الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1641

(2016/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية

مبادئ توجيهية لأمن بيانات عملاء الخدمات السحابية

التوصية ITU-T X.1641

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
القياسات البيومترية عن بُعد	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية	X.1349–X.1340
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	**X.1659–X.1640**
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1641

مبادئ توجيهية لأمن بيانات عملاء الخدمات السحابية

ملخص

تقدم التوصية ITU-T X.1641 مبادئ توجيهية عامة لأمن بيانات عملاء الخدمات السحابية (CSC). وهي تحلل دورة حياة أمن بيانات عملاء الخدمات السحابية وتطرح متطلبات أمنية في كل مرحلة من مراحل دورة حياة البيانات. وعلاوةً على ذلك، تقدم التوصية ITU-T X.1641 مبادئ توجيهية عن توقيت استعمال كل من هذه الضوابط بالنسبة إلى أفضل الممارسات الأمنية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1641	2016-09-07	17	11.1002/1000/12853

مصطلحات أساسية

بيانات عملاء الخدمات السحابية، ضوابط أمن البيانات، دورة حياة أمن البيانات.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1641

مبادئ توجيهية لأمن بيانات عملاء الخدمات السحابية

1 مجال التطبيق

تقدم هذه التوصية مبادئ توجيهية لأمن بيانات عملاء الخدمات السحابية (CSC) في الحوسبة السحابية، بالنسبة إلى الحالات التي يكون فيها مورد الخدمة السحابية (CSP) مسؤولاً عن كفالة تداول البيانات بالأمن الأمثل. وليست هذه هي الحالة الغالبة، حيث يكون عملاء الخدمات السحابية أنفسهم هم المسؤولين في بعض الخدمات السحابية عن أمن البيانات. وفي حالات أخرى يجوز أن تكون المسؤولية مشتركة.

فعلى سبيل المثال، يجوز أن يكون مورد الخدمات السحابية مسؤولاً، في بعض الحالات عن تقييد النفاذ إلى البيانات، في حين يظل عميل الخدمة السحابية مسؤولاً عن تحديد أي من مستعملي الخدمة السحابية (CSU) الذين يمكنهم النفاذ إليها وسلوك أي من القواعد أو التطبيقات التي يعالج بها المستعملون هؤلاء البيانات.

وتحدد هذه التوصية ضوابط الأمن لبيانات عملاء الخدمات السحابية التي يمكن استعمالها في المراحل المختلفة لدورة الحياة الكاملة للبيانات وقد تختلف ضوابط الأمن هذه عندما يتغير مستوى أمن بيانات عملاء الخدمات السحابية. لذا، تقدم هذه التوصية مبادئ توجيهية عن توقيت استعمال كل من هذه الضوابط بالنسبة إلى أفضل الممارسات الأمنية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية.

والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1601] التوصية ITU-T X.1601 (2015) *إطار أمني للحوسبة السحابية*.

[ITU-T X.1631] التوصية ITU-T X.1631 (2015) | ISO/IEC 27017: 2015، *تكنولوجيا المعلومات – تقنيات الأمن – مدونة القواعد المراعية لضوابط أمن المعلومات في خدمات الحوسبة السحابية استناداً إلى المعيار ISO/IEC 27002*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 استيقان [b-NIST-SP-800-53]: التحقّق من هوية المستعمل أو العملية أو الجهاز، غالباً كشرط أساسي للسماح بالنفاذ إلى الموارد في نظام المعلومات أو إلى موارد افتراضية بتوفير ذاتي للخدمة والإدارة حسب الطلب.

2.1.3 الحوسبة السحابية [b-ITU-T Y.3500]: نموذج للتمكين من النفاذ الشبكي إلى مجموعة قابلة للزيادة ومرنة من الموارد المادية أو الموارد الافتراضية التي يمكن تقاسمها والتزود بها على أساس الخدمة الذاتية وإدارتها حسب الطلب.

ملاحظة – تشمل أمثلة الموارد المخدمات وأنظمة التشغيل والشبكات والبرمجيات والتطبيقات ومعدات التخزين.

3.1.3 خدمة سحابية [b-ITU-T Y.3500]: قدرة أو عدد أكبر من القدرات تُقدم عن طريق الحوسبة السحابية وتُلبى باستخدام سطح بيني محدد.

