المواصفة القياسية الدولية

أيــزو/ اللجنة الدولية الكهروتقنية
٢٧٠٠١

الترجمة الرسمية
Official translation
Traditionofficials

تكنولوجيا المعلومات ـ تقنيات الأمننظم إدارة أمن المعلومات – المتطلبات

Information technology — Security techniques — Information security management systems — Requirements (E)

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences (F)

طبعت في الأمانة المركزية ISO في جنيف، سويسرا كترجمة عربية رسمية بالإنابة عن١٠هيئات أعضاء في ISOالتي أعتمدت دقة الترجمة (انظر القائمة في صفحة ii).

الرقم المرجعى
ISO\IEC 27001:2013 ***(A)***
الترجمة الرسمية

جهات التقييس العربية التي اعتمدت المواصفة

■ مؤسسة المواصفات والمقاييس الأردنية	الأردن
■ هيئة الإمارات للمواصفات والمقاييس	الإمارات
■ المعهد الجزائري للتقييس	الجزائر
■ الهيئة السعودية للمواصفات والمقاييس	السعودية
■ الجهاز المركزي للتقييس والسيطرة النوعية	العراق
■ الهيئة العامة للصناعة	الكويت
■ الهيئة السودانية للمواصفات والمقاييس	السودان
■ الهيئة اليمنية للمواصفات والمقاييس وضبط الجودة	اليمن
■ المعهد الوطني للمواصفات والملكية الصناعية	تونس
■ هيئة المواصفات والمقاييس العربية السورية	سوريا
■ المركز الوطني للمواصفات والمعايير القياسية	ليبيا
■ الهيئة المصرية العامة للمواصفات والجودة	مصر

مكتب حقوق ملكية المنظمة الدولية للتقييس
الرمز البريدي: ٥٦ -Ch-1211- جنيف ٢٠
هاتف: ٠٠٤١٢٢٧٤٩٠١١١
فاكس: ٠٠٤١٢٢٧٤٩٠٩٤٧
بريد الكتروني: copyright@iso.org
الموقع الالكتروني: www.iso.org
تم نشر النسخةالعربية في٢٠١٧
تم النشر في سويسرا

المحتويات

تمهيد ... iv
٠ مقدمة ... v
١ المجال ... ١
٢ المراجع التكميلية ... ١
٣ المصطلحات والتعاريف ... ١
٤ بيئة المنشأة ... ١
١/٤ فهم المنشأة فى بيئتها ... ١
٢/٤ فهم احتياجات وتوقعات الأطراف المعنية ... ١
٣/٤ تحديد مجال نظام إدارة أمن المعلومات ... ١
٤/٤ نظام إدارة أمن المعلومات ... ٢
٥ القيادة ... ٢
١/٥ القيادة والالتزام ... ٢
٢/٥ السياسات ... ٢
٣/٥ الأدوار والمسؤوليات والسلطات التنظيمية ... ٢
٦ التخطيط ... ٣
١/٦ الإجراءات استهداف المخاطر والفرص ... ٣
٢/٦ تقدير مخاطر أمن المعلومات ... ٤
٧ الدعم ... ٥
١/٧ الموارد ... ٥
٢/٧ الكفاءة ... ٥
٣/٧ التوعية ... ٥
٤/٧ الاتصالات ... ٥
٥/٧ المعلومات الموثقة ... ٦
٨ التشغيل ... ٧
١/٨ التخطيط للتشغيل والرقابة ... ٧
٢/٨ تقدير مخاطر أمن المعلومات ... ٧
٣/٨ معالجة مخاطر أمن المعلومات ... ٧
٩ تقييم الأداء ... ٧
١/٩ الرصد والقياس والتحليل والتقييم ... ٧
٢/٩ التدقيق الداخلي ... ٨
٣/٩ مراجعة الإدارة ... ٨
١٠ التحسين ... ٩
١/١٠ عدم المطابقة والإجراءات التصحيحية ... ٩
٢/١٠ التحسين المستمر ... ٩
مرفق أ (استرشادي) أهداف الضبط والضوابط المرجعية ... ١٠
المصادر ... ٢١

