

أيزو/ أي إي سي ٢٧٠١٧

المواصفة القياسية الدولية

الترجمة الرسمية  
Official translation  
Traduction officielle

تقنية المعلومات – تقنيات التأمين – كود الممارسة لضوابط تأمين المعلومات المبنية على  
المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢ للخدمات السحابية

*Information technology – Security techniques – Code of practice for  
information security controls based on ISO/IEC 27002 for cloud services (E)*

*Technologies de l'information — Techniques de sécurité — Code de pratique pour les  
contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du  
nuage (F)*

[ISO/IEC 27017:2015](https://standards.iteh.ai/catalog/standards/sist/f1cdcf95-c8ee-4fa9-9e35-e56c34b305df/iso-iec-27017-2015)

<https://standards.iteh.ai/catalog/standards/sist/f1cdcf95-c8ee-4fa9-9e35-e56c34b305df/iso-iec-27017-2015>

طبعت في الأمانة المركزية ISO في جنيف، سويسرا كترجمة عربية رسمية بالإنابة عن ١٠ هيئات أعضاء في ISO التي اعتمدت دقة الترجمة  
( انظر القائمة في صفحة ii ).

الرقم المرجعي  
ISO/IEC 27017/2015 (A)  
الترجمة الرسمية

©ISO/IEC 2015



### إخلاء مسؤولية (تنويه)

قد يحتوي هذا الملف (PDF) على خطوط مُدمجة ، وبموجب سياسة الترخيص لـ Adobe فإنه يمكن طباعة هذا الملف أو الإطلاع عليه ، على ألا يتم تعديله ما لم تكن الخطوط المُدمجة فيهمُرخصة و مُحَمَّلة في الحاسوب الذي يتم فيه التعديل . و تتحمل الأطراف - عند تنزيل هذا الملف - مسؤولية عدم الإخلال بسياسة الترخيص لـ Adobe، في حين أن السكرتارية العامة لأيزو لا تتحمل أي مسؤولية قانونية حيال هذا المجال .

تعد الـ Adobe علامة تجارية مسجلة للشركة المتحدة لنظم الـ Adobe.

يمكن الحصول على جميع التفاصيل الخاصة بالبرامج المستخدمة في إنشاء هذا الملف من المعلومات العامة المتعلقة بملف (PDF) ، ولأجل الطباعة فقد حُسِّنت المتغيرات الداخلة في إنشاء (PDF)، حيث رُوِيَ أن يكون استخدام هذا الملف ملائماً لأعضاء المنظمة الدولية للتقييس ، وفي حالة حدوث أي مشكلة تتعلق بهذا الملف ، يُرجى إبلاغ السكرتارية العامة على العنوان المسجل أدناه.

### جهات التقييس العربية التي أعتمدت المواصفة

- مؤسسة المواصفات والمقاييس الأردنية
- هيئة الإمارات للمواصفات والمقاييس
- المعهد الجزائري للتقييس
- الهيئة السعودية للمواصفات والمقاييس
- الجهاز المركزي للتقييس والسيطرة النوعية
- الهيئة العامة للصناعة
- الهيئة السودانية للمواصفات والمقاييس
- الهيئة اليمنية للمواصفات والمقاييس وضبط الجودة
- المعهد الوطني للمواصفات والملكية الصناعية
- هيئة المواصفات والمقاييس العربية السورية
- المركز الوطني للمواصفات والمعايير القياسية
- الهيئة المصرية العامة للمواصفات والجودة



وثيقة حماية حقوق الطبع والنشر

أيزو/ أي إي سي ٢٠١٥ ©

جميع الحقوق محفوظة. وما لك يرد خلاف ذلك، لا يجوز إعادة إنتاج أي جزء من هذا الإصدار أو استخدامه بأي شكل أو بأي وسيلة إلكترونية أو ميكانيكية بما في ذلك النسخ والأفلام الدقيقة دون إذن خطي إما من المنظمة الدولية للتقييس على العنوان أدناه أو احد الهيئات الأعضاء في المنظمة الدولية للتقييس في دولة الجهة الطالبة.