4.1.3 عميل الخدمة السحابية [b-ITU-T Y.3500]: طرف يكون مرتبطاً بعلاقة تجارية لأغراض استخدام الخدمات السحابية.

ملاحظة – لا تستوجب العلاقة الضرورية بالضرورة ترتيبات مالية.

5.1.3 بيانات عملاء الخدمات السحابية [b-ITU-T Y. 3500]: صنف أشياء البيانات قيد المراقبة، طبقاً لدواعي قانونية أو أي دواعي أخرى، الخاصة بعميل الخدمة السحابية والمدخلة إلى الخدمة السحابية، أو الناتجة عن استعمال قدرات الخدمة السحابية بواسطة عميل الخدمة السحابية أو بالنيابة عنه عن طريق سطح بيني معلن للخدمة السحابية.

الملاحظة 1 – من أمثلة الضوابط القانونية حق النسخ.

الملاحظة 2 – يجوز أن تتضمن الخدمة السحابية أو تعمل على بيانات خلاف بيانات عملاء الخدمات السحابية؛ وقد تكون هذه البيانات هي تلك التي يوفرها موردو الخدمات السحابية أو يتم الحصول عليها من مصدر آخر أو قد تكون بيانات متاحة للعامة. وبالتالي، فإن أي بيانات خرج تنتج عن إجراءات يقوم بها عميل الخدمة السحابية باستعمال قدرات الخدمة السحابية على هذه البيانات، يرجح أن تكون من بيانات عملاء الخدمات السحابية، طبقاً للمبادئ العامة لحق النسخ، ما لم تكن هناك أحكام محددة في اتفاق الخدمة السحابية تنص على خلاف ذلك.

6.1.3 بيانات مشتقة من الخدمة السحابية [b-ITU-T Y.3500]: صنف أشياء بيانات تخضع لتحكم مقدم الخدمة السحابية وتشتق كنتيجة لتعامل عميل الخدمة السحابية مع هذه الخدمة.

7.1.3 مقدم الخدمة السحابية [b-ITU-T Y.3500]: طرف يتيح توافر الخدمات السحابية.

8.1.3 مستعمل الخدمة السحابية [b-ITU-T Y.3500]: شخص طبيعي أو كيان يعمل بالنيابة عنه يرتبط بأحد عملاء الخدمة السحابية ويستعمل الخدمات السحابية.

ملاحظة – تشمل الأمثلة على هذه الكيانات الأجهزة والتطبيقات.

9.1.3 البنية التحتية كخدمة (IaaS) [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية من نوع قدرات البُنى التحتية.

10.1.3 تعدد الشاغلين [b-ITU-T Y.3500]: توزيع الموارد المادية والافتراضية بحيث يتم عزل الشاغلين المتعددين وحساباتهم وبياناتهم عن بعضهم البعض، ويكون النفاذ غير ممكن فيما بين بعضهم البعض.

11.1.3 المنصات كخدمة (PaaS) [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية من نوع قدرات المنصة.

12.1.3 الطرف [b-ITU-T Y.3500]: شخص طبيعي أو اعتباري، اكتسب الشخصية الاعتبارية أم لم يكتسبها، أو مجموعة تضم كليهما.

13.1.3 المعلومات المحدِّدة لهوية شخص (PII) [b-ISO/IEC 29100]: معلومات (أ) يمكن أن تستخدم للتعرّف إلى هوية الشخص الذي تتعلق به هذه المعلومات، أو (ب) قد تكون مرتبطة بشكل مباشر أو غير مباشر بهوية الشخص المراد التعرف عليه من خلالها.

14.1.3 صاحب المعلومات المحددة لهوية شخص (PII) [b-ISO/IEC 29100]: شخص طبيعي تخصه المعلومات المحددة لهوية شخص (PII).

ملاحظة – طبقاً للولاية القضائية والتشريعات السارية لحماية البيانات والخصوصية، يمكن استعمال المرادف "موضوع البيانات" بدلاً من مصطلح "صاحب المعلومات المحددة لهوية شخص"

15.1.3 البرمجيات كخدمة (SaaS) [b-ITU-T Y.3500]: فئة من الخدمات السحابية تكون فيها القدرات السحابية المقدمة لعميل الخدمة السحابية من نوع قدرات التطبيقات.

