفين على قدر عال من التدريب والتأهيل على قضايا أمن المعلومات قبل السماح لهم بالوصول إلى المعلومات الحساسة ونظم المعلومات.
- التأكد من أن كل المنسوبين ملتزمون بشروط ومهام العمل التي تشمل سياسة أمن المعلومات.
- العمل على تلقي كافة المنسوبين التدريب المناسب والوعي بأمن المعلومات والتحديثات التي تدخل في سياسة المنظمة الأمنية.
- اعتماد لوائح رسمية لعقاب العاملين الذين يرتكبون خروقات أمنية.
- تستخدم عملية العقاب لردع ومنع المنسوبين من انتهاك السياسات الأمنية والإجرائية للمنظمة.

3/5 إنهاء الخدمة أو التعديل في الوظيفة.

يهدف هذا المعيار إلى تنظيم عمليات إنهاء عمل الموظفين أو تغيير وظائفهم، وأن كل المعدات والأجهزة والمعلومات وأسماء المستخدم قد تم استرجاعها وأن كافة صلاحيات الوصول للمعلومات قد تمت إزالتها.

ويوجد العديد من توجيهات التطبيق تحت هذه المعايير الفرعية منها:

- يجب أن يتم وبوضوح تعريف وتخصيص المسؤوليات المتعلقة بإنهاء الخدمة أو تغيير الوظيفة.
- يجب أن تتم عمليات التغيير في الوظائف بنفس إجراءات إنهاء العمل.
- يجب أن تشمل عمليات إنهاء الخدمة إعادة كل البرمجيات والوثائق والمعدات وممتلكات المنظمة الأخرى.
- يجب إلغاء كافة صلاحيات الوصول الفيزيائي والمنطقي لكافة الذين انتهت علاقاتهم الوظيفية بالمنظمة.
- يجب تغيير كلمة المرور للحسابات النشطة والتي يكون الموظف المنهي عمله على علم بها.

الفصل السادس: الأمن المادي والبيئي

يهدف هذا الفصل إلى وضع ضوابط لمنع الوصول المادي غير المرخص به، وتفادي أية أضرار قد تحدث لمباني ومرافق المنظمة ويتكون هذا الفصل من معياريين هما:

1. تأمين المناطق.
2. تأمين المعدات.

يشتمل هذان المعياران على (13) معيارا فرعيا، كما يتضح من الشكل رقم (3):

الشكل رقم (3) المعايير الفرعية بمعيار الأمن المادي والبيئي.

تأمين المناطق	تأمين المعدات
• - أمن المحيط الخارجي. - ضبط المداخل. - تأمين المناطق من الداخل. - الحماية من التهديدات الخارجية. - العمل في محيط آمن. - تأمين المناطق العامة داخل المنظمة	• - تثبيت المعدات وحمايتها. - تأمين أجهزة الكهرباء والمياه والتدفئة. - تأمين الكابلات. - صيانة المعدات. - تأمين المعدات خارج أماكن العمل. - تأمين التخلص من أو - إعادة استخدام المعدات. - نقل الممتلكات.

1/6 تأمين المناطق

يهدف هذا المعيار إلى وضع ضوابط للحماية المادية للمناطق التي تحتوي على المعلومات ومرافق معالجتها، وتأمين المكاتب والقاعات وسبل التأمين ضد الأضرار الناتجة عن الحرائق والفيضانات والزلازل، وتأمين نقاط الدخول وأماكن الشحن والتسليم.

ومن أهم التوجيهات التي وردت تحت هذه المعايير الفرعية ما يلي:

- يجب تحديد الحدود الأمنية لمباني المنظمة بوضوح.

- تحديد وسائل لضبط الدخول الشخصي للمواقع والمباني.
- تشييد حاجز عمراني حول مباني وأراضي المنظمة.
- تسجيل تاريخ ووقت دخول وخروج الزوار.
- يقتصر الوصول إلى مرافق معالجة المعلومات على الأفراد المخولين فقط.
- عدم وضع علامات بارزة أو لوحات تدل على مرافق معالجة المعلومات
- العمل على تفادي الأضرار الناتجة عن تسرب المياه أو النيران
- لا يسمح بإدخال معدات التصوير الفوتوغرافي والفيديو إلى المواقع بدون إذن من الجهات المسؤولة.
- تأمين مناطق الشحن والتفريغ حتى لا يتمكن عمال الشحن من الوصول إلى أجزاء أخرى من المبني.
- فحص المواد والأجهزة قبل دخولها مناطق معالجة المعلومات.

2/6 تأمين المعدات

يهدف هذا المعيار إلى وضع ضوابط لحماية معدات وأجهزة المنظمة من أية أخطار بشرية أو طبيعية وحمايتها من الضياع أو الإتلاف، ومنع الوصول غير المرخص.

