International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1641

(09/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security best practices and guidelines

Guidelines for cloud service customer data security

Recommendation ITU-T X.1641

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
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
Cloud computing security design	X.1602–X.1639
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

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1641

Guidelines for cloud service customer data security

Summary

Recommendation ITU-T X.1641 provides generic security guidelines for the cloud service customer (CSC) data in cloud computing. It analyses the CSC data security lifecycle and proposes security requirements at each stage of the data lifecycle. Furthermore, Recommendation ITU-T X.1641 provides guidelines on when each control should be used for best security practice.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1641	2016-09-07	17	11.1002/1000/12853

Keywords

Cloud service customer data, data security controls, data security lifecycle.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1641

Guidelines for cloud service customer data security

1 Scope

This Recommendation provides guidelines for cloud service customer (CSC) data security in cloud computing, for those cases where the cloud service provider (CSP) is responsible for ensuring that the data is handled with proper security. This is not always the case, since for some cloud services the security of the data is the responsibility of CSCs themselves. In other cases, the responsibility may be mixed.

For example, in some cases the CSP may be responsible for restricting access to the data, while the CSC remains responsible for deciding which cloud service users (CSUs) should have access to it, and the behaviour of any scripts or applications with which the CSU processes the data.

This Recommendation identifies security controls for CSC data that can be used in different stages of the full data lifecycle. These security controls can differ when the security level of the CSC data changes. Therefore, this Recommendation provides guidelines on when each control should be used for best security practice.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T X.1631] Recommendation ITU-T X.1631 (2015) | ISO/IEC 27017:2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-NIST-SP-800-53]: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.2 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.3 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.4 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using **cloud services**.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.5 cloud service customer data [b-ITU-T Y.3500]: Class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service.

NOTE 1 – An example of legal controls is copyright.

NOTE 2 – It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers , or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.

3.1.6 cloud service derived data [b-ITU-T Y.3500]: Class of data objects under cloud service provider control that are derived as a result of interaction with the cloud service by the cloud service customer.

3.1.7 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.8 cloud service user [b-ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.9 infrastructure as a service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

3.1.10 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.

3.1.11 platform as a service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

3.1.12 party [b-ITU-T Y.3500]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.13 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.1.14 PII principal [b-ISO/IEC 29100]: Natural person to whom the personally identifiable information (PII) relates.

NOTE – Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

3.1.15 software as a service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3.1.16 tenant [b-ITU-T Y.3500]: One or more cloud service users sharing access to a set of physical and virtual resources.

3.1.17 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CSC Cloud Service Customer

CSP Cloud Service Provider

CSU Cloud Service User

IaaS Infrastructure as a Service

PaaS Platform as a Service

PII Personally Identifiable Information

SaaS Software as a Service

5 Conventions

None.

6 Overview

6.1 Specification of the data in this Recommendation

CSC data includes private data of customers stored on a cloud platform and related data through cloud services for CSC, such as account information, login record and operation log.

The difference between the terms CSC (see clause 3.1.4) and CSU (see clause 3.1.8) is further distinguished as follows.

The CSC is the person or organization that enters into the legal relationship with the CSP. So the CSC could be an enterprise, a subsidiary, a government department or an individual consumer.

The CSU is the person, device or application that uses the cloud service that has been contracted for. The CSU could be a government employee, an application running on a smartphone, an individual consumer or a member of a household, such as a child. The CSC usually nominates some CSUs to act as administrators and manage the relationship between the CSC and the CSP. A CSU always acts on behalf of a CSC. Most employee CSUs need to have little or no visibility of what or how the CSP operates, or the services that the CSC has contracted for, unless the CSC decides they need to know (e.g. administrators and internal auditors).

A CSC can include multiple cloud tenants. A tenant can include multiple CSUs.

6.2 Data security threats for cloud service customers

As the cloud service environment is typically multi-tenant, loss or leakage of data is a serious threat to the CSC. The lack of appropriate management of cryptographic information, such as encryption keys, authentication codes and access privilege, could lead to significant damage, such as data loss and unexpected data leakage. For example, insufficient authentication, authorization and audit controls; inconsistent use of encryption or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data centre reliability and disaster recovery, can be recognized as major sources of this threat and may be associated with the challenges.

As for the security of storage data, since all CSC data is actually stored in the equipment of CSPs, and the storage resources is shared by different CSCs, it may face several risks, including:

1) CSP insiders with privileges can gain unauthorized access resulting in leakage of CSC data;
2) malicious users or hackers can also gain unauthorized access resulting in leakage of CSC data;

3) cross-border data flow can lead to data leakage, especially for sensitive data;

4) software and hardware failures, power outages and natural disasters can result in data loss.