16.1.3 شاغل [b-ITU-T Y.3500]: مستعمل واحد أو أكثر من مستعملي الخدمات السحابية الذين يتقاسمون النفاذ إلى مجموعة من الموارد المادية والافتراضية.

17.1.3 تهديد [b-ISO/IEC 27000]: السبب المحتمل لحادث غير مرغوب قد يُلحق ضرراً بنظام أو منظمة.

2.3 مصطلحات معرفة في هذه التوصية

لا يوجد.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

CSC عميل الخدمة السحابية *(Cloud Service Customer)*

CSP مورد الخدمة السحابية *(Cloud Service Provider)*

CSU مستعمل الخدمة السحابية *(Cloud Service User)*

IaaS البنية التحتية كخدمة *(Infrastructure as a Service)*

PaaS المنصة كخدمة *(Platform as a Service)*

PII المعلومات المحددة لهوية شخص *(Personally Identifiable Information)*

SaaS البرمجيات كخدمة *(Software as a Service)*

5 الاصطلاحات

لا يوجد.

6 لمحة عامة

1.6 مواصفات البيانات المتناولة في هذه التوصية

تشمل بيانات عملاء الخدمات السحابية بيانات خاصة للعملاء مخزنة في منصة سحابية والبيانات ذات الصلة لعملاء الخدمات السحابية عبر هذه الخدمات، مثل معلومات الحسابات وسجلات تسجيل الدخول وسجل التشغيل وما إلى ذلك.

والفارق بين مصطلحي عميل الخدمات السحابية (انظر الفقرة 4.1.3 أعلاه) ومستعمل الخدمات السحابية (انظر الفقرة 8.1.3 أعلاه)، يتم تمييزه مجدداً على النحو التالي.

فعميل الخدمة السحابية (CSC) هو الشخص أو المنظمة الذي يدخل أو تدخل في علاقة قانونية مع مورد الخدمة السحابية. لذا، يجوز أن يكون عميل الخدمة السحابية شركة أو جهة فرعية أو إدارة حكومية أو عميل فردي.

ومستعمل الخدمة السحابية (CSU) هو الشخص أو الجهاز أو التطبيق الذي يستعمل الخدمة السحابية التي تعاقد بشأنها. وقد يكون مستعمل الخدمة السحابية موظفاً حكومياً أو تطبيقاً يتم تشغيله على هاتف ذكي أو عميل فردي أو فرد من أي أسرة كطفل مثلاً. ويعين عميل الخدمة السحابية عادةً بعض مستعملي الخدمة السحابية للعمل كمديرين ولإدارة العلاقة بين عميل الخدمة السحابية وموردها. ويعمل أي مستعمل للخدمة السحابية عادةً بالنيابة عن عميل من عملاء الخدمة السحابية. ومعظم مستعملي الخدمة السحابية من الموظفين يحتاجون إلى قدر ضئيل أو لا يحتاجون بالمرة إلى رؤية ما يقوم به مورد الخدمة السحابية أو كيف يقوم

به، أو الخدمات التي يكون عميل الخدمة السحابية قد تعاقد عليها، ما لم يحدد عميل الخدمة السحابية ضرورة معرفتهم لهذه الأمور (مثل المديرين والمراجعين الداخليين).

ويمكن لعميل الخدمة السحابية أن يضم العديد من الشاغلين. ويمكن للشاغل أن يضم العديد من مستعملي الخدمة السحابية.

2.6 تهديدات أمن البيانات بالنسبة إلى عملاء الخدمات السحابية

بما أن بيئة الخدمة السحابية هي عادةً بيئة متعددة الشاغلين، فإن فقدان البيانات أو تسربها يشكل تهديداً خطيراً لعميل الخدمة السحابية. فقد يسبب غياب الإدارة المناسبة لمعلومات التجفير، مثل مفاتيح التجفير وشفرات الاستيقان وامتيازات النفاذ، ضراراً بالغاً مثل فقدان البيانات وتسربها غير المتوقع إلى الخارج. وعلى سبيل المثال فإن النقص في الاستيقان والترخيص وضوابط المراجعة؛ والاستعمال غير المتوافق لمفاتيح التجفير و/أو الاستيقان؛ والإخفاقات التشغيلية؛ ومشاكل التخلص من المخلّفات؛ والمسائل القضائية والسياسية؛ واعتمادية مركز البيانات؛ والتعافي من الكوارث، هي كلها عوامل يمكن اعتبارها مصادر كبيرة لهذا التهديد ويمكن ربطها بالتحديات.