مكتب حقوق ملكية المنظمة الدولية للتقييس

الرمز البريدي: ٥٦-1211-Ch- جنيف ٢٠

هاتف: ٠٠٤١٢٢٧٤٩٠١١١

فاكس: ٠٠٤١٢٢٧٤٩٠٩٤٧

بريد الكتروني: copyright@iso.org

الموقع الإلكتروني: www.iso.org

تم نشر النسخة العربية في ٢٠١٨

تم النشر في سويسرا

## تمهيد

تشكل المنظمة الدولية للتقييس أيزو و اللجنة الكهروتقنية الدولية أي إي سي المنظمة المتخصصة للتقييس على المستوى العالمي . تشارك الهيئات الوطنية الأعضاء في أيزو أو أي إي سي في تطوير المواصفات الدولية من خلال اللجان الفنية التي كونتها أي من المنظمين للتعامل مع مجالات بعينها من النشاط الفني. وتتعاون اللجان الفنية في كل من أيزو و أي إي سي في المجالات ذات الاهتمام المشترك. المنظمات الدولية الأخرى الحكومية منها وغير الحكومية، المتواصلة مع أيزو و أي إي سي، تقوم بدورها في هذا العمل ، وفي مجال تكنولوجيا المعلومات، أنشأت أيزو أي إي سي لجنة فنية مشتركة، هي أيزو/أي إي سي اللجنة الفنية المشتركة ١ .

تعد صياغات المواصفات الدولية وفقا للقواعد الواردة في توجيهات أيزو/أي إي سي ، في جزءها الثاني.

والمهمة الرئيسية للجنة الفنية المشتركة هي إعداد المواصفات الدولية. وتوزع مشروعات المواصفات الدولية المعتمدة من قبل اللجنة الفنية المشتركة على الهيئات القومية للتصويت. ويتطلب النشر كمواصفة دولية موافقة ٧٥٪ على الأقل من الهيئات القومية المشاركة في التصويت.

ونلفت الانتباه هنا إلى احتمال أن تكون بعض عناصر هذا المستند موضوعا لحقوق براءات الاختراع. وسوف لن تكون أيزو و أي إي سي مسؤولة عن تحديد أي أو كل من مثل هذه الحقوق لبراءات الاختراع.

أعدت المواصفة الدولية أيزو/أي إي سي ٢٧٠١٧ اللجنة الفنية المشتركة أيزو/أي إي سي اللجنة الفنية المشتركة الخاصة بتقنية المعلومات ، اللجنة الفرعية ٢٧ ، تقنيات تأمين المعلومات ، بالتعاون مع قطاع الاتصالات بالاتحاد الدولي للاتصالات (ITU-T) . النص المناظر منشور بالخدمات السحابية

<https://standards.iteh.ai/catalog/standards/sist/flcdcf95-c8ee-4fa9-9e35-e56c34b305df/iso-iec-27017-2015>

الاتحاد الدولي للاتصالات

**X.1631**  
(07/2015)

**ITU-T**  
قطاع مواصفات الاتصالات  
باتحاد الاتصالات الدولي

السلسلة X : شبكات البيانات، اتصالات وأمن النظم المفتوحة

أمن الحوسبة السحابية – تصميم أمن الحوسبة السحابية

THE STANDARD PUBLISHING HOUSE  
(standards.itu-t.org)

تقنية المعلومات – تقنيات التأمين – كود ممارسات ضوابط  
أمن المعلومات المبنية على المواصفة أيزو/أي إي سي  
٢٧٠٠٢ للخدمات السحابية

توصية قطاع الاتصالات بالاتحاد الدولي للاتصالات ITU-T X.1631



ITU-T

## DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY PUBLIC

	X.1–X.199
PUBLIC DATA NETWORKS	
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
<b>Cloud computing security design</b>	<b>X.1602–X.1639</b>
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

ولمزيد من التفاصيل، يرجى الرجوع إلى قائمة توصيات قطاع مواصفات الاتصالات باتحاد الاتصالات الدولية

**INTERNATIONAL STANDARD ISO/IEC 27017**  
**RECOMMENDATION ITU-T X.1631**

تقنية المعلومات – تقنيات التأمين – كود ممارسات ضوابط أمن المعلومات المبنية على المواصفة أيزو/أي إي سي ٢٧٠٠٢ للخدمات السحابية

ملخص:

تقدم التوصيات " ISO/IEC 27017/ITU-T X.1631 "دليلا إرشاديا لضوابط تأمين المعلومات المطبقة على تزويد الخدمات السحابية واستخدامها بواسطة تقديم :

- إرشادات تطبيق إضافية للضوابط ذات العلاقة في المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢.
- ضوابط إضافية مع إرشادات تطبيق ترتبط حصريا بالخدمات السحابية

تقدم هذه التوصيات /المواصفة الدولية ضوابط وإرشادات التطبيق لكل من مزودي الخدمة السحابية وزبائنهم.