Data security also lies in the process of transmission. Data can be stolen or tampered with during transmission, thus lead to confidentiality leakage, if the data is not encrypted properly. If CSCs have not adopted adequate encryption, CSPs should verify the integrity of the data and take corresponding encryption measures.

Another threat is the leakage of residual data. When a CSC unsubscribes its service, its data is cleared and the storage space released or reallocated to other CSCs. It is the responsibility of the CSP to ensure that the residual data of one CSC or tenant cannot be recovered by another.

6.3 Existing requirements related to about data security

The security framework for cloud computing specified in [ITU-T X.1601] provides the requirements related to data security, including data isolation, protection and confidentiality protection.

1) Data isolation

   In a cloud computing context, a tenant is prevented from accessing data belonging to another tenant, even when the data is encrypted, except when explicitly authorized. Data isolation may be realized logically or physically, depending on the required isolation granularity and the specific deployment of cloud computing software and hardware.

   NOTE – In cloud computing, isolation occurs at the tenant level. A given CSC may have multiple tenants in the cloud, for example, to separate different subsidiaries, divisions or business units.

2) Data protection

   Data protection ensures that CSC data and cloud service derived data held in a cloud computing environment is appropriately secured so that it can only be accessed or changed as authorized by the CSC (or according to applicable law). This protection may include some combination of access control lists, integrity verification, error correction/data recovery, encryption and other appropriate mechanisms. When a CSP provides storage encryption for CSCs, this function can be client-side encryption (e.g., within a CSP application) or server-side encryption.

3) Confidentiality protection

   Private information can include personally identifiable information (PII) and confidential corporate data. The collection, use, transfer, handling, storage and destruction of private information can be subject to confidentiality regulations or laws. This restriction applies to both CSPs and their CSCs, e.g., a CSC must be able to permanently delete a data table containing private information, even though the CSP is not aware of the table contents. CSPs may also need to support information handling, e.g., searching of CSC data in its transformed or encrypted form.

   Confidentiality protection extends to private information that may be observed or derived from CSC activities, such as business trends, relationships or communications with other parties, and activity levels and patterns.

   Confidentiality protection is also responsible for ensuring that all private information (including observed or derived data) is used only for those purposes that have been agreed between a CSC and a CSP.

   A risk assessment of private information (called a "confidentiality risk assessment") can assist a CSP in identifying the specific risks of confidentiality breaches involved in an envisaged operation. The CSP should identify and implement capabilities to address the confidentiality risks identified by the risk assessment and treatment of private information.

NOTE – In some jurisdictions, individual natural persons (i.e., human users) are treated separately from their employers for confidentiality purposes. In such circumstances, confidentiality of the CSU will be appropriately protected in addition to that of the CSC or tenant.

6.4 Data security lifecycle

Based on the actual situation of cloud service, the CSC data security lifecycle includes:

1) Creation: This is probably better named creation/update because it applies to creating or changing a data/content element, not just a document or database. Creation is the generation of new digital content, or the alteration/updating of existing content.
2) Transmission: This is the communication process of transferring data from one place to another.
3) Storage: Storage is the act of committing the digital data to some sort of repository, and typically occurs nearly simultaneously with creation.
4) Use: Data is viewed, processed, shared or otherwise used in some sort of activity.
5) Migration: Data migration is the process of transferring data between storage types, formats, or computer systems. It is a key consideration for any system implementation, upgrade, or consolidation. Data migration occurs for a variety of reasons, including: server or storage equipment replacements or upgrades; website consolidation; server maintenance; and data centre relocation.
6) Destruction: Data is permanently destroyed using physical or digital means (e.g., crypto shredding).
7) Backup and restoration: Users can create data backups and restore data from backups.

7 Guidelines for security controls related to data security

This clause provides guidelines for security controls related to the stages of the data security lifecycle described in clause 6.4.

7.1 Security controls in create stage

Guidelines for security controls in the create stage include the following:

a) CSPs should define categories of data sensitivity. User tagging of data may be leveraged to help classify the data.
b) Data should be classified according to its sensitivity when it is created.
c) CSPs should consider enterprise digital rights mechanisms or encryption to protect sensitive data from unauthorized access.

7.2 Security controls in transmit stage

Guidelines for security controls in the transmit stage include the following:

a) CSPs should apply technological methods to ensure the security of the authentication data.
b) CSPs should support users in the maintenance of secure transmission of critical operation data and management data.
c) Damage to data integrity should be detected promptly during transmission and necessary measures taken to restore data integrity after errors are detected.

7.3 Security controls in storage stage

Guidelines for security controls in the storage stage include the following:

a) CSPs should identify access controls available to the CSC to use with users' data from storage repositories, such as those defined in [ITU-T X.1631].

b) CSPs should apply encryption technology or other safeguards to ensure the storage confidentiality of authentication data.

c) CSPs should support users in the maintenance of confidential storage of critical operation data and management data.

d) CSPs should provide effective hard disk protection methods or adopt fragmentally storage mechanisms to prevent unauthorized users obtaining valid user data from the hard disk, even if it is stolen.

e) Damage to storage data integrity should be detected promptly and necessary measures taken to restore data integrity after errors are detected.

f) A user's optional configuration of encryption parameters, such as algorithms, strength and schemas, should be supported.

g) CSPs should support users in the selection of a third-party encryption mechanism to encrypt the key data.

h) CSPs should support data encryption using secure keys and support storage and maintenance of the secure keys locally.

i) CSPs should provide effective virtual machine image file loading protection methods to prevent unauthorized users running their own computing resources from the hard disk, even if it is stolen.

7.4 Security controls in use stage

Guidelines for security controls in the use stage include the following:

a) CSPs should authorize and verify the utilization of data.

b) Utilization of sensitive data should be audited, with audit logs generated.

c) CSPs should apply malicious activity monitoring and enforcement mechanisms according to their responsibility and rights to discover threats and control data usage.

7.5 Security controls in migrate stage

Guidelines for security controls in the migrate stage include the following:

a) Network connectivity should be assessed prior to data migration to ensure the safety of the migration process.

b) CSPs should ensure that data integrity and confidentiality is not affected during a migration.

c) CSPs should ensure that data migration does not affect the continuity of services and applications.

d) CSPs should conduct data backup and recovery-related work appropriately during data migration.

e) CSPs should establish a migration scheme, assess its feasibility and associated risks, then develop risk control measures accordingly as preparations for data migration.

7.6 Security controls in destroy stage

Guidelines for security controls in the destroy stage include the following:

a) CSPs should be able to erase all key material related to encrypted data.

b) CSPs should utilize physical destruction, such as degaussing of physical media when decommissioning storage hardware.

c) CSPs should utilize data recovery techniques to confirm destruction processes.

d) CSPs should be able to provide means to help clear legacy data caused by the migration of data among different cloud platforms, the termination of service and contract, and natural disasters.

e) CSPs should provide means to remove all copies of the data.

f) CSPs should ensure that the storage space for user authentication information, such as the user account and password, are not released or reallocated to other users until that information is fully cleared.

g) CSPs should ensure that the storage space for resources, such as files, directories and database records, are not released or reallocated to other users until those resources are fully cleared.

h) CSPs should provide means to prevent the recovery of destroyed data.

7.7 Security controls in backup and restore stage

Guidelines for security controls in the backup and restore stage include the following:

a) CSPs should utilize content recovery mechanisms, like those for data loss prevention, to assist in identifying and auditing data that needs to be backed up.

b) CSPs should support an appropriate encryption algorithm for long-term (archival) storage media backup, such as the use of long encryption keys and planning for replacement with an improved encryption algorithm.

c) CSPs should provide local data backup and recovery functions. Complete data backup should be conducted at least once a week and the incremental backup at least once a day.

d) A remote disaster recovery centre should be established, with facilities such as communication lines, network equipment and data processing equipment that are needed for disaster recovery integrated into them.

e) A redundancy disaster recovery centre could be established. It should provide a basic equivalent capability for business operation and synchronize data in real time via a high-speed link. It could share the operations of the business and management systems simultaneously while maintaining business continuity through an emergency switch in disaster situations.

f) For data that is categorized as either important or sensitive, the CSPs should provide remote data backup functions together with the capability for timely data recovery. One approach to providing this service would be via a network utilizing a disaster recovery centre.

Appendix I

Guidelines for using security controls

(This appendix does not form an integral part of this Recommendation.)

Table I.1 provides example sets of controls that could be used to meet the guidelines for some example data scenarios based on data classification and lifecycle stage.

Table I.1 – Example sets of controls

Type	Data lifecycle						
	Creation	**Transmission**	**Storage**	**Use**	**Migration**	**Destruction**	**Backup and restoration**
IaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), c), d), e), f)
PaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), f), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)
SaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e),f), g), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)

Bibliography

[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>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017