وكما هو الحال بالنسبة إلى أمن بيانات التخزين، فما دامت جميع بيانات مستعملي الخدمات السحابية تخزن في معدات موردي هذه الخدمات، وما دامت موارد التخزين يتم تقاسمها بين عملاء خدمات سحابية مختلفين، فإن هذه البيانات قد تواجه العديد من المخاطر، بما في ذلك:

1) يمكن أن تتعرض الأطراف الداخلية ذات الامتيازات للنفاذ غير المخول مما يؤدي إلى تسرب بيانات عملاء الخدمات السحابية؛
2) يمكن للمستعملين غير الأسوياء أو القراصنة أن يحصلوا أيضاً على نفاذ غير مخول مما يؤدي إلى تسرب عملاء الخدمات السحابية؛
3) يمكن لتدفق البيانات عبر الحدود أن يؤدي إلى تسربها، خاصة البيانات السحابية؛
4) أعطال البرمجيات والعتاد وانقطاع الطاقة الكهربائية والكوارث الطبيعية يمكن أن تؤدي إلى فقدان البيانات.

ويكمن أمن البيانات أيضاً في عملية النقل. حيث يمكن سرقة البيانات أو تغييرها أثناء النقل، مما يؤدي بدوره إلى انتهاك السرية إذا كانت البيانات غير مجفرة بشكل سليم . وعندما لا يعتمد عملاء الخدمات السحابية التجفير المناسب، ينبغي لموردي الخدمات السحابية التحقق من سلامة البيانات واتخاذ تدابير التجفير المقابلة.

وهناك تهديد آخر يتمثل في تسرب البيانات المتبقية. فعندما يلغي أحد عملاء الخدمات السحابية خدمته، تتم إزالة بياناته وتحرر مساحة التخزين الخاصة به أو يعاد توزيعها لعملاء خدمات سحابية آخرين. وتقع على كاهل مورد الخدمة السحابية مسؤولية ضمان عدم إمكانية استعادة أطراف أخرى للبيانات المتبقية لأحد عملاء الخدمات السحابية أو الشاغلين.

3.6 المتطلبات الحالية المتعلقة بأمن البيانات

يوفر "الإطار الأمني للحوسبة السحابية الموصف في التوصية [ITU-T X.1601]" المتطلبات المتعلقة بأمن البيانات، بما في ذلك عزل البيانات وحمايتها وحماية السرية.

1) عزل البيانات

يُمنع الشاغل في إطار الحوسبة السحابية من النفاذ إلى بيانات تخص شاغلاً آخر، حتى وإن كانت البيانات مجفّرة، إلا إذا كان النفاذ مسموحاً صراحةً. وقد يتحقق عزل البيانات بطريقة منطقية أو مادية تبعاً لدقة العزل المطلوب والنشر المحدد لبرمجيات الحوسبة السحابية وتجهيزاتها.

ملاحظة – يحدث العزل في الحوسبة السحابية على مستوى الشاغل. وقد يكون لأحد عملاء الحوسبة السحابية عدة شاغلين في الخدمة السحابية، وذلك مثلاً لفصل الكيانات التابعة أو الشعب أو الوحدات التجارية المختلفة عن بعضها البعض.

2) حماية البيانات

تضمن حماية البيانات أن تكون بيانات عميل الخدمة السحابية والبيانات المشتقة منها والمحتفظ بها في بيئة الحوسبة السحابية محمية بالشكل الصحيح بحيث لا يمكن النفاذ إليها أو تغييرها إلا على النحو الذي سمح به عميل الخدمة السحابية (أو وفقاً لقانون ساري المفعول). وقد تشمل هذه الحماية توليفة من قوائم التحكم في النفاذ، وتدقيق السلامة، وتصحيح الأخطاء/استعادة البيانات، والتجفير، وغير ذلك من الآليات المناسبة. وعندما يوفر مقدم الخدمة السحابية لعملاء الخدمة السحابية إمكانية تجفير التخزين، فقد تكون هذه الوظيفة تجفيراً من جانب العميل (مثلاً ضمن تطبيق خاص بعميل الخدمة السحابية) أو تجفيراً من جانب المخدّم.

3) حماية الخصوصية

يمكن أن تشمل حماية الخصوصية المعلومات المحددة لهوية الشخص (PII) والبيانات السرية للشركات. وقد يخضع جمع المعلومات الخاصة واستعمالها ونقلها وتداولها وتخزينها وإتلافها إلى اللوائح أو القوانين المتعلقة بالخصوصية. وينطبق هذا التقييد على كل من موردي الخدمات السحابية وعملاء الخدمة السحابية التابعين لهم، إذ يتعين مثلاً على عميل الخدمة السحابية أن يكون قادراً على حذف جدول بيانات بشكل دائم يحتوي على معلومات خاصة حتى ولو كان مقدم الخدمة السحابية على غير علم بمحتويات الجدول. وقد يتعين على مقدمي الخدمات السحابية أيضاً دعم عملية تداول المعلومات، كالبحث مثلاً في بيانات عملاء الخدمة السحابية بشكليها المحوّل أو المجفّر.

وتمتد حماية الخصوصية لتشمل المعلومات الخاصة التي يمكن رصدها أو استخلاصها من أنشطة عملاء الخدمة السحابية، مثل الاتجاهات التجارية، أو العلاقات أو الاتصالات مع باقي الأطراف، ومستويات النشاط وأنماطه.

كما أن حماية الخصوصية مسؤولة عن التأكد من أن جميع المعلومات الخاصة (بما فيها المعلومات المرصودة أو المستخلصة) لا تستعمل إلا للأغراض المتفق عليها بين عميل الخدمة السحابية ومورد الخدمة السحابية.

وقد يسهم إجراء تقييم للمخاطر المتعلقة بالمعلومات الخاصة (يسمى "تقييم مخاطر الخصوصية") بمساعدة مورد الخدمة السحابية في تحديد المخاطر الخاصة بانتهاك الخصوصية التي تدخل في إحدى العمليات المتوخاة. ويتعين على مورد الخدمة السحابية أن يحدد وينفذ القدرات اللازمة للتصدي لمخاطر الخصوصية التي حددها تقييم مخاطر المعلومات الخاصة ومعالجتها.

ملاحظة – في بعض الولايات القضائية، يُعامل الأفراد الطبيعيون (أي المستعملون من البشر) بشكل منفصل عن مستخدميهم لأغراض الخصوصية. وفي مثل تلك الظروف تكون خصوصية مستعمل الخدمة السحابية (CSU) محمية بالشكل المناسب بالإضافة إلى عميل الخدمة السحابية (CSC) أو شاغل الخدمة السحابية.

4.6 دورة حياة أمن البيانات

استناداً إلى الوضع الفعلي للخدمة السحابية، تتضمن دورة حياة أمن بيانات عملاء الخدمات السحابية المراحل التالية:

1) الاستحداث: يرجح أن يفضل تسمية هذه المرحلة استحداث/تحديث لأنها تنطبق على استحداث أو تغيير عنصر بيانات/محتوى، وليس وثيقة أو قاعدة بيانات فقط. فالاستحداث هو توليد محتوى رقمي جديد أو تعديل/تحديث محتوى قائم.

2) النقل: هذه هي عملية الاتصالات الخاصة بنقل البيانات من مكان إلى آخر.

3) التخزين: التخزين هو عملية تسليم البيانات الرقمية إلى نوع معين من مستودعات التخزين وتحدث عادةً بالتزامن تقريباً مع مرحلة الاستحداث.

4) الاستعمال: معاينة البيانات أو معالجتها أو تقاسمها أو غير ذلك من الاستعمال في بعض أنواع الأنشطة.

5) الانتقال: انتقال البيانات هي عملية انتقالها بين أنواع مستودعات التخزين أو أنساق التخزين أو الأنظمة الحاسوبية. وهي أحد الاعتبارات الرئيسية لتنفيذ أي نظام أو ترقيته أو توحيده. وتحدث عملية انتقال البيانات لمجموعة من الأسباب المختلفة، بما في ذلك: عمليات الإحلال للمخدمات أو معدات التخزين أو ترقيتها؛ توحيد الموقع الإلكتروني؛ صيانة المخدمات؛ تغيير موقع مركز البيانات.