الإصدارات والتعديلات

الكود المميز*	مجموعة الدراسة	تاريخ الاعتماد	رقم التوصيات	الإصدار
<a href="#">12490/1000/11.1002</a>	17	2015-07-14	ITU-T X.1631	١.٠

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

[ISO/IEC 27017:2015](#)

<https://standards.iteh.ai/catalog/standards/sist/flcdef95-c8ee-4fa9-9e35-e56c34b305df/iso-iec-27017-2015>

للوصول إلى التوصيات أكتب الـ <http://handle.itu.int/> في حقل العنوان متبوعا بالكود المميز للتوصيات مثال ذلك <http://handle.itu.int/11.1002/1000/11830-en> ،

## تمهيد

الاتحاد الدولي للاتصالات (ITU) هو وكالة الأمم المتحدة المتخصصة في مجال الاتصالات اللاسلكية والمعلومات وتقنيات الاتصال (ICTs). وقطاع توصيف الاتصالات اللاسلكية (ITU-T) هي عضو مهم في اتحاد الاتصالات الدولي. والقطاع مسئول عن دراسة توصيفالاتصالات اللاسلكية على أساس دولي. والجمعية الدولية لمواصفات الاتصالات العالمية (WTSA)، والتي تجتمع كل أربعة سنوات، توضع موضوعات الدراسة من قبل مجموعات الدراسة، التي تقوم بدورها بانتاج توصيات في هذا الصدد. وتعتمد توصيات القطاع التي تغطيها الإجراءات الموضوعية في المنشور ١ للجمعية الدولية لمواصفات الاتصالات العالمية. وفي بعض جوانب تقنية المعلومات التي تقع في نطاق مواصفات اتحاد الاتصالات الدولي - الضرورية فهي تعد بالتعاون مع منظمة التقييس الدولية ايزو واللجنة الكهروتقنية الدولية اي إي سي.

### ملحوظة:

في هذه التوصيات يستخدم تعبير "الإدارة" على سبيل الاختصار ليعني كلا من إدارة الاتصالات ووكالة التشغيل المعترف بها. والامتثال لهذه التوصيات طوعي. ومع ذلك فقد تحتوى المواصفة على عدة متطلبات الزامية (للتأكد التشغيل التبادلي / البيئي أو الانطباقية) ويتحقق الامتثال لهذه التوصيات عند الوفاء بجميع المتطلبات الإلزامية. وتستخدم الكلمات "ينبغي" أو غيرها مما يفيد الإلزام مثل "يجب" ومرادفاتها المنفية للتعبير عن المتطلبات / الاشتراطات. ولا يعنى استخدام أي من هذه الكلمات أن الامتثال لهذه التوصيات مطلوب من قبل أية جهة.

## iTeh STANDARD PREVIEW

### حقوق الملكية الفكرية

يلفت اتحاد الاتصالات الدولي الانتباه إلى احتمال أن تتضمن ممارسات أو تطبيقات هذه المواصفة استخدام حقوق مطلوبة للملكية الفكرية. ولا يتخذ اتحاد الاتصالات الدولي موقفا فيما يختص بدليل أوصحة أو انطباقية حقوق الملكية الفكرية المطلوبة، سواء كانت مطلوبة من قبل أعضاء في اتحاد الاتصالات الدولي أو من غيرهم من خارج عملية تطوير التوصيات. ولم ينلق اتحاد الاتصالات الدولي - حتى تاريخ اعتماد هذه التوصيات - ما يشير إلى حق للملكية الفكرية محمي ببراءات اختراع، قد تكون ضرورية لتطبيق هذه التوصيات. وعلى أية حال يحذر القائمون بالتطبيق من أن المعلومات الحالية في هذا الصدد قد لا تمثل أحدث المعلومات ومن ثم فهم مطالبون بالرجوع إلى قواعد بيانات براءات اختراع TSB على موقعه <http://www.itu.int/ITU-T/ipr/>

اتحاد الاتصالات الدولي ٢٠١٥

جميع الحقوق محفوظة. ولا يجوز إعادة انتاج جزء من هذا المنشور ، بأي طريق كان، دون إذن كتابي من اتحاد الاتصالات الدولي