تمهيد

الأيزو (المنظمة الدولية للتقييس) هي اتحاد عالمي لجهات التقييس الوطنية (الجهات الأعضاء في الأيزو)،وغالبا مايتم إعداد المواصفات الدولية من خلال اللجان الفنية للأيزو،وإذا كانت الجهة العضو لها اهتمام بموضوع قد شُكِّلت له لجنة فنية، فإن لهذا العضو الحق في أن يكون له ممثّل في تلك اللجنة.ويشارك في العمل كذلك المنظمات الدولية الحكومية منها وغير الحكومية، التي لها تواصل مع الأيزو.وتتعاون الأيزو تعاونا وثيقا مع اللجنة الدولية الكهروتقنية (هـ د ك) في جميع الأمور التي تهم التقييس في المجال الكهرو تقني.

وتصاغ المواصفات الدولية وفقا للوائح الواردة في توجيهات الأيزو/هـ د ك - الجزء الثاني.
المهمة الرئيسية للجان الفنية هو اعداد المواصفات الدولية. ويتم توزيع مشاريع المواصفات الدولية على الهيئات الوطنية للتصويت.ويتطلب اصدار هذه المشاريع كمواصفات دولية موافقة ٧٥% على الأقل من الهيئات الوطنية التي يحق لها التصويت.

ونود لفت الانتباه إلى احتمالية أن تكون بعض عناصر هذه الوثيقة خاضعة لحقوق براءة الاختراع. ولن تتحمل المنظمة الدولية للتقييس (ISO) مسؤولية تحديد أيّ من هذه الحقوق أو جميعها.

وقد تم إعداد مواصفة الأيــزو/ اللجنة الدولية الكهرو تقنية ٢٧٠٠١ بواسطة اللجنة الفنية المشتركة ISO / IEC JTC 1، تكنولوجيا المعلومات، اللجنة الفرعية SC 27 ، تقنيات الأمن.
تلغى هذه الطبعة الثانية، الطبعة الأولى (ISO / IEC 27001: 2005) حيث تم تنقيحها من الناحية الفنية.

٠ مقدمة

١/٠ عام

أعدت هذه المواصفة الدولية لتقدم متطلبات وضع وتنفيذ وصيانة منظومة إدارة تأمين المعلومات والتحسين المستمر لها. ويعد قرار تبنى منظومة إدارة أمن المعلومات قرارا استراتيجيا للمنشأة، يتأثرهذا النظام فى بنائه وفى وضعه موضع التطبيق باحتياجات المنشأة وأهدافها وبمتطلبات الأمن وبالعمليات التنظيمية المستخدمة وكذلك بحجم وهيكل المنشأة. وهي المؤثرات التي بتوقع أن تتغير مع الزمن.
تقوم منظومة إدارة تأمين المعلومات بالحفاظ على سرية واتساق وإتاحة المعلومات من خلال تطبيق عملية لإدارة المخاطر ومن خلال إعطاء الأطراف المعنية الثقة فى أن المخاطر تعالج بالأساليب المناسبة.
من المهم أن تكون منظومة إدارة تأمين المعلومات جزء من عمليات المنشأة ومتكاملة معها ومع هيكل الإدارة ككل وأن يؤخذ تأمين المعلومات فى الاعتبار عند تصميم العمليات ونظم المعلومات والضوابط. ومن المتوقع أن يتناسب نظام تأمين المعلومات فى تنفيذه مع احتياجات المنشأة
يمكن استخدام هذه المواصفة لتقييم المطابقة من قبل الجهات الداخلية والخارجية، لتقييم قدرة المنشأة لتحقيق متطلباتها فيما يختص بأمن المعلومات.
ولا يعكس ترتيب عرض هذه المتطلبات فى المواصفة الدولية أهمية هذه المتطلبات، ولا يقتضي ترتيب وضعها موضع التنفيذ. ويأتي ترقيم عناصر القائمة فقط لأغراض المرجعية.
تقدم المواصفة ISO / IEC 27000 نظرة عامة ومفردات نظم إدارة أمن المعلومات، ومرجعها فى ذلك عائلة مواصفات نظام إدارة أمن المعلومات (التي تضم [2] ISO / IEC 27003، [3] ISO / IEC 27004] و ISO [4] IEC 27005 /])، مع المصطلحات والتعاريف ذات الصلة.