6) التدمير: تدمير البيانات نهائياً باستعمال وسائل مادية أو رقمية (مثل فك التجفير).

7) إعداد نسخ احتياطية واستعادة البيانات: يمكن للمستعملين إعداد نسخ احتياطية للبيانات واستعادة البيانات من هذه النسخ.

7 مبادئ توجيهية بشأن الضوابط الأمنية المتعلقة بأمن البيانات

تقدم هذه الفقرة مبادئ توجيهية بشأن الضوابط الأمنية المتعلقة بمراحل دورة حياة أمن البيانات المشروحة في الفقرة 4.6

1.7 الضوابط الأمنية في مرحلة الاستحداث

تشمل المبادئ التوجيهية بشأن الضوابط الأمنية في مرحلة الاستحداث ما يلي:

أ) ينبغي لموردي الخدمات السحابية تحديد فئات حساسية البيانات. ويمكن الاستفادة من وسم المستعملين للبيانات في المساعدة في تصنيف البيانات.

ب) ينبغي تصنيف البيانات طبقاً لحساسيتها عند استحداثها.

ج) ينبغي لموردي الخدمات السحابية النظر في آليات الحقوق الرقمية للشركات أو التجفير لحماية البيانات الحساسة من النفاذ غير المرخص.

2.7 الضوابط الأمنية في مرحلة النقل

تشمل المبادئ التوجيهية بشأن الضوابط الأمنية في مرحلة النقل ما يلي:

أ) ينبغي لموردي الخدمات السحابية تطبيق أساليب تكنولوجية لضمان أمن بيانات الاستيقان.

ب) ينبغي لموردي الخدمات السحابية دعم المستعملين في تأمين النقل الآمن لبيانات العمليات الحساسة وبيانات الإدارة.

ج) ينبغي اكتشاف مظاهر الإضرار بسلامة البيانات سريعاً أثناء النقل واتخاذ التدابير اللازمة لاستعادة سلامة البيانات بعد اكتشاف الأخطاء المتعلقة بسلامتها.

3.7 الضوابط الأمنية في مرحلة التخزين

تشمل المبادئ التوجيهية بشأن الضوابط الأمنية في مرحلة التخزين ما يلي:

أ) ينبغي لموردي الخدمات السحابية تحديد ضوابط النفاذ المتاحة لكي يستعملها عميل الخدمة السحابية مع بيانات المستعملين المستقاة من مستودعات تخزين مثل تلك المحددة في التوصية [ITU-T X.1631].

ب) ينبغي لموردي الخدمات السحابية تطبيق تكنولوجيا تجفير أو أي وسائل حماية أخرى لضمان سرية تخزين بيانات الاستيقان.

ج) ينبغي لموردي الخدمات السحابية دعم المستعملين لتأمين التخزين السري لبيانات العمليات الحرجة وبيانات الإدارة.

د) ينبغي لموردي الخدمات السحابية توفير وسائل حماية فعّالة للأقراص الصلبة أو اعتماد آليات تخزين قابلة للتجزئة لمنع المستعملين غير المخولين من الحصول على بيانات مستعمل شرعي من القرص الصلب حتى ولو تمت سرقته.

هـ) ينبغي اكتشاف مظاهر الإضرار بسلامة بيانات التخزين سريعاً واتخاذ التدابير اللازمة لاستعادة سلامة البيانات بعد اكتشاف الأخطاء المتعلقة بسلامتها.

و) ينبغي دعم التشكيل الاختياري لمعلمات التجفير من قبل المستعملين مثل الخوارزميات والشدة والمخططات.

ز) ينبغي لموردي الخدمات السحابية دعم المستعملين في اختيار آلية تجفير طرف ثالث لتجفير بيانات المفاتيح.

ح) ينبغي لموردي الخدمات السحابية دعم تجفير البيانات باستعمال مفاتيح مؤمنة ودعم التخزين والحفاظ على المفاتيح المؤمنة محلياً.

ط) ينبغي لموردي الخدمات السحابية توفير أساليب حماية فعالة لتحميل ملفات صور الآلات الافتراضية لمنع المستعملين غير المخولين من تشغيلها على مواردهم الحاسوبية من القرص الصلب حتى ولو تمت سرقته.

