International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1053

(11/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Security management

Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations

Recommendation ITU-T X.1053

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed legder technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
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.1053

Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations

Summary

Recommendation ITU-T X.1053 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security controls in small and medium-sized telecommunication organizations (SMTOs) based on Recommendation ITU-T X.1051. This Recommendation also provides an implementation baseline of information security controls for SMTOs to ensure the confidentiality, integrity and availability of telecommunication facilities and services and information handled, processed or stored by the facilities and services.

The objectives of this Recommendation are to provide practical guidance suited for SMTOs on commonly accepted goals of information security specifically suited for these organizations.

As a result of implementing this Recommendation, SMTOs, both within and between jurisdictions, will:

a) be able to ensure the confidentiality, integrity and availability of the specific SMTO facilities and services and the information handled, processed or stored within the facilities and services;

b) have adopted secure collaborative processes and controls ensuring the lowering of risks in the delivery of telecommunication services;

c) be able to deliver information security in an effective and efficient manner;

d) have adopted a consistent holistic approach to information security; and

e) be able to improve the security culture of organizations, raise staff awareness and increase public trust.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1053	2017-11-13	17	11.1002/1000/13367

Keywords

Availability, confidentiality, controls, integrity, security, SMTO.

---

* 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

Introduction

Small and medium-sized telecommunication organizations (SMTOs) typically spend little time considering how to manage information security and how to implement security controls, even though they face the same security threats and vulnerabilities as large telecommunication organizations. SMTOs should ensure that appropriate security considerations be adopted to minimize business risk and to ensure information security of their contracts and service level agreements (SLAs).

Recommendation ITU-T X.1053 provides guidelines for the implementation of information security management (ISM) that targets SMTOs based on Recommendation ITU-T X.1051, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

Security features (confidentiality, integrity, and availability) and terminologies used in this Recommendation are in line with those used in Recommendation ITU-T X.1051.

In order to provide telecommunication services, even in SMTOs, telecommunication organizations need to interconnect and/or share their telecommunication services and facilities, and/or use the telecommunication services and facilities of other telecommunication organizations. Therefore, the management of information security in telecommunication organizations is mutually dependent, and may include any and all areas of network infrastructure, services applications and other facilities.

Regardless of operational scale, service areas, service types, or number of employees, telecommunication organizations should implement appropriate controls to ensure confidentiality, integrity, availability, and any other security property of telecommunication.

This Recommendation provides SMTOs, and those responsible for information security, together with security vendors, auditors, telecommunication terminal vendors, and application content providers, with a common set of general security control objectives based on Recommendation ITU-T X.1051. It further provides these organizations with specific controls and information security management guidelines that allow for the selection and implementation of such controls.

Recommendation ITU-T X.1053

Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations

1 Scope

This Recommendation defines guidelines supporting the implementation of information security controls in small and medium-sized telecommunication organizations （SMTOs) based on [ITU-T X.1051] and [ISO/IEC 27002].

The adoption of this Recommendation will allow SMTOs to meet baseline security requirements of confidentiality, integrity, availability, and any other relevant security property specific to these organizations.

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.1051] Recommendation ITU-T X.1051 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this Recommendation, the definitions given in [ITU-T X.1051] and [ISO/IEC 27002] apply. Additionally, the following definitions apply:

3.1.1 confidentiality or non-disclosure agreement: A legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes.

3.1.2 data centre: A facility used to house computer systems and associated components, such as telecommunication and storage systems.

3.1.3 outsourcing: When an enterprise contracts out one or more of its internal processes and/or functions to an outside company. Outsourcing moves enterprise resources to an outside enterprise and keeps a retained capability to manage the relationship with the outsourced processes.

3.1.4 parent company: A company that owns enough voting stock in another firm to control management and operations by influencing or electing its board of directors.

3.1.5 small and medium-sized telecommunication organization: A telecommunication organization classified as a small and medium-sized business in accordance with the legislation or the regulations of the country or region in which the business is registered.

3.2 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CEO Chief Executive Officer

CISO Chief Information Security Officer

DMZ Demilitarized Zone

IT Information Technology

PII Personally Identifiable Information

SLA Service Level Agreement

SME Small Medium Enterprise

SMTO Small and Medium-sized Telecommunication Organization

4 Overview

4.1 Characteristics of the SMTO

A small and medium-sized telecommunication organization (SMTO) is generally defined according to certain criteria such as the number of employees, sales figures and asset scales (see Annex A).