## المحتويات

١	..... المجال	١
١	..... المراجع التكميلية	٢
١	..... ١/٢ التوصيات   المواصفات الدولية المماثلة	١
١	..... ٢/٢ المراجع الإضافية	١
١	..... التعاريف والاختصارات	٣
١	..... ١/٣ المصطلحات المعرفة في أماكن أخرى	١
٢	..... ٢/٣ الاختصارات	٢
٢	..... المفاهيم الخاصة بالقطاع السحابي	٤
٢	..... ١/٤ نظرة عامة	٢
٢	..... ٢/٤ علاقات الموردين في الخدمات السحابية	٢
٣	..... ٣/٤ العلاقات بين زبائن زبائن الخدمات السحابية ومزودها	٣
٣	..... ٤/٤ إدارة مخاطر أمن المعلومات في الخدمات السحابية	٣
٣	..... ٥/٤ هيكل هذه المواصفة	٣
٤	..... سياسات أمن المعلومات	٥
٤	..... ١/٥ توجهات الإدارة الخاص بأمن المعلومات	٤
٥	..... تنظيم أمن المعلومات	٦
٥	..... ١/٦ التنظيم الداخلي	٥
٥	..... ٢/٦ الأجهزة المحمولة والعمل عن بعد	٥
٦	..... أمن الموارد البشرية	٧
٦	..... ١/٧ قبل التوظيف	٦
٦	..... ٢/٧ أثناء التوظيف	٦
٧	..... ٣/٧ إنهاء التوظيف أو تغيير الوظيفة	٧
٧	..... إدارة الأصول	٨
٧	..... ١/٨ المسؤولية عن الأصول	٧
٨	..... ٢/٨ تصنيف المعلومات	٨
٨	..... ٣/٨ تداول الوسائط	٨
٨	..... ضبط الوصول	٩
٨	..... ١/٩ متطلبات / اشتراطات الأعمال في ضبط الوصول	٨
٩	..... ٢/٩ ادارة وصول المستخدمين	٩
١٠	..... ٣/٩ مسؤوليات المستخدمين	١٠
١٠	..... ٤/٩ ضبط الوصول للنظم والتطبيقات	١٠
١١	..... التشفير	١٠
١١	..... ١/١٠ ضوابط التشفير	١١
١٢	..... التأمين المادي والبيئي	١١
١٢	..... ١/١١ المناطق الآمنة	١٢
١٢	..... ٢/١١ المعدات	١٢
١٣	..... أمن العمليات	١٢
١٣	..... ١/١٢ الإجراءات والمسؤوليات التشغيلية	١٣
١٤	..... ٢/١٢ الحماية من البرامجيات الضارة	١٤
١٤	..... ٣/١٢ النسخ الاحتياطي	١٤
١٥	..... ٤/١٢ التسجيل والرصد	١٥
١٦	..... ٥/١٢ ضبط البرامجيات التشغيلية	١٦
١٦	..... ٦/١٢ إدارة نقاط الضعف الفنية	١٦
١٧	..... ٧/١٢ اعتبارات تدقيق نظم المعلومات	١٧

١٧	تأمين الاتصالات	١٣
١٧	١/١٣ إدارة تأمين الشبكات	
١٧	٢/١٣ تحويل / نقل المعلومات	
١٨	اقتناء وتطوير وصيانة النظم	١٤
١٨	١/١٤ متطلبات التأمين لنظم المعلومات	
١٨	٢/١٤ التأمين في عمليات التطوير والدعم	
١٩	٣/١٤ بيانات الاختبار	
١٩	علاقات الزبائن	١٥
١٩	١/١٥ تأمين المعلومات في علاقات الزبائن	
٢٠	٢/١٥ إدارة تقديم المورد للخدمة	
٢٠	إدارة حالات تأمين المعلومات	١٦
٢٠	١/١٦ إدارة حالات تأمين المعلومات والتحسينات	
٢٢	جوانب تأمين المعلومات من إدارة استمرارية النشاط	١٧
٢٢	١/١٧ استمرارية تأمين المعلومات	
٢٢	٢/١٧ التكرارات	
٢٢	الامتثال	١٨
٢٢	١/١٨ الامتثال للمتطلبات القانونية والتعاقدية	
٢٣	٢/١٨ مراجعات تأمين المعلومات	
٢٥	ملحق أ - مجموعة الضوابط الموسعة للخدمات السحابية	
٢٩	ملحق ب - مراجع في مخاطر تأمين المعلومات المرتبطة بالحوسبة السحابية	
٣٠	المصادر	