4.7 الضوابط الأمنية في مرحلة الاستعمال

تشمل المبادئ التوجيهية بشأن الضوابط الأمنية في مرحلة الاستعمال ما يلي:

أ) ينبغي لموردي الخدمات السحابية تخويل استخدام البيانات والتحقق منه.

ب) ينبغي مراجعة استخدام البيانات الحساسة، بإعداد سجلات مراجعة.

ج) ينبغي لموردي الخدمات السحابية تطبيق آليات للمراقبة والإنفاذ للأنشطة الضارة طبقاً لمسؤولياتهم وحقوقهم في اكتشاف التهديدات ومراقبة استعمال البيانات.

5.7 الضوابط المنية في مرحلة الانتقال

تشمل المبادئ التوجيهية بشأن الضوابط الأمنية في مرحلة الانتقال ما يلي:

أ) ينبغي تقييم توصيلية الشبكة قبل انتقال البيانات لضمان سلامة عملية الانتقال.

ب) ينبغي لموردي الخدمات السحابية ضمان عدم تأثر سلامة البيانات وسريتها أثناء أي عملية من عمليات الانتقال.

ج) ينبغي لموردي الخدمات السحابية ضمان عدم تأثير انتقال البيانات على استمرارية الخدمات والتطبيقات.

د) ينبغي لموردي الخدمات السحابية الاضطلاع بأعمال إنشاء النسخ الاحتياطية للبيانات واستعادتها بشكل مناسب أثناء انتقال البيانات.

ه) ينبغي لموردي الخدمات السحابية إعداد مخطط انتقال وتقييم جدواه والمخاطر ذات الصلة، ثم وضع تدابير تحكم طبقاً لذلك عند التحضير لانتقال البيانات.

6.7 الضوابط الأمنية في مرحلة التدمير

تشمل المبادئ التوجيهية بشأن الضوابط الأمنية في مرحلة التدمير ما يلي:

أ) ينبغي لموردي الخدمات السحابية أن تكون لديهم القدرة على إزالة جميع المواد الرئيسية المتعلقة بالبيانات المشفرة.

ب) ينبغي لموردي الخدمات السحابية استخدام التدمير المادي، مثل إزالة مغناطيسية الوسائط المادية عند إلغاء استخدام عتاد التخزين.

ج) ينبغي لموردي الخدمات السحابية استخدام تقنيات استرجاع البيانات للتحقق من عمليات التدمير.

د) ينبغي لموردي الخدمات السحابية أن تكون لديهم القدرة على توفير وسائل للمساعدة في إزالة البيانات التقليدية الناتجة عن انتقال البيانات بين المنصات السحابية المختلفة، وعن إنهاء الخدمة والعقد وعن الكوارث الطبيعية.

ه) ينبغي لموردي الخدمات السحابية توفير وسيلة لإزالة جميع النسخ الخاصة بالبيانات.

و) ينبغي لموردي الخدمات السحابية التأكد من أن مساحة التخزين الخاصة بمعلومات الاستيقان من المستعمل مثل حساب المستعمل وكلمة السر الخاصة به لن يتم تحريرها أو إعادة تخصيصها لمستعملين آخرين قبل إزالة هذه الموارد بشكل كامل.

ز) ينبغي لموردي الخدمات السحابية التأكد من أن مساحة التخزين الخاصة بموارد مثل الملفات والمجلدات وسجلات قواعد البيانات لا يتم تحريرها أو إعادة تخصيصها لمستعملين آخرين قبل إزالة هذه الموارد بشكل كامل.

ح) ينبغي لموردي الخدمات السحابية توفير وسائل لمنع استرجاع البيانات المدمرة.

7.7 الضوابط الأمنية في مرحلة إنشاء النسخ الاحتياطية واستعادة البيانات

تشمل المبادئ التوجيهية بشأن الضوابط الأمنية في مرحلة إنشاء النسخ الاحتياطية واستعادة البيانات ما يلي:

أ) ينبغي لموردي الخدمات السحابية استخدام آليات استرجاع المحتوى مثل آليات منع فقدان البيانات للمساعدة في تحديد ومراجعة البيانات التي تحتاج إلى إعداد نسخ احتياطية.