ويوجد العديد من التوجيهات والملاحظات التي وردت تحت هذه المعايير ومنها:

- تحديد مواقع الأجهزة والمعدات ووضع ضوابط لحمايتها.
- منع الأكل والشرب والتدخين بالقرب من معدات وأجهزة معالجة المعلومات.
- وضع أجهزة رصد درجات الحرارة والرطوبة والتي يمكن أن تؤثر على أداء المعدات والأجهزة.
- تثبيت خطوط نقل الطاقة والاتصالات تحت سطح الأرض كلما أمكن ذلك.
- فصل خطوط الطاقة عن خطوط الاتصالات لتجنب التشويش.
- صيانة الأجهزة والمعدات دوريا وفقا لمواصفات الجهات المنتجة.
- توفر التغطية التأمينية الكافية لحماية المعدات الموجودة خارج مقر المنظمة.
- استخدام طرق وأساليب مأمونة عند مسح أو تهيئة وسائط التخزين.
- وضع حدود زمنية لنقل المعدات خارج المقر.
- تسجيل المعدات عند نقلها خارج مقر المنظمة.
- وضع نقاط تفتيش لمنع نقل المعدات غير المرخص وفقا للتشريعات واللوائح.

الفصل السابع: إدارة العمليات / الاتصالات

يهدف هذا الفصل إلى وضع إجراءات تشغيلية لجميع مرافق تجهيز ومعالجة المعلومات، ووضع ضوابط لرصد وتوثيق خدمات المعلومات المقدمة من منظمات خارجية، والحماية من البرامج الخبيثة، ووضع سياسات تحظر استخدام البرامج غير المصرح بها. والعمل على امتلاك نسخ احتياطية من المعلومات والبرامج، ووضع ضوابط لحماية أمن شبكة المعلومات بالمنظمة، ووضع معايير للتعامل مع وسائل الإعلام، وكيفية وضع اتفاقيات لتبادل المعلومات والبرمجيات مع منظمات أخرى، وحماية خدمات التجارة الالكترونية، وتوثيق أحداث أمن المعلومات.

ويعتبر هذا الفصل من أكثر الفصول اشتمالا على المعايير الرئيسة والفرعية حيث يتكون من عشرة معايير رئيسة هي:

1. الإجراءات التنفيذية.
2. إدارة تقديم الخدمات لأطراف خارجية.
3. تخطيط وإعداد الأنظمة.
4. الحماية من البرامج الخبيثة.
5. النسخ الاحتياطي.
6. إدارة تأمين الشبكات.
7. التعامل مع وسائط التخزين.
8. تبادل المعلومات.
9. خدمات التجارة الالكترونية.
10. المراقبة والتوثيق.

وتتكون هذه المعايير من 32 معيارا فرعيا يمكن تفصيلها على النحو التالي:

1/7 الإجراءات التنفيذية

يهدف هذا المعيار إلى ضمان التنفيذ الصحيح لإجراءات التشغيل وتأمين مرافق معالجة المعلومات ويتكون من أربعة معايير فرعية هي:

1. توثيق العمليات التشغيلية.
2. إدارة التغيير.
3. تحديد الصلاحيات.
4. الفصل بين مرافق التشغيل

ومن أهم التوجيهات التي وردت تحت هذه المعايير:

- توثيق إجراءات التشغيل، وتسجيل التغيرات الهامة.
- الفصل بين صلاحيات الموظفين وتحديدها بدقة.

2/7 إدارة تقديم الخدمات لأطراف خارجية

يهدف هذا المعيار إلى الحفاظ على مستوى مناسب من أمن المعلومات عند عقد اتفاقيات مع أطراف خارجية لتقديم خدمات المعلومات داخل المنظمة.

ويتكون هذا المعيار من ثلاثة معايير فرعية هي:

1. إيصال الخدمة.
2. مراقبة ومراجعة خدمات الطرف الثالث.
3. إدارة التغيرات في خدمات الطرف الثالث.

ومن أهم التوجيهات التي وردت تحت هذا المعيار ما يلي:

- تحديد ووصف للخدمات المقدمة للأطراف الخارجية بما يضمن أمن وسلامة المعلومات.
- توثيق ورصد التقارير المقدمة من الطرف الثالث بشأن تقديم الخدمات.
- رصد التغيرات التي تحدث من تقديم تحسينات على الخدمات المقدمة.

3/7 تخطيط وإعداد الأنظمة.

يهدف هذا المعيار إلى التخطيط المسبق لضمان اختيار أفضل الموارد والقدرات واختبارها قبل استخدامها.

ويتكون هذا المعيار من معياريين فرعيين هما:

1. إدارة بناء القدرات.
2. نظام القبول.

وورد تحت هذين المعيارين عدداً من توجيهات التطبيق أهمهما:

- تحديد الاحتياجات الفعلية لإدارة النظام.
- وضع معايير محددة لاختيار نظم معلومات جديدة.

4/7 الحماية من البرامج الخبيثة

يهدف هذا المعيار إلى حماية وسلامة البرامج والمعلومات، ومنع إدخال برامج غير مصرح بها للنظام.ويتكون من معيارين فرعين هما:

- ضبط البرامج الخبيثة.
- ضبط مكونات البرامج.

وأهم التوجيهات التطبيقية في هذين المعيارين:

- استخدام أقصى درجات الحماية من البرامج الخبيثة.
- وضع سياسة رسمية تحظر استخدام البرامج غير المصرح بها.
- إجراء اختبارات دورية لنظام المعلومات للكشف عن أية برامج خبيثة.
- التحقق من سلامة الملفات المخزنة على وسائط التخزين وكذلك التي يتم استلامها عن طريق الشبكات.
- تحديد المسؤوليات والإجراءات الإدارية للتعامل مع البرامج الخبيثة.

5/7 النسخ الاحتياطي

يهدف هذا المعيار إلى الحفاظ على سلامة البيانات والمعلومات ومرافقها.