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 27017:2015](https://standards.iteh.ai/catalog/standards/sist/flcdcf95-c8ee-4fa9-9e35-e56c34b305df/iso-iec-27017-2015)

<https://standards.iteh.ai/catalog/standards/sist/flcdcf95-c8ee-4fa9-9e35-e56c34b305df/iso-iec-27017-2015>

## مقدمة

الإرشادات الواردة في هذه التوصيات | المواصفة الدولية هي إضافة إلى الإرشادات الواردة في أيزو/أي إي سي ٢٧٠٠٢ ومكملة لها . وعلى سبيل الخصوص تقدم هذه التوصيات | المواصفة الدولية إرشادات داعمة لتطبيق ضوابط تأمين المعلومات لزيائن و لمزودي الخدمة السحابية. بعض هذه الإرشادات هو لزيائن و لزيائن الخدمة السحابية الذين يطبقون الضوابط وبعضها لمزودي الخدمة السحابية لدعم تطبيق الضوابط. واختيار ضوابط أمن المعلومات المناسبة وإعمال إرشادات التطبيق الواردة ، يعتمد على تقديرات المخاطر وأي متطلبات /اشتراطات قانونية أو تعاقدية أو تنظيمية أو غيرها من متطلبات أمن المعلومات الخاصة بالقطاع السحابي.

# iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/IEC 27017:2015

<https://standards.iteh.ai/catalog/standards/sist/flcdcf95-c8ee-4fa9-9e35-e56c34b305df/iso-iec-27017-2015>

## تقنية المعلومات – تقنيات التأمين – كود الممارسة لضوابط تأمين المعلومات المبنية على المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢ للخدمات السحابية

### ١- المجال

تعطي هذه التوصيات/ المواصفة الدولية إرشادات لضوابط تأمين المعلومات المطبقة على تقديم واستخدام الخدمات السحابية بواسطة تقديم:

- إرشادات التطبيق الإضافية للضوابط ذات العلاقة في المواصفة أيزو/أي إي سي ٢٧٠٠٢.
  - الضوابط الإضافية مع إرشادات التطبيق التي تتصل بخصوصية الخدمات السحابية.
- تقدم هذه التوصيات/ المواصفة الدولية الضوابط وإرشادات التطبيق لكل من مقدمى ومستخدمى الخدمات السحابية.

### ٢- المراجع التكميلية

تتضمن التوصيات والمواصفات الدولية التالية الأسانيد التي تشكل – عبر الإشارة المرجعية لها في هذا النص- أسانيد/ مراجع هذه التوصيات | المواصفة الدولية. وقد كانت الطبقات المشار إليها للمواصفات والتوصيات سارية المفعول ، في وقت النشر. وتخضع جميع التوصيات والمواصفات للمراجعة، وأطراف الاتفاقيات المبنية على أساس هذه التوصيات | المواصفة مطالبون ببحث إمكانية تطبيق أحدث طبعة من التوصيات والمواصفات الواردة أدناه. يحتفظ أعضاء أيزو و أي إي سي بسجلات بالمواصفات الدولية السارية المفعول حالياً. يحتفظ مكتب تقييس الاتصالات التابع للاتحاد الدولي للاتصالات بقيادة توصيات قطاع الاتصالات بالاتحاد الدولي للاتصالات (ITU-T) الصالحة حالياً.

#### ١/٢ التوصيات /المواصفات الدولية المماثلة

- Recommendation ITU-T Y.3500 (in force) | ISO/IEC 17788: (in force), *Information technology – Cloud computing – Overview and vocabulary.*
- Recommendation ITU-T Y.3502 (in force) | ISO/IEC 17789: (in force), *Information technology – Cloud computing – Reference architecture.*

<https://standards.iteh.ai/catalog/standards/sist/f1cdef95-c8ee-4fa9-9e5e-6e5e5e5e5e5e/iso-iec-27017-2015>

#### ٢/٢ المراجع الإضافية

- ISO/IEC 27000: (in force), *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*
- ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.*

### ٣- المصطلحات والتعاريف

#### ١/٣ المصطلحات المعرفة في أماكن أخرى

لأغراض هذه التوصيات | المواصفة الدولية ، تسرى المصطلحات والتعاريف الواردة في المواصفات ISO/IEC 27000, Rec. ITU-T Y.3500 | ISO/IEC 17788, Rec. ITU-T Y.3502 | ISO/IEC 17789 إلى جانب التعاريف التالية :