ب) ينبغي لموردي الخدمات السحابية دعم خوارزمية تجفير مناسبة من أجل إعداد النسخ الاحتياطية لوسائط التخزين طويلة الأجل (الأرشيفية)، كاستخدام مفاتيح تجفير طويلة والتخطيط للإحلال بخوارزمية تجفير محسنة.

ج) ينبغي لموردي الخدمات السحابية توفير وظائف محلية لإعداد النسخ الاحتياطية للبيانات واسترجاعها. وينبغي إعداد نسخ احتياطية كاملة للبيانات مرة كل أسبوع على الأقل وإعداد النسخ الاحتياطية الجزئية مرة واحدة يومياً على أقل تقدير.

د) ينبغي إنشاء مركز استرجاع للبيانات عن بُعد في حالات الكوارث، مزود بوسائل مثل خطوط الاتصالات والمعدات الشبكية ومعدات معالجة البيانات من الوسائل اللازمة لاسترجاع البيانات في حالات الكوارث.

ه) يمكن إنشاء مركز احتياطي لاسترجاع البيانات في حالات الكوارث. وينبغي لهذا المركز أن يوفر قدرة أساسية مكافئة لتشغيل الأعمال ومزامنة البيانات في الوقت الفعلي عبر وصلة عالية السرعة. ويمكن لهذا المركز تقاسم عمليات تشغيل الأعمال وأنظمة الإدارة في آن واحد مع الحفاظ على استمرارية الأعمال من خلال مفتاح طوارئ للتبديل في حالات الكوارث.

و) بالنسبة إلى البيانات التي تعتبر إما مهمة أو حساسة، ينبغي لموردي الخدمات السحابية توفير وظائف إعداد نسخ احتياطية للبيانات عن بُعد مع القدرة على استرجاع البيانات في الوقت المناسب. ومن النهج المتاحة لتوفير هذه الخدمة هو أن تنفذ عن طريق شبكة باستخدام مركز من مراكز استرجاع البيانات في حالات الكوارث.

التذييل I

مبادئ توجيهية لاستعمال الضوابط الأمنية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم الجدول 1.I أمثلة لمجموعات من الضوابط التي يمكن استعمالها لتطبيق المبادئ التوجيهية بالنسبة إلى بعض الأمثلة الخاصة بسيناريوهات البيانات استناداً إلى تطبيق البيانات والمرحلة من دورة الحياة.

الجدول 1.I – مثال لمجموعات من الضوابط

النوع	دورة حياة البيانات						
	الاستحداث	**النقل**	**التخزين**	**الاستعمال**	**الانتقال**	**التدمير**	**إعداد النسخ الاحتياطية واستعادة البيانات**
IaaS البنية التحتية كخدمة	1.7 أ)، ب)، ج)	2.7 أ)، ب)، ج)	3.7 أ)، ب)، ج)، د)، هـ)، ح)، ط)	4.7 أ)، ب)، ج)	5.7 أ)، ب)، ج)، د)، هـ)	6.7 أ)، ب)، ج)، د)، هـ)، و)، ز)، ح)	7.7 أ)، ج)، د)، هـ)، و)
PaaS المنصة كخدمة	1.7 أ)، ب)، ج)	2.7 أ)، ب)، ج)	3.7 أ)، ب)، ج)، د)، هـ)، و)، ح)	4.7 أ)، ب)، ج)	5.7 أ)، ب)، ج)، د)، هـ)	6.7 أ)، ب)، ج)، د)، هـ)، و)، ز)، ح)	7.7 أ)، ب)، ج)، د)، هـ)، و)
SaaS البرمجيات كخدمة	1.7 أ)، ب)، ج)	2.7 أ)، ب)، ج)	3.7 أ)، ب)، ج)، د)، هـ)، و)، ز)، ح)، ط)	4.7 أ)، ب)، ج)	5.7 أ)، ب)، ج)، د)، هـ)	6.7 أ)، ب)، ج)، د)، هـ)، و)، ز)، ح)	7.7 أ)، ب)، ج)، د)، هـ)، و)

بيبليوغرافيا

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology -- Security techniques -- Privacy framework*.

[b-NIST-SP-800-53] NIST Special Publication 800-53 Revision 4_ (2015), *Security and privacy controls for Federal information systems and organizations*, Available [viewed 2016-12-10] at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2017