In contrast to large organizations, SMTOs typically face difficulties in the implementation of information security controls due to limited resources (e.g., limitations of funds, manpower, skills and technology capacity). These can commonly be seen in the following ways:

a) the size and organization of SMTOs normally means that they do not have sufficient resources to focus on security issues in a full-time capacity, and that consequently security issues are often dealt with in parallel with other business tasks and functions. Since primary tasks handle other business functions and processes as a priority, security issues are often seen as a secondary task with low priority;

b) the development and deployment of standardized business procedures or standards for information security by SMTOs are often not as extensive or effective as in large organizations due to manpower restrictions;

c) the specified definition of information security in business processes is very often deficient or entirely lacking;

d) SMTOs generally have limited experience in the use of technology-based solutions, business applications and processes, and the storage and utilization of information. They tend to depend on limited executive experience and skills;

e) awareness of information security is often insufficient and information security policies are scarcely established. SMTOs sometimes fail to focus on some of the basic elements of an information security management system, such as identification of assets, risk assessments, access control and countermeasures for security incidents;

f) SMTOs feature greater chief executive officer (CEO)-centred decision making, making patterns in comparison with business as a whole. Therefore, SMTOs need simpler and more optimized (simplification of existing information security management system) information security activities; and

g) while large organizations tend to be capable of establishing their own internal expertise and developing and deploying more consistent information security management system by themselves, SMTOs find difficulty in procuring the correct expertise internally. An SMTO generally needs help from external professionals/institutions to deal with the main body of its security activities.

4.2 Implementation of information security management for SMTOs

4.2.1 Security considerations for SMTOs

The requirement for a generic security framework in an SMTO has originated from different sources:

a) customers/subscribers require confidence in the network and the services to be provided, including the availability, integrity and confidentiality of services according to the customer/subscriber service level agreement (SLA); and

b) network operators and service providers themselves require security to safeguard their own operational and business interests, as well as public and national infrastructure interests, and to meet their contractual obligations to their customers and their own suppliers (and public interests in general where necessary).

For an SMTO to protect information assets from different sources and under various telecommunication environments, security guidelines, policies and procedures and key activities to support the effective implementation of information security management are indispensable in an SMTO.

The security guidelines should be applicable to the following:

a) SMTO seeking a business advantage and investment opportunity through the implementation of an information security management system;

b) SMTO seeking the confidence and assurance that the information security requirements of their interested parties (e.g., suppliers, customers, regulators) will be satisfied;

c) users and suppliers of the information security-related products and services for the SMTO;

d) those parties, internal or external to the SMTO, who assess and audit the information security management system for conformity with the requirements of [b-ISO/IEC 27001]; and

e) those internal or external parties to the SMTO who give advice or training on the information security management system appropriate to that organization.

4.2.2 Design principles of implementation guidance for SMTOs

This Recommendation is structured in line with the format of [ITU-T X.1051] and/or [ISO/IEC 27002]. Considering the situations of SMTOs, there are four cases to provide control and implementation guidance:

a) in cases where controls specified in [ITU-T X.1051] are applicable without a need for any additional information, only a reference is provided to [ITU-T X.1051] and/or [ISO/IEC 27002];

b) in cases where controls are not necessarily required for SMTOs, only a reference is provided for information purposes;

c) in cases where controls do not need all of the implementation guidance in [ITU-T X.1051], the SMTO implementation guidance was constructed by removing unnecessary parts from the original [ITU-T X.1051] implementation guidance text; and

d) in cases where controls need some implementation guidance applicable to SMTOs, new guidance is provided as SMTO implementation guidance.

4.3 Structure of the guidance

The structure of this Recommendation is as follows:

– Clause 4 describes the security aspects of SMTOs to be considered for the effective implementations of information security controls; and

– Clauses 5 to 18 provide specific controls for SMTOs based on [ITU-T X.1051]. Each clause has the following internal structure:

  a) a control objective, which states what is to be achieved;

b) one or more controls that can be applied to achieve the control objective;

c) SMTO implementation guidance, which provides more detailed information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the SMTO's specific control requirements;

d) other information for SMTO, which provides further information that may need to be considered, for example legal considerations and references to other standards. If there is no other information to be provided this part is not shown.

– Annex A provides telecommunication extended control set for SMTOs based on [ITU-T X.1051].

NOTE – For each of the control objectives there may be one or more controls and associated implementation guidance.

5 Security policy

The control objective and the contents from [ISO/IEC 27002] clause 5 apply.

However, due to the characteristics of SMTOs, the degree of implementation needs to be (down-)scaled accordingly to fit their level of resources.

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

SMTO implementation guidance

SMTOs should have policies to guide information security activities to support their business purpose with consideration of the regulatory and legislative requirements.

Such policies should be approved by top management of SMTOs such as CEO or chief information security officer (CISO) and should be aware to all employees. Security responsibilities, roles, deviations and exceptions should be clarified through the approved policies.

5.1.2 Review of the policies for information security

Control and the contents from 5.1.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

Control and the contents from 6.1.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

SMTO implementation guidance

Since it would not be easy to segregate duties in small organizations, SMTOs should secure inter-independence among classified duties to minimize information security incidents.

6.1.3 Contact with authorities

Control and the contents from 6.1.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

6.1.4 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

SMTO implementation guidance

SMTOs should establish linkages with special interest groups or forums who have previous experience in improving information security environments (e.g., by establishing relationships and/or exchanging information). If it is difficult for SMTOs to establish linkages with special interest groups or forums due to limited resources, SMTOs may consider contracting with external partners. External partners could be relied on for advice on how to secure the information environment.