#### ١/١/٣ المصطلح التالي معرف في المواصفة الدولية أيزو ١٩٤٤٠

- القدرة : مدى جودة إمكانية أداء نشاط بعينه

#### ٢/١/٣ المصطلحات التالية معرفة في المواصفة الدولية أيزو/أي إي سي ٢٧٠٤٠

- اختراق البيانات : استغلال أمني يؤدي إلى التدمير العرضى أو المخالف للقانون أو إلى الفقد أو التغيير أو الكشف غير المصرح به أو الوصول لبيانات محمية منقولة أو مخزونة أو معالجة بغير ذلك من الأشكال
- تأمين تعدد المستخدمين : نوع تعدد المستخدمين الذى يوظف ضوابط التأمين للحماية الصريحة ضد الاختراقات الأمنية ويقدم التحقق من صلاحية هذه الضوابط لأغراض الحوكمة السليمة.
- ملحوظة ١ - يوجد تأمين تعدد المستخدمين عندما يكون نمط المخاطر المميز للمستخدم المنفرد ليس أكثر منه عندما يكون فى بيئة مخصصة للمستخدم المنفرد
- ملحوظة ٢ - فى البيانات البالغة التأمين ، حتى هوية المستخدم يحتفظ بها سرية

## ٣/١/٣ المصطلحات المعرفة في المواصفة الدولية أيزو/ أي إي سي ١٧٢٠٣

- الماكينة الافتراضية : البيئة المتكاملة الداعمة لتنفيذ برامج مستضافة

ملحوظة - الماكينة الافتراضية هو احتواء كامل للعتاد الافتراضى والأقراص الصلبة الافتراضية والبيانات الفوقية (البيانات المعرفة بالبيانات) المرتبطة بها. تسمح الماكينات الافتراضية بالاستخدام المضاعف للماكينة المادية (الملموسة) عبر طبقة برمجية تسمى المشرف الفوقى (العلوى).

## ٢/٣ الاختصارات

لأغراض هذه التوصيات المواصفة الدولية ، تسرى الاختصارات التالية:

IaaS	Infrastructure as a Service	البنية الأساسية كخدمة
PaaS	Platform as a Service	المنصة كخدمة
PII	Personally Identifiable Information	معلومات تحديد الشخصية
SaaS	Software as a Service	البرامج كخدمة
SLA	Service Level Agreement	اتفاقية مستوى الخدمة
CaaS	Communications as a Service	الاتصالات كخدمة
VM	Virtual Machine	الماكينة الافتراضية

## ٤ - المفاهيم الخاصة بالقطاع السحابى

## ١/٤ نظرة عامة

غير استخدام الحوسبة السحابية كيف ينبغي للمنظمات تقدير وتجنب مخاطر تامين المعلومات وذلك للتغيرات الهامة فى كيفية تصميم الموارد الحاسوبية وتشغيلها وحوكمتها. تقدم هذه التوصيات/المواصفة الدولية إرشادات تطبيق إضافية للخصوصية السحابية مبنية على المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢ وتقدم ضوابط إضافية لتستهدف التهديدات والمخاطر الخاصة بتأمين المعلومات من منظور الحوسبة السحابية.

ينبغي أن يرجع مستخدمو هذه التوصيات/المواصفة الدولية إلى البندين ٥ و ١٨ من المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢ للضوابط وإرشادات التطبيق ولمعلومات أخرى.فالكثير من الضوابط وإرشادات التطبيق والمعلومات الأخرى تسرى على كل من السياقات العامة وسياقات الحوسبة السحابية للمنشأة. مثال ذلك "البند ٢/١/٦ توزيع / تقسيم الواجبات " فى المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢ تقدم ضابطا يمكن استخدامه إذا ما كانت المنشأة تعمل كمزود بالخدمة أم لا. إضافة إلى ذلك يمكن لزبون الخدمة السحابية أن يحصل على متطلبات توزيع / تقسيم المهام فى البيئة السحابية من نفس الضابط ، كما فى تقسيم زبائن الخدمة السحابية إلى مديرين للخدمة السحابية ومستخدمين لها.