ويتكون من معيار فرعي واحد هو النسخ الاحتياطي للمعلومات وأهم توجيهات التطبيق التي وردت تحته ما يلي:

- امتلاك نسخ احتياطية من المعلومات والبيانات والبرامج واختبارها بانتظام وفق سياسة متفق عليها.
- التأكيد على أن تكون المنظمة قادرة على استرداد المعلومات والبرامج بعد وقوع حوادث أو كوارث.
- تخزين النسخ الاحتياطية في أماكن أمنة بعيدة عن الموقع الرئيس للمنظمة.

6/7 إدارة أمن الشبكة

يهدف هذا المعيار إلى ضمان حماية المعلومات في الشبكات وحماية البنية التحتية الداعمة

يتكون هذا المعيار من معيارين فرعين هما:

1. الضوابط الأمنية للشبكات.
2. تأمين خدمات الشبكات.

وأهم توجيهات التطبيق التي وردت تحتها ما يلي:

- أخذ كل التدابير اللازمة للحفاظ على سلامة معلومات الشبكات.
- توثيق متطلبات خدمات الشبكات ضمن اتفاقيات الخدمة.

7/7 التعامل مع وسائط التخزين

يهدف هذا المعيار إلى منع الوصول غير المصرح لوسائط التخزين وحمايتها من التعديل أو الإتلاف غير الرسمي.

ويتكون هذا المعيار من أربعة معايير فرعية هي:

1. إدارة وسائط التخزين القابلة للإزالة.
2. التخلص من وسائط التخزين.
3. إجراءات التعامل مع المعلومات.
4. حماية وثائق المنظمة.

ومن أهم توجيهات التطبيق التي وردت تحت هذه المعايير ما يلي:

- جميع وسائط التخزين يجب أن تكون مخزنة في بيئة آمنة.
- إنشاء سجلات يدون فيها بيانات وسائط التخزين وطبيعة المعلومات المخزنة عليها.
- التخلص من وسائط التخزين بشكل آمن عندما تقرر المنظمة ذلك وبإجراءات أمنية معتمده.
- اختيار الشركات ذات السمعة الجيدة لإدارة وإزالة الأوراق والمعدات ووسائط التخزين لتجنب تسريب المعلومات المخزنة عليها.
- تصنيف وسائط التخزين والمعدات ووضع علامات تشير إلى محتوياتها.
- إتباع تعليمات التخزين الصادرة من المنتجين.
- تخزين وثائق نظام المعلومات في مكان آمن ويسمح فقط للأشخاص المخولين بالاطلاع عليها.

8/7 تبادل المعلومات

يهدف هذا المعيار إلى تبني سياسة رسمية لتبادل المعلومات والبرامج مع جهات خارجية، وأن تتم عمليات التبادل وفقا لاتفاقيات موثقة تضمن حقوق كل الأطراف.

ويتكون هذا المعيار من خمسة معايير فرعية هي:

1. سياسات وإجراءات تبادل المعلومات.
2. اتفاقيات التبادل.
3. الوسائط المادية في حالة النقل.
4. المراسلة الالكترونية.
5. أنظمة المعلومات التجارية.

ومن أهم توجيهات التطبيق التي وردت تحت هذه المعايير الفرعية ما يلي:

- وضع سياسات وإجراءات لحماية تبادل المعلومات.
- وضع سياسات لاستخدام آلات النسخ والفاكس لضمان سرية المعلومات.
- وضع اتفاقيات لتبادل المعلومات والبرمجيات بين المنظمة والأطراف الخارجية.
- تحديد المسؤوليات في حال وقوع حوادث أمنية بسبب تبادل المعلومات.
- وضع حقوق النشر والتأليف وتراخيص البرامج في اتفاقيات التبادل.
- العمل على ضمان عدم الوصول غير المصرح للمعلومات المتبادل بها.
- حماية الرسائل الالكترونية من الوصول غير المصرح.
- تقييد الوصول إلى الوثائق الحساسة المتعلقة بنظام المعلومات.

9/7 خدمات التجارة الإلكترونية

يهدف هذا المعيار إلى ضمان حماية خدمات التجارة الالكترونية، ويتكون هذا المعيار من ثلاثة معايير فرعية هي:

1. التجارة الالكترونية.
2. التحويلات المباشرة.
3. المعلومات المتاحة للجمهور.

ويوجد العديد من توجيهات التطبيق تحت هذه المعايير أهمها:

- ضمان سرية التعاملات الالكترونية لكل الأطراف.
- ضمان مصداقية الأسعار المعلن عنها.
- ضمان وصول المنتجات إلى العملاء.
- وضع الاعتبارات الأمنية لاستخدام التوقيعات الالكترونية.

10/7 توثيق أحداث أمن المعلومات.

يهدف هذا المعيار إلى رصد وتوثيق أحداث أمن المعلومات للاستفادة منها في المستقبل.

ويتكون هذا المعيار من ستة معايير فرعية هي:

1. مراجعة التسجيلات.
2. مراقبة استخدام الأنظمة.
3. حماية سجل المعلومات.
4. سجلات المدراء والمشغلين.
5. تدوين الأخطاء.
6. مزامنة الوقت.

ويوجد العديد من توجيهات التطبيق أهمها:

- تدوين تواريخ وأوقات وتفاصيل أحداث أمن المعلومات.
- تدوين محاولات الدخول للنظام الناجحة والفاشلة.
- حماية سجلات حوادث آمن المعلومات.
- ضمان تشغيل نظام المعلومات على مدار الساعة.