٢/٠ التوافق مع مواصفات نظم الإدارة الأخرى

تطبق/ تستخدم هذه المواصفة الدولية الهيكل / الإطار الفوقيالإجمالي، وعناوين البنود الفرعية، ونصوصا مماثلة، والمصطلحات الشائعة، والتعاريف الأساسية المعرفة فى الملحق SL من الجزء الأول من توجيهات ISO / IEC، فى الجزء الأول، ملحق ISO المجمع، ومن ثم تحافظ على التوافق مع مواصفات نظم الإدارة أخرى المعايير التي اعتمدت الملحق .SL

يكون هذا النهج المشترك المحدد في الملحق SL مفيدا لتلك المنشئات التي تختار تشغيل نظام واحد للإدارة يفي بمتطلبات اثنين أو أكثر من مواصفات نظم الإدارة.

تكنولوجيا المعلومات ـ تقنيات الأمن- نظم إدارة أمن المعلومات – المتطلبات

١ـ المجال

تحدد هذه المواصفة الدولية متطلبات الإنشاء والتنفيذ والصيانة والتحسين المستمر لنظام إدارة أمن المعلومات في بيئة المنشأة. وتضم هذه المواصفة أيضا متطلبات تقدير ومعالجة مخاطر أمن المعلومات وفقا لاحتياجات المنشأة. المتطلبات المنصوص عليها في هذه المواصفة الدولية متطلبات عامة وأولية ويقصد بها أن تكون منطبقة على جميع المنظمات، بغض النظر عن النوع أو الحجم أو الطبيعة. ليس من المقبول استبعاد أي من الشروط المحددة في البنود من الرابع إلى العاشر، عندما تدعي المنشأة تطابقها مع هذه المواصفة الدولية.

٢ـ المراجع التكميلية

تعتبر الوثائق المرجعية التالية اساسية لتطبيق هذه المواصفة . بالنسبة للمراجع المؤرخة يلزم تطبيق النسخ الواردة أدناه فقط اما بالنسبة للمراجع عير المؤرخة فإنه يلزم تطبيق آخر إصدار من الوثيقة المرجعية (متضمنا اى تعديلات).

ISO / IEC 27000 ، وتكنولوجيا المعلومات ـ تقنيات الأمن ـ إدارة نظم أمن المعلومات – الإطار العام والمفردات

٣ـ المصطلحات والتعاريف

لأغراض هذه الوثيقة، تطبق المصطلحات والتعاريف الواردة في ISO / IEC 27000

٤ـ بيئة المنشأة

١/٤ فهم المنشأة فى بيئتها

يجب على المنشأة تحديد القضايا الخارجية والداخلية ذات الصلة بأغراضها والتي تؤثر على قدرتها على تحقيق النتائج المرجوة من نظام إدارة أمن المعلومات الخاصة بها.

ملحوظة تحديد هذه القضايا يرجع إلى بناء المحيطين الخارجي والداخلي للمنشأة على النحو المعتبر الوارد فى البند ٥- ٣ من المواصفة ISO 31000:2009 [5]

٢/٤ فهم احتياجات وتوقعات الأطراف المعنية

يجب على المنشأة تحديد ما يلي:

أ) الأطراف المعنية ذات الصلة بنظام إدارة أمن المعلومات،

ب) متطلبات هذه الأطراف المهتمة ذات الصلة بأمن المعلومات.