SMTOs should receive security vulnerability and attack information from reputable external sources which are trustworthy and often include vendor websites, industry news groups, mailing list or feeds.

6.1.5 Information security in project management

Control

Information security should be addressed in project management, regardless of the type of the project.

SMTO implementation guidance

SMTOs should have a procedure to ensure that information security risks are identified and addressed as part of a project. The procedure should be documented or published on the organization's bulletin to provide information regarding management of any project.

Risk assessment should be conducted to identify security risks and controls of the organizations. Information security issues, identified as a part of risk assessment, should be resolved and reviewed regularly for all projects. Security objectives and responsibilities for information security should be a part of risk assessment.

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

Control

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

SMTO implementation guidance

SMTOs should have mobile device usage guidelines which are suitable to their working environments. The guidelines should include recommendation for security of user activities and measures to avoid and mitigate security risks from mobile device usage. Risk assessment for mobile supporting environment should be recommended. SMTOs should decide on acceptable levels of security and should conduct some measures to avoid and mitigate security risks from the risk assessment result. Access to sensitive data and personally identifiable information (PII) should be restricted in unprotected mobile environments. Data recovery plans should be implemented according to the data stored in mobile devices.

6.2.2 Teleworking

Control and the contents from 6.2.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

7 Human resource security

7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

Control

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

SMTO implementation guidance

SMTOs should have a verification procedure for hiring employees. Information about all employees being considered for positions for granting or authorizing access within the organization should also be collected and handled in accordance with the procedure.

By the operation of the procedure (e.g., credit review or review of criminal records), SMTOs should also ensure that sensitive data and PII should be appropriately protected.

The procedure should be documented with consideration of PII protection and information security related regulations and employment-based legislation.

7.1.2 Terms and conditions of employment

Control and the contents from 7.1.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

7.2.1 Management responsibilities

Control and the contents from 7.2.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

7.2.2 Information security awareness, education and training

Control

All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

SMTO implementation guidance

SMTOs should make a plan to improve awareness of information security for all employees.

SMTOs should consider utilizing online education media with content which includes possible and existing information security incidents.

For security managers, SMTOs should devote to raising awareness of the information security related to the critical communication systems.

SMTOs should consider utilizing online education media with content that is focused on case studies about detection and prevention of information security events/incidents.

Appropriate knowledge and understanding of information security should be accompanied by appropriate action in order to:

a) achieve a better understanding of the level of perceived risk;

b) determine how the organization and its employees might be affected by inadequate information security; and

c) establish a corporate information security culture.

7.2.3 Disciplinary process

Control

There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

SMTO implementation guidance

SMTOs should establish a documented procedure to review any violation related to the organization's information security policies and procedures.

The procedure should consider to include the following:

a) how to approve collection of evidence;

b) how to review the collected evidence;

c) how to set criteria of penalties according to the level of violation of the regulation;

d) how to take an action on urgent and critical cases; and

e) how to announce the verification results.

The disciplinary procedure should be communicated to all employees in order to prevent violation of the organizational security policies and procedures.

7.3 Termination and change of employment

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

7.3.1 Termination or change of employment responsibilities

Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.

SMTO implementation guidance

SMTOs should state on the employment contracts that confidentiality or non-disclosure agreements and legal responsibilities may persist even after employees leave the organizations.

SMTOs should request additional confidentiality agreements for employees who have had privileges to access sensitive data and PII.

Confidentiality obligations and information security requirements should be informed to employees.

8 Asset management

8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

8.1.1 Inventory of assets

Control

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

SMTO implementation guidance

SMTOs should have documented criteria to maintain controls for critical assets. The value of the assets should be defined based on the business impact. The document of the asset inventory should include the owners and the classification and be kept up-to-date. (More information for the classification can be found in 8.2).

Other information for SMTO

Asset protection level should be considered with asset valuable level by [b-ITU-T X.1057].

8.1.2 Ownership of assets

Control and the contents from 8.1.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

8.1.3 Acceptable use of assets

Control and the contents from 8.1.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

8.1.4 Return of assets

Control and the contents from 8.1.4 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

8.2.1 Classification of information

Control

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

SMTO implementation guidance

SMTOs should classify the minimum amount of information that is necessary for a sustainable telecommunication service.

In classifying information, in addition to the general requirements for organizational sensitive and critical information, SMTOs should also take into account the following:

a) the possible need to separately classify the information related to non-disclosure of communications in terms of the existence, content, source, destination and date and time of the communicated information (see Annex A/TEL.18.1.7 of [ITU-T X.1051]); and

b) the distinction between the essential communications that need to be handled with priority in an emergency or at a risk of emergency, and non-essential communications (see Annex A/TEL.18.1.8 of [ITU-T X.1051]).

8.2.2 Labelling of information

Control and the contents from 8.2.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

8.2.3 Handling of assets

Control and the contents from 8.2.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

8.3.1 Management of removable media

Control

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

SMTO implementation