الفصل الثامن: التحكم في الوصول

يهدف هذا الفصل إلى وضع سياسات لضبط الوصول إلى المعلومات ومرافقها وضمان وصول الأفراد المصرح لهم فقط، وإتباع إجراءات رسمية لتسجيل المستخدمين ولإلغاء التسجيل، وإتباع طرق آمنة لاختبار واستخدام كلمات المرور والحفاظ على سريتها وقصر الوصول لنظم التشغيل على أفراد تم اختيارهم وفقا لطبيعة وظائفهم، وإتباع أسلوب دقيق وآمن لتوثيق هوية المستخدمين.

ويتكون الفصل الثامن من سبعة معايير هي:

1. شروط الدخول للنظام.
2. إدارة دخول المستخدم.
3. مسؤوولیات المستخدم.
4. التحكم في الوصول للشبكة.
5. التحكم في الدخول لأنظمة التشغيل.
6. التحكم في الدخول إلى برامج التطبيقات.
7. التحكم في الدخول من خارج المنظمة.

وبلغ عدد المعايير الفرعية تحت هذه المعايير 25 معيارا فرعيا يمكن تفصيلها على النحو التالي:

1/8 شروط الدخول للنظام.

يهدف هذا المعيار إلى وضع سياسة لضبط الوصول للمعلومات تتوافق مع السياسات الأمنية للنظام وأن توثق هذه السياسات وتراجع وتقيم باستمرار، ووردت تحته مجموعة من توجيهات التطبيق أهمها:

- وضع سياسة للتحكم في الوصول تلبي الاحتياجات الأمنية للمنظمة.
- وضع قواعد للدخول مبنية على مبدأ (كل شيء ممنوع ما لم يسمح به صراحة)
- أن قواعد التحكم في الوصول يجب أن تدعم بواسطة إجراءات رسمية ومسؤوليات محددة وواضحة.

2/8 إدارة دخول المستخدم

يهدف هذا المعيار إلى ضمان وصول المستخدم المصرح له لنظام المعلومات، ووضع إجراءات رسمية لضبط عملية الحصول على حقوق الوصول لنظم المعلومات والخدمات.

ويتكون هذا المعيار من أربعة معايير فرعية هي:

1. تسجيل المستخدم.
2. إدارة امتيازات المستخدم.
3. إدارة كلمة المرور.
4. مراجعة وصول المستخدم للنظام.

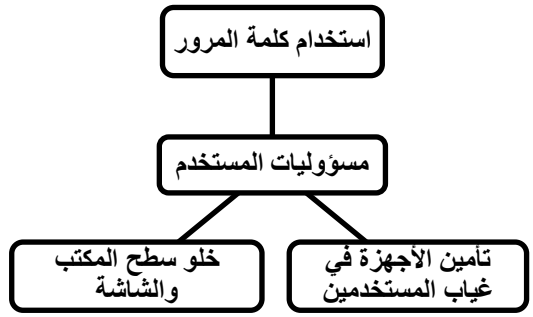
ومن أهم توجيهات التطبيق التي وردت تحت هذه المعايير ما يلي:

- استخدام محدد هوية مميز للمستخدمين يمكنهم من التواصل فيما بينهم.
- التحقق من أن الصلاحيات الممنوحة للدخول للنظام تتوافق مع طبيعة الوظائف.
- إعطاء المستخدمين وثيقة مكتوبة تبين حقوقهم وصلاحياتهم ومسؤولياتهم.
- توقيع المستخدمين على إقرار بالموافقة على شروط الاستخدام.
- إنشاء سجل رسمي للمستخدمين المسجلين لاستخدام خدمة معينة.
- إلغاء حق الوصول أو إغلاق حسابات الموظفين التي تغيرت وظائفهم أو تركوا العمل في المنظمة.
- تخصيص الامتيازات للمستخدمين على أساس الحاجة للاستخدام.
- وضع إجراءات للتحقق من هوية المستخدم قبل منحة اسم مستخدم وكلمة المرور
- تجنب إرسال كلمات المرور عبر رسائل الكترونية غير مشفرة.
- على المستخدمين تأكيد استلامهم لكلمات المرور.
- مراجعة صلاحيات الوصول للمستخدمين بشكل دوري منتظم.

3/8 مسؤوليات المستخدم

يهدف هذا المعيار إلى التأكيد على التزام المستخدمين بالحفاظ على سرية كلمات المرور وتأمين الأجهزة الرسمية والشخصية ضد الاستخدام غير المرخص في فترة عدم الاستخدام.

الشكل رقم (4) المعايير الفرعية بمعيار مسؤوليات المستخدم.



ومن أهم التوجيهات التي وردت تحت هذه المعايير ما يلي:

- الحفاظ على سرية كلمات المرور.
- تجنب كتابة أو الاحتفاظ بكلمة المرور على ورقة أو ملف إلكتروني أو جهاز.
- التغيير الفوري لكلمة المرور عند وجود أي مؤشرات لاحتمال اختراق النظام أو كلمة المرور.
- التغيير المنتظم لكلمة المرور، وعدم استخدام كلمة المرور نفسها لأغراض العمل ولغير أعراض العمل.
- حماية وتأمين أجهزة المستخدمين في حالة غيابهم أو في خارج ساعات الدوام.
- تنظيف مكاتب المستخدمين من أية وثائق سرية أو حساسة.
- تأمين سطح المكتب بكلمات مرور لتقليل مخاطر السطو على الملفات بعد ساعات الدوام.