ملحوظة قد تتضمن متطلبات الأطراف المعنية متطلبات قانونية وتنظيمية والتزامات تعاقدية.

٣/٤ تحديد مجال نظام إدارة أمن المعلومات

يجب على المنشأة تعيين حدود ومدى انطباق نظام إدارة أمن المعلومات لتحديد مجاله.

عند تحديد هذا المجال، يتعين على المنشأة أن تأخذ فى الاعتبار ما يلي:

أ) القضايا الخارجية والداخلية المشار إليها فى ١/٤.

ب) المتطلبات المشار إليها فى ٢/٤.

ج) مناطق التلاقي والاعتمادية بين الأنشطة التي تقوم بها المنشأة، وتلك التي يتم تنفيذها من قبل منظمات أخرى.

يجب أن يكون النطاق متاحا كمعلومات موثقة.

٤/٤ نظام إدارة أمن المعلومات

يجب على المنشأة إنشاء وتنفيذ وصيانة نظام إدارة أمن المعلومات وتحسينه باستمرار، وفقا لمتطلبات هذه المواصفة الدولية.

٥- القيادة

١/٥ القيادة والالتزام

يجب أن تبدى الإدارة العليا القيادة والالتزام فيما يتعلق بنظام إدارة تأمين المعلومات وذلك من خلال :-

أ) التحقق من أن سياسات وأهداف أمن المعلومات قد وضعت ومن أنها متوافقة مع التوجه الاستراتيجي للمنشأة.

ب) التحقق من تكامل / دمج متطلبات نظام إدارة أمن المعلومات في عمليات المنشأة.

ت) التحقق من اتاحة / توفير الموارد اللازمة لنظام إدارة أمن المعلومات.

ث) نشر أهمية الإدارة الفعالة لأمن المعلومات وأهمية مطابقتها لمتطلبات نظام إدارة أمن المعلومات.

ج) التحقق من أن نظام إدارة أمن المعلومات يحقق النتائج المرجوة.

ح) توجيه ودعم الأشخاص للإسهام في فعالية نظام إدارة أمن المعلومات.

خ) تعزيز التحسين المستمر.

د) دعم أدوار الإدارة الأخرى ذات الصلة بإبداءالقيادة، كل على النحو المناسب لمنطقة مسؤوليته.

٢/٥ السياسات

يجب على الإدارة العليا وضع سياسة لأمن المعلومات من شأنها أن:

أ)تكون مناسبة لأغراض المنشأة؛
ب) تشمل أهداف أمن المعلومات (انظر ٦-٢) أو تقدم إطارا لوضع أهداف أمن المعلومات؛
ج)تتضمن التزاما بالوفاء بالمتطلبات الواجب تطبيقها فيما يتعلق بأمن المعلومات،
د)تتضمن التزاما بالتحسين المستمر لنظام إدارة أمن المعلومات.
ويجب أن تكون سياسة أمن المعلومات:
ه) متاحة كمعلومات موثقة؛
و) منشورة خلال المنشأة،
ز) متاحة للأطراف المعنية ، حسب الاقتضاء.

٣/٥ الأدوار والمسؤوليات والسلطات التنظيمية

يجب على الإدارة العليا التأكد من أن المسؤوليات والسلطات المطلوبة للقيام بالأدوار ذات الصلة بأمن المعلومات قد تم تخصيصها وإبلاغها.

يجب أن تخصص الإدارة العليا المسؤوليات والسلطات من أجل:
أ)ضمان توافق نظام إدارة أمن المعلومات مع متطلبات هذه المواصفة الدولية،
ب) إصدار التقارير للإدارة العليا بشأن أداء نظام إدارة أمن المعلومات.

ملحوظة قد تقوم الإدارة العليا أيضا بالتكليف بمسؤوليات وسلطات إصدار تقارير أداء نظام إدارة أمن المعلومات عبر المنشأة.