وكامتداد للمواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢ تقدم التوصيات /المواصفة الدولية المزيد من الضوابط وإرشادات التطبيق والمعلومات الأخرى ذات الخصوصية السحابية (انظر البند ٥/٤) والمقصود بها تجنب المخاطر التى تصاحب الخصائص الفنية والتشغيلية للخدمات السحابية (انظر الملحق ب). يمكن لكل من زبائن الخدمة السحابية ومزودى الخدمة السحابية الرجوع إلى المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢

وإلى هذه التوصيات /المواصفة الدولية لاختيار الضوابط مع إرشادات التطبيق وإضافة ضوابط أخرى إذا دعت الضرورة . يمكن تنفيذ هذه العملية بإجراء تقييم مخاطر أمن المعلومات وعلاج هذه المخاطر فى سياقها المنظومى وسياق الأعمال الذى تستخدم فيه الخدمة أو تقدم (انظر البند ٤/٤).

## ٢/٤ علاقات الموردين فى الخدمات السحابية

تقدم المواصفة أيزو/أي إي سي ٢٧٠٠٢ فى البند ١٥ "علاقات الموردين" الضوابط وإرشادات التطبيق والمعلومات الأخرى لإدارة أمن المعلومات فى علاقات الموردين. ويعد تقديم واستخدام الخدمات السحابية لونا من علاقات الزبائن ، يمثل فيه زبون الخدمة السحابية جانب الطالب فى حين يمثل مزود الخدمة السحابية جانب المورد. لذلك يطبق البند على زبائن الخدمة السحابية وعلى مقدميها.

يمكن أيضا أن يشكل مستخدمو الخدمة السحابية ومزودوها سلسلة توريد . لنفترض أن مزودا للخدمة السحابية يقوم بتقديم خدمة من نوع قدرات البنية التحتية. إضافة إلى ذلك ، يقدم مزود آخر للخدمة السحابية خدمة من نوع قدرات التطبيقات. ففى هذه الحالة يعد مزود الخدمة السحابية الثانى زبون خدمة سحابية بالنسبة للأول ويعد مزودا للخدمة السحابية بالنسبة لزبون الخدمة السحابية المستخدم لخدماته. يصور هذا المثال الحالة التى تطبق فيها هذه التوصيات/ المواصفة الدولية على منشأة تكون بمثابة زبون للخدمة السحابية ومزود لها . ولأن زبون الخدمة السحابية والمزود لها يشكلان سلسلة توريد عبر تصميم

وتنفيذ الخدمات السحابية ، فإن البند " ٣/١٥ " سلسلة توريد تقنية الاتصالات والمعلومات " من المواصفة أيزو/أي إي سي ٢٧٠٠٢ " يطبق هنا .  
وتقدم المواصفة في البند ١٥ الضوابط وإرشادات التطبيق والمعلومات الأخرى لإدارة أمن المعلومات في علاقات الزبائن .  
ويعد تقديم واستخدام الخدمات السحابية لونا من علاقات الزبائن ، يمثل فيه زبون الخدمة السحابية جانب الطالب في حين يمثل جانب مزود الخدمة السحابية جانب المورد . زمن ثم يطبق البند على زبائن الخدمة السحابية وعلى مقدميها .  
تقدم المواصفة أيزو/ أي إي سي ٢٧٠٣٦ المتعددة الأجزاء ، " أمن المعلومات في علاقات الزبائن " إرشادات تفصيلية فيما يختص بأمن المعلومات في علاقات الزبائن ، للطالب والمزود للمنتجات والخدمات .  
تتناول المواصفة الدولية أيزو/ أي إي سي ٢٧٠٣٦ في جزءها الرابع عل نحو مباشر أمن الخدمات السحابية في علاقات الزبائن . وتطبق هذه المواصفة أيضا على زبائن الخدمة السحابية كطالبيين وعلى مقدمي الخدمة السحابية كموردين .

#### ٣/٤ العلاقات بين زبائن الخدمة السحابية ومزودها

في بيئة الحوسبة السحابية ، تخزن بيانات زبون الخدمات السحابية وتنقل وتعالج من قبل الخدمة السحابية . ومن ثم يمكن أن تعتمد عمليات الأعمال لزبون الخدمات السحابية على تأمين معلومات الخدمة السحابية . ودون الرقابة الكافية على الخدمة السحابية ، فإن زبون الخدمة السحابية قد يكون بحاجة إلى اتخاذ تدابير حماية إضافية إلى جانب ممارساته لأمن المعلومات .  
وقبل الدخول في علاقة مع المورد ، يحتاج زبون الخدمة السحابية إلى اختيار الخدمة السحابية ، اخذاً في الحسبان الفجوات المحتملة بين متطلبات تأمين المعلومات لزبون الخدمة السحابية وقدرات تأمين المعلومات المقدمة من قبل الخدمة .  
ولدى اختيار الخدمة ، ينبغي على زبون الخدمة السحابية إدارة استخدام الخدمة السحابية على النحو الذي يفى بمتطلبات تأمين المعلومات . وفي هذه العلاقة ، ينبغي على مزود الخدمة السحابية تقديم الدعم المعلوماتي والتقني الضروري للوفاء بمتطلبات تأمين المعلومات لزبون الخدمة السحابية . وعندما تكون ضوابط تأمين المعلومات موضوعة سلفا بحيث لا يمكن تغييرها من قبل زبون الخدمة السحابية ، فإن زبون الخدمة السحابية قد يحتاج إلى أعمال ضوابط إضافية في ذاتها لتجنب المخاطر .

#### ٤/٤ إدارة مخاطر تأمين المعلومات في الخدمات السحابية

ينبغي على زبائن الخدمة السحابية ومزودها كليهما ، وضع عمليات إدارة مخاطر تأمين المعلومات موضع التنفيذ . وكلاهما ينصح بالرجوع إلى المواصفة الدولية أيزو/ أي إي سي ٢٧٠٠١ للحصول على متطلبات إجراء إدارة المخاطر في نظم لتأمين المعلومات وكذلك الرجوع للمواصفة أيزو/ أي إي سي ٢٧٠٠٥ للمزيد من الإرشادات حول إدارة المخاطر التأمين ذاتها . كما تساعد المواصفة أيزو ٣١٠٠٠ التي تطبق معها المواصفتان أيزو/ أي إي سي ٢٧٠٠١ وأيزو/ أي إي سي ٢٧٠٠٥ على فهم عام لإدارة المخاطر .

وعلى النقيض من الانطباقية العامة لعمليات إدارة المخاطر و تأمين المعلومات ، فإن للحوسبة السحابية لها أنواعها الخاصة من مصادر المخاطر ، وتتضمن التهديدات ونقاط الضعف ، الناتجة عن خصائصها ، مثل التشبيك ومقاييس مرونة النظام وتقاسم الموارد وتقديمية الخدمة الذاتية والإدارة طبقا للطلب . وتقديمية الخدمة العابرة للنظم القضائية ومحدودية الرؤية في وضع الضوابط موضع التنفيذ . يقدم الملحق ب المراجع التي تقدم المعلومات عن مصادر المخاطر والمخاطر ذات العلاقة في تقديم واستخدام الخدمات السحابية .  
تستهدف الضوابط وإرشادات الاستخدام الواردة في البنود من ٥ إلى ١٨ والملحق أ من هذه التوصيات / المواصفة الدولية ، مصادر المخاطر والمخاطر الخاصة بالحوسبة السحابية .

#### ٥/٤ هيكل هذه المواصفة

تم صياغة هذه التوصيات / المواصفة الدولية في هيكل مماثل لهيكل المواصفة أيزو/أي إي سي ٢٧٠٠٢ . وتتضمن هذه التوصيات / المواصفة الدولية البنود من ٥ إلى ١٨ من التوصيات / المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢ بذكر انطباقية نصوص كل بند وفقرة .

عندما تطبق الأهداف والضوابط في المواصفة أيزو/أي إي سي ٢٧٠٠٢ دون حاجة إلى أي معلومات إضافية ، وتكون المرجعية إلى المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢ .  
ولدى الحاجة إلى أهداف مع الضوابط أو إلى ضوابط جديدة تحت أهداف موجودة في المواصفة أيزو/أي إي سي ٢٧٠٠٢ بالإضافة إلى تلك الواردة في المواصفة أيزو/أي إي سي ٢٧٠٠٢ ، فإنها واردة في الملحق أ : مجموعة الضوابط الممتدة الخاصة بالخدمة السحابية . وعند احتياج ضوابط من المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٢ أو الملحق أ من هذه التوصيات / المواصفة الدولية إلى إرشادات تطبيق إضافية خاصة بالخدمات السحابية ذات علاقة بالضابط ، فإنها ترد تحت العنوان الفرعي " إرشادات التطبيق للخدمات السحابية " ، وتقدم الإرشادات في واحد من النوعين التاليين :  
النوع الأول ويستخدم عندما تكون هناك إرشادات منفصلة لكل من زبون الخدمة السحابية ومزودها  
النوع الثاني ويستخدم عندما تكون الإرشادات هي نفسها لكل من زبون الخدمة السحابية ومزودها  
النوع الأول

زبون الخدمة السحابية	مزود الخدمة السحابية