4/8 التحكم في الوصول للشبكة.

يهدف هذا المعيار إلى منع الوصول غير المصرح لخدمات الشبكة وتطبيق طرق مناسبة لتوثيق المستخدمين والأجهزة ووضع ضوابط تحكم وصول المستخدمين لخدمات المعلومات.

ويتكون هذا المعيار من سبعة معايير فرعية هي:

1. سياسة استخدام خدمات الشبكة.
2. توثيق اتصالات المستخدم الخارجية.
3. توثيق الأجهزة قبل دخولها للشبكة.
4. حماية المنافذ.
5. الفصل بين الشبكات.
6. التحكم في وصلات الشبكة.
7. التحكم في مسارات الشبكة.

ومن أهم توجيهات التطبيق تحت هذه المعايير ما يلي:

- منح صلاحيات الوصول للخدمات للمصرح لهم باستخدامها فقط.
- تحديد وتوثيق المسموح لهم بالوصول للشبكات والخدمات الشبكية.
- وضع ضوابط لاستخدام شبكة داخلية وأخرى خارجية.

5/8 التحكم في الوصول لنظم التشغيل

يهدف هذا المعيار إلى منع الوصول غير المصرح به لنظم التشغيل واستخدام أقصى درجات الأمن لقصر الوصول لنظم التشغيل، واستخدام أقصى درجات الأمن لقصر الوصول لنظم التشغيل على المستخدمين المصرح لهم، وتوثيق وتسجيل المستخدمين ومحاولات الدخول الناجحة والفاشلة وصلاحيات النظام. ويتكون هذا المعيار من ستة معايير فرعية هي:

1. الدخول الآمن للمستخدمين.
2. تعريف المستخدمين.
3. إدارة كلمة المرور.
4. استخدام الأدوات المساعدة.
5. انتهاء زمن جلسة العمل.
6. تحديد زمن الاتصال.

وورد عدد كبير من توجيهات التطبيق تحت هذه المعايير الفرعية أهمها:

- لا تظهر أية معرفات عن النظام إلا بعد الدخول للنظام بنجاح.
- عدم إظهار أية رسائل مساعدة أثناء عملية الدخول للنظام.
- يجب استخدام محدد الهوية لتعقب ممارسات مستخدمي النظام.
- يسمح للمستخدمين باختبار وتغيير كلمات المرور الخاصة بهم.
- فرض اختيار كلمات مرور قوية وإجبار المستخدمين على تغيير كلمات المرور بعد الدخول الأول.
- فصل أدوات النظام المساعدة عن برمجيات التطبيق.
- قصر استخدام أدوات النظام على الحد الأدنى من المستخدمين الموثوق بهم والمصرح لهم.
- رصد وتوثيق كافة استخدامات أدوات النظام.
- إغلاق التطبيق والارتباط بالشبكة بعد فترة زمنية محددة غير نشطة.
- تحديد زمن الارتباط والاتصال بالشبكة بمواعيد محددة حسب طبيعة كل وحدة.

6/8 التحكم في الوصول لبرامج التطبيقات

يهدف هذا المعيار إلى منع المستخدمين غير المصرح لهم من الوصول للمعلومات التي تحملها تطبيقات النظام، ووضع سياسة للتحكم وتحديد الأشخاص المخول لهم للوصول إلى هذه البرامج.

ويتكون هذا المعيار من معيارين فقط هما:

1. تقييد الوصول إلى التطبيقات.
2. عزل الأنظمة الحساسة.

وجاء تحت هذين المعيارين عدداً من توجيهات التطبيق أهمها:

- توفير قوائم تساعد على ضبط الوصول لوظائف التطبيق.
- التحكم في صلاحيات المستخدمين والتطبيقات الأخرى.
- تحديد التطبيقات الحساسة وتحديد المخاطر الناتجة عند تشغيلها مع برامج تطبيقات أخرى.

7/8 التحكم في دخول الحاسبات المتنقلة

يهدف هذا المعيار إلى أخذ كل التدابير الأمنية عند استخدام الحاسبات المتنقلة ووضع وتطبيق إجراءات وخطط تشغيل عند السماح بالدخول لأنظمة المعلومات عند بعد.

ويتكون هذا المعيار من معيارين فرعيين هما:

1. العمل والاتصال عن بعد.
2. مراقبة العمل عن بعد.

وورد تحت هذه المعيار عدداً من توجيهات التطبيق أهمها:

- التأكيد من تأمين النظام والمعلومات والبرامج عند استخدام الحاسبات المتنقلة والكروت الذكية والهواتف المحمولة داخل الشبكات.
- حماية أجهزة الحاسبات المحمولة الخاصة بالمنظمة عند استخدامها في الاجتماعات والأماكن العامة خارج حدود المنظمة.
- التأكد من وجود أمن مادي لمواقع العمل عن بعد.
- وضع ضوابط لعدم وصول أفراد العائلة والأصدقاء للمعلومات المخزنة على الحاسبات المتنقلة.
- إزالة كل التراخيص وحقوق الوصول عند انتهاء أنشطة العمل عن بعد.

الفصل التاسع: حيازة وتطوير وصيانة أنظمة المعلومات.

يهدف هذا الفصل إلى اعتبار أمن نظام المعلومات جزءً هاماً من نظم المعلومات، ومنع الأخطاء والخسائر وإساءة استخدام المعلومات، وحماية سرية وصحة المعلومات من خلال برامج التشفير، وضمان أمن ملفات النظام والحد من وجود ثغرات أمنية ومراقبة نقاط الضعف التقني.

ويشمل هذا الفصل على ستة معايير رئيسة هي:

1. الشروط الأمنية لنظم المعلومات.
2. المعالجة في التطبيقات.
3. ضوابط التشفير.
4. أمن ملفات النظام.
5. الأمن في تطوير ودعم العمليات.
6. إدارة الثغرات التقنية

وتتكون هذه المعايير من (16) معيارا فرعيا يمكن تفصيلها على النحو التالي:

1/9 الشروط الأمنية لنظم المعلومات

يهدف هذا المعيار إلى تحليل وتوصيف الإجراءات الفنية وتحديد المتطلبات الأمنية اللازمة لحفظ وتأمين أنظمة المعلومات.

ويشتمل هذا المعيار على معيار فرعي واحد هو(تحليل وتحديد مواصفات متطلبات الأمن)، وورد به عدد من توجيهات التطبيق أهمها:

- يجب أن تتلاءم المتطلبات الأمنية مع قيمة وحساسية المعلومات الموجودة بالنظام والأضرار المحتملة التي يمكن أن تحدث نتيجة الاختراق الأمني.
- تحديد المتطلبات الأمنية بوضوح في عقود الجهات التي تنفذها.

2/9 المعالجة في التطبيقات

يهدف هذا المعيار إلى التحقق من صحة البيانات المدخلة والمخرجة من نظام المعلومات، ووضع رقابة على عمليات معالجة البيانات والتعديل غير المصرح أو إساءة استخدام المعلومات المخزنة على نظام المعلومات.

ويتكون هذا المعيار من أربعة معايير فرعية هي:

1. التحقق من صحة البيانات المدخلة.
2. الرقابة على المعالجات الداخلية.
3. التحقق من صحة رسائل النظام.
4. التحقق من صحة البيانات المخرجة (المعلنة)

وورد تحت هذا المعيار العديد من توجيهات التطبيق أهمها:

- التأكد من صحة وسلامة بيانات المنسوبين والعملاء.
- الاستعراض الدوري لمحتويات ملفات النظام للتأكد من صحتها.
- تحديد مسؤوليات جميع الموظفين المشاركين في إدخال البيانات.
- وضع إجراءات لمنع تشغيل برامج بطريق الخطأ.
- التأكد من صحة وسلامة الرسائل المخزنة والصادرة عن النظام.

3/9 ضوابط التشفير

يهدف هذا المعيار إلى حماية سرية وسلامة المعلومات من خلال وسائل التشفير وإنشاء إدارة مستقلة داخل النظام لدعم استخدام تقنيات التشفير.

ويتكون هذا المعيار من معيارين فرعيين هما:

1. السياسة العامة في استخدام التشفير.
2. إدارة مفاتيح التشفير.

ومن أهم توجيهات التطبيق تحت هذين المعيارين ما يلي:

- وضع سياسة واضحة للتشفير.
- تحديد مستوى الحماية المطلوبة، وخوارزمية التشفير المطلوبة.
- استخدام التشفير في حماية المعلومات المخزنة على الحاسبات المتنقلة أو وسائل التخزين القابلة للإزالة.
- استخدام التشفير عند استخدام التوقيعات الالكترونية.
- جميع مفاتيح التشفير يجب أن تكون محمية من التعديل أو التدمير.

4/9 أمن ملفات النظام

يهدف هذا المعيار إلى وضع ضوابط للتحكم في الوصول إلى ملفات النظام، وتقييد الوصول إلى شفرات النظام.

ويتكون هذا المعيار من ثلاثة معايير فرعية هي:

1. التحكم في برامج التشغيل.
2. حماية بيانات نظم اختبار أمن النظام.
3. مراقبة الدخول إلى شفرات أمن النظام.

ويوجد العديد من توجيهات التطبيق وردت تحت هذه المعايير هي:

- تحديث البرمجيات والتطبيقات يتم فقط عن طريق المدراء المدربين والمصرح لهم بذلك.
- اختيار نظم التشغيل وبرامج التطبيقات يتم على أساس قابلية الاستخدام والأمن والتوافق مع البرامج الأخرى وسهولة الاستخدام.
- تبني إستراتيجية واضحة لتغيير الأنظمة والبرمجيات.
- الإبقاء على الإصدارات السابقة كتدبير طوارئ.

- رفع مستوى أنظمة التشغيل (الترقية) يتم فقط عندما تكون هناك حاجة لذلك.
- تجنب قواعد بيانات التشغيل التي تحتوي على معلومات شخصية أو حساسة.
- التحكم في شفرة مصدر البرنامج وفقا للإجراءات المعمول بها.
- إعطاء موظفي الدعم الفني وصول مقيد إلى برامج التطبيقات.
- وضع قوائم البرامج في بيئة آمنة.

5/9 الأمن في تطوير ودعم العمليات.

يهدف هذا المعيار إلى المحافظة على أمن برمجيات ومعلومات نظام التطبيق، وأن أية تغييرات على هذه البرمجيات لابد وأن تخضع لإجراءات مراقبة رسمية واختبار نظم تشغيل التطبيقات قبل أحداث أي تغييرات عليها.

ويتكون هذا المعيار من خمسة معايير هي:

1. إجراءات ضبط التغيير.
2. مراجعة فنية للتطبيقات بعد إجراء تعديلات عليها.
3. تقييد التغيرات إلى أحزمة البرمجيات.
4. تسرب المعلومات.
5. الاستعانة بمصادر خارجية لتطوير البرمجيات.

ومن أهم توجيهات التطبيق التي وردت تحت هذه المعايير ما يلي:

- توثيق الإجراءات الرسمية لتغيير نظم التطبيقات.
- تقييم المخاطر وتحليل الآثار المترتبة على التغيرات.
- الحصول على موافقة رسمية من الإدارة المسؤولة قبل إجراء أية تغييرات.
- اختبار إجراءات السلامة للتأكد من أنها لم تتأثر بأية تغيرات في نظام التشغيل.
- إمكانية الحصول على التعديلات من المورد أو المنتج الأصلي.
- منع فرص تسرب المعلومات.
- الاستعانة بمصادر خارجية لتطوير البرمجيات يجب أن يخضع لإشراف ورقابة المنظمة.
- التأكد من صحة التراخيص وحقوق الملكية الفكرية عند التعامل مع جهات خارجية لتطوير البرامج.

6/9 إدارة الثغرات التقنية.

يهدف هذا المعيار إلى الحد من المخاطر الناتجة عن استغلال نقاط الضعف التقنية، ومراقبة ومراجعة نقاط الضعف التقني وتحديد المسؤوليات والأدوار المرتبطة بإدارة الضعف التقني.

ويتكون هذا المعيار من معيار فرعي واحد هو" التحكم في الثغرات التقنية " وردت تحته مجموعة من توجيهات التطبيق أهمها:

- الحصول على معلومات عن مواطن الضعف في أنظمة المعلومات.
- الجرد الكامل لأصول البرامج والتطبيقات.
- تحديد الأدوار والمسؤوليات المرتبطة بإدارة الثغرات التقنية.
- تحديد المخاطر المرتبطة بالثغرات التقنية.
- توثيق كل إجراءات إدارة الثغرات التقنية.

الفصل العاشر: إدارة حوادث أمن المعلومات.

يهدف هذا الفصل إلى التأكيد على أمن المعلومات، والتبليغ عن مواطن الضعف في أنظمة المعلومات والتعامل معها، ومراجعتها في أقرب وقت ممكن وتحديد الإجراءات والمسؤوليات والإدارات المنوط بها التعامل مع حوادث أمن المعلومات، والإفادة من المعلومات المكتسبة من حوادث امن

المعلومات في المستقبل، والتأكيد على تدخل الجهات الأمنية المنوط بها التحقيق في الوقت المناسب قبل الطمس المتعمد للحقائق.

ويتكون هذا الفصل من معيارين رئيسيين هما:

1. الإبلاغ عن حوادث أمن المعلومات.
2. إدارة حوادث أمن المعلومات.

ويوجد خمسة معايير فرعية تحت هذين المعيارين يمكن تفصيلها كالتالي:

1/10 الإبلاغ عن حوادث أمن المعلومات ونقاط الضعف الأمنية.

ويوجد تحت هذا المعيار معيارين فرعين هما:

1. الإبلاغ عن حوادث أمن المعلومات.
2. الإبلاغ عن نقاط الضعف الأمنية.

ويوجد تحتهما العديد من توجيهات التطبيق أهمها:

- التبليغ عن الحوادث الأمنية في النظام عبر القنوات الرسمية في أقرب وقت ممكن.
- التأكيد على وجود نقاط اتصال معروفة لكل المنسوبين لاستخدامها في التبليغ والاستجابة في أسرع وقت.
- توفير نماذج تقارير للتبليغ عن الحوادث الأمنية.
- تدريب كل المنسوبين على السلوك الصحيح الواجب اتخاذه في حال وقوع حوادث أمن المعلومات.

2/10 إدارة حوادث أمن المعلومات.

يهدف هذا المعيار إلى وجود نسق ونهج فعال لتطبيق إدارة الحوادث الأمنية وتحديد الإجراءات والمسؤوليات المتبعة عن وقوع حوادث أمن المعلومات.

ويتكون هذا المعيار من ثلاثة معايير فرعية هي:

1. المسؤوليات والإجراءات.
2. التعلم من حوادث أمن المعلومات.
3. جمع الأدلة.

ويوجد العديد من توجيهات التطبيق تحت هذه المعايير أهمها:

- تفعيل الإجراءات اللازمة لضمان سرعة وفعالية الرد عند وقوع حوادث أمنية.
- تحليل المعلومات والأدلة ومحتويات الحوادث الأمنية.
- تقديم تقارير دورية عن الحوادث الأمنية.
- الاستفادة من معلومات التقييم للحد من الخسائر في المستقبل.

الفصل الحادي عشر: إدارة استمرارية الأعمال.

يهدف هذا الفصل إلى الحد من كل الأنشطة التي تحاول إعاقة سير العمل في المنظمة والعمل على حماية نظم المعلومات من الأعطال الرئيسة أو الكوارث وضمان إعادة تشغيل النظام في الوقت المناسب.

ويتكون هذا الفصل من معيار واحد هو:

1/11 إدارة عمليات أمن المعلومات واستمرارية العمل ويتكون هذا المعيار من خمسة معايير فرعية هي:

1. تضمين أمن المعلومات في إدارة استمرارية العمل.
2. استمرارية العمل وتقييم المخاطر.
3. وضع وتطوير تخطيط لاستمرارية العمل.
4. إطار تخطيط استمرارية العمل.
5. اختبار وصيانة وإعادة تقييم لمخططات استمرارية العمل.

ويوجد العديد من توجيهات التطبيق تحت هذه المعايير أهمها:

- الحفاظ على خصوصية وسرية حوادث أمن المعلومات.
- جمع الأدلة في أقرب وقت ممكن بعد وقوع الحادث.
- تحديد موارد مالية وإدارية وفنية وبيئية للإفادة منها لإعادة استمرارية العمل.
- ضمان سلامة الموظفين وحماية مرافق المعلومات والممتلكات التابعة للمنظمة.
- تحديد الأحداث التي يمكن أن تسبب انقطاع الأعمال.
- توثيق كل العمليات والإجراءات التي تم اتخاذها لإعادة استمرارية العمل.
- اختبار وصيانة وإعادة تقييم خطط استمرارية العمل.

الفصل الثاني عشر: إدارة الامتثال أوالتوافق.

يهدف هذا الفصل إلى تجنب أي اختراق للقوانين والأنظمة والالتزامات التعاقدية، وتحديد وتوثيق هذه القوانين والأنظمة وتحديثها كلما لزم الأمر، ومنع إساءة استخدام المعلومات ومرافقها، وحماية خصوصية البيانات والمعلومات الشخصية.

ويتكون هذا الفصل من ثلاثة معايير رئيسة هي:

1. الامتثال للشروط القانونية.
2. التوافق مع السياسات والمعايير الأمنية والفنية.
3. مراجعة أنظمة المعلومات.

تشتمل هذه المعايير على عشر معايير فرعية يمكن تفصيلها كالتالي:

1/11 الامتثال للشروط القانونية.

يهدف هذا المعيار إلى تحديد التشريعات المعمول بها وحماية حقوق الملكية الفكرية والحد من سوء استخدام المعلومات الشخصية ووضع ضوابط لبرامج التشفير والتأكد من أنها تتوافق مع التشريعات.

ويتكون هذا المعيار من ستة معايير فرعية هما:

1. التعرف على التشريعات سارية المفعول.
2. حقوق الملكية الفكرية.
3. حماية سجلات المنظمة.
4. حماية البيانات وخصوصية المعلومات الشخصية.
5. الوقاية من سوء استخدام المعلومات ومرافق المعلومات.
6. تنظيم ضوابط التشفير.

ويوجد العديد من توجيهات التطبيق تحت هذه المعايير الفرعية أهمها:

- تعريف وتحديد التشريعات المطبقة.
- التأكيد على حماية حقوق الملكية الفكرية.
- الحصول على البرامج والتطبيقات الأصلية.
- المحافظة على تراخيص الاستخدام وأدلة التشغيل وأقراص التثبيت.
- وضع سياسة للتخلص من البرمجيات أو إعارتها للآخرين.
- عدم النسخ كليا أو جزئيا للكتب والمقالات وغيرها من الوثائق، بخلاف ما يسمح به قانون حقوق التأليف والنشر.
- وضع ضوابط ومبادئ توجيهية بشأن حفظ وتخزين وتداول والتخلص من السجلات والمعلومات.
- تحديد طرق وأساليب استخدام المعلومات ومرافقها.
- وضع ضوابط للتشفير تتفق مع اللوائح والتشريعات المعمول بها.

2/11 التوافق مع السياسات والمعايير الأمنية والفنية.

يهدف هذا المعيار إلى ضمان الامتثال للسياسات التنظيمية والمعايير الأمنية والتحقق من التوافق التقني. ويشتمل هذا المعيار على معيارين فرعين هما:

1. الامتثال للسياسات والمعايير الأمنية.
2. التحقق من التوافق التقني.

ويوجد العديد من توجيهات التطبيق تحت هذين المعيارين منها:

- التأكد من أن الإجراءات الأمنية المتبعة تتوافق مع السياسات والمعايير الأمنية المحلية والدولية.
- تحليل نظم المعلومات والتأكد من توافقها مع المعايير التقنية.

3/11 مراجعة أنظمة المعلومات.

يهدف هذا المعيار إلى تحقيق أقصى درجات الدقة للتأكد من حماية نظم المعلومات وسلامة ومنع استخدام أساليب ووسائط المراجعة.

ويتكون هذا المعيار من معيارين فرعيين هما:

1. ضوابط تدقيق نظم المعلومات. 2. حماية أدوات مراجعة نظم المعلومات.

ويوجد العديد من توجيهات التطبيق تحت هذين المعيارين أهمها:

- التحقق من حسابات وأنشطة أنظمة المعلومات.
- حفظ ملفات النظام وحمايتها وعدم السماح مطلقا بالتغيير فيها إلا للموظفين المخولين فقط.
- حماية سجلات ومراجعة نظم التشغيل من سوء الاستخدام.
- فصل ملفات البيانات عن نظم التشغيل.

*** *** ***