٦ـ التخطيط

١/٦ الإجراءات استهداف المخاطر والفرص

١/١/٦ عام

عند التخطيط لنظام إدارة أمن المعلومات، يجب على المنشأة أن تأخذ فى الاعتبار القضايا المشار إليها في ١/٤ والمتطلبات المشار إليها في ٢/٤ وتحديد المخاطر والفرص المطلوب استهدافها من أجل:

أ) ضمان أن نظام إدارة أمن المعلومات يحقق نتائجه المقصودة؛

ب)منع أو تقليل ، التأثيرات غير المرغوبة ،

ج)تحقيق التحسين المستمر.

يجب على المنشأة التخطيط لما يلى :

د) إجراءات استهداف هذه المخاطر والفرص .

هـ) كيفية :

١) دمج هذه الإجراءات في عمليات نظام إدارة أمن المعلومات في المنشأة ووضعها موضع التنفيذ؛

٢) تقييم فعالية هذه الإجراءات.

٢/١/٦ تقدير مخاطر أمن المعلومات

يجب على المنشأة تحديد وتطبيق عملية لتقدير مخاطر أمن المعلومات من شأنها:

أ) تحديد وصيانة معايير مخاطر أمن المعلومات التي تشمل:

١) معايير قبول المخاطر،

٢) معايير أداء عمليات تقدير مخاطر أمن المعلومات؛

ب) ضمان أن تقييمات مخاطر أمن المعلومات المتكررة تسفر عن نتائج متسقة،و صحيحة وقابلة للمقارنة ؛

ج)تحديد مخاطر أمن المعلومات:

١) تطبيق عملية تقدير مخاطر أمن المعلومات لتحديد المخاطر المرتبطة بفقدان السرية والاتساق والاتاحة للمعلومات في نطاق نظام إدارة أمن المعلومات ،

٢) تحديد أصحاب المخاطر؛

د) تحليل مخاطر أمن المعلومات:

١) تقدير العواقب المحتملة التي قد تترتب على ما إذا كانت المخاطر التي تم تحديدها في **٢/١/٦** ج قد صارت واقعا.

٢) تقييم الاحتمالات الواقعية لحدوث المخاطر التي تم تحديدها ف في **٢/١/٦** ج

٣) تحديد مستويات المخاطر؛

هـ) تقييم مخاطر أمن المعلومات:
١) مقارنة نتائج تحليل المخاطر مع معايير المخاطر الموضوعة فى ٢/١/٦
٢) وضع أولويات المخاطر المحللة لأغراض معالجة المخاطر.

ويجب أن تحتفظ المنشأة بمعلومات موثقة حول عملية تقييم مخاطر أمن المعلومات.

٣/١/٦ معالجة مخاطر أمن المعلومات

يجب على المنشأة تحديد وتطبيق عملية لمعالجة مخاطر أمن المعلومات بغرض:
أ) تحديد خيارات العلاج المناسبة لمخاطر أمن المعلومات، مع الأخذ في الحسبان نتائج تقدير المخاطر؛
ب)تحديد جميع الضوابط اللازمة لتنفيذ خيارات علاج مخاطر أمن المعلومات المختارة؛

ملحوظة: يمكن للمنظمات تصميم الضوابط على النحو المطلوب، أو تحديدها من أي من مصادرها

ج) مقارنة الضوابط المحددة في ٦-١-٣ ب أعلاه مع تلك الموجودة في المرفق أ والتحقق من عدم حذف أى من الضوابط اللازمة؛

ملحوظة ١ المرفق أ يحتوي على قائمة شاملة من أهداف الرقابة والضوابط. يوجه مستخدمو هذه المواصفة الدولية للمرفق أ لضمان عدم التغاضي عن ضوابط ضرورية.

ملحوظة ٢ أهداف الضبط مشمولة ضمنا في الضوابط المختارة. أهداف الرقابة والضوابط الواردة في المرفق أ ليست حصرية، وربما تكون هناك حاجة إلى أهداف إضافية للرقابة وإلى ضوابط إضافية.

د) وضع إعلان الانطباقية الذى يحتوي على الضوابط الضرورية (انظر ٦/١/٣ ب) و ج)) ومبررات التضمين، وما إذا كانت تنفذ أم لا، و مبررات الاستبعادات من الضوابط الواردة فى المرفق أ ؛
هـ) صياغة / وضع خطة العلاج لمخاطر أمن المعلومات ،
و) الحصول على موافقة أصحاب المخاطر على خطة علاج مخاطر أمن المعلومات وقبول مخاطر أمن المعلومات المتبقية.
ويجب على المنشأة الاحتفاظ بمعلومات موثقة عن عملية معالجة مخاطر أمن المعلومات.
ملحوظة :عملية تقييم مخاطر أمن المعلومات و عملية المعالجة في هذا المعيار الدولي تنسجم مع المبادئ والخطوط الإرشادية الأولية المنصوص عليها في. [5] ISO 31000

٢/٦ أهداف أمن المعلومات وخطط تحقيقها

يجب على المنشأة تحديد أهداف أمن المعلومات في الوظائف والمستويات ذاتالصلة.
يجب أن تكون أهداف أمن المعلومات:

أ) متسقة مع سياسة أمن المعلومات؛

ب) قابلة للقياس (إذا كان ذلك عمليا)؛

ج) آخذة في الاعتبار متطلبات أمن المعلومات المطبقة،ونتائج تقييم المخاطر ومعالجة المخاطر؛

د) واصلة للمعنيين وذوي الصلة؛

ه) يتم تحديثها حسب الاقتضاء.

ويجب أن تحتفظ المنشأة بمعلومات موثقة عن أهداف أمن المعلومات.

عند التخطيط لكيفية تحقيق أهداف الأمن لمعلوماتها، يجب على المنشأة تحديد ما يلي:

و) ما سيتم القيام به؛

ز) ما هي الموارد المطلوبة؛

ح) من الذي سيكون مسؤولا؛

ط) متى سيتم الانتهاء منه؛

ي) كيف يتم تقييم النتائج.

٧- الدعم

١/٧ الموارد

يجب على المنشأة تحديد وتوفير الموارد اللازمة للإنشاء والتنفيذ والصيانة والتحسين المستمر لنظام إدارة أمن المعلومات.

٢/٧ الكفاءة

يجب أن تقوم المنشأة بما يلي:

أ) تحديد الكفاءات المطلوبة للشخص (الأشخاص) الذين يقومون بأعمال تحت سيطرتها من شأنها التأثير على أداء أمن المعلومات فيها؛

ب)ضمان كفاءة الاشخاص على أساس من التعليم والتدريب ، أو الخبرات المناسبة ؛

ج)حيثما ينطبق ذلك ، اتخاذ الاجراءات لاكتساب الكفاءة اللازمة ، و تقييم فعالية الإجراءات المتخذة ،

د) الاحتفاظ بالمعلومات الموثقة المناسبة كدليل على الكفاءة.

ويمكن أن تشمل الإجراءات المنطبقة-على سبيل المثال: توفير التدريب للأفراد، والعمل تحت إشراف زميل أقدم ، أو إعادة تأهيل الموظفين الحاليين ، أو التوظيف أو التعاقد مع أشخاص اكفّاء .

٣/٧ التوعية

يجب أن يكون الأشخاص العاملون تحت سيطرة المنشأة على وعى بما يلي:

أ) سياسة أمن المعلومات؛

ب)إسهاماتهم فى فعالية نظام إدارة أمن المعلومات، بما في ذلك عوائد تحسين أداء أمن المعلومات،

ج) تداعيات عدم التوافق مع متطلبات نظام إدارة أمن المعلومات.

٤/٧الاتصالات

يجب على المنشأة تحديد احتياجاتها من الاتصالات الداخلية والخارجية ذات الصلة بنظام إدارة أمن المعلومات بما في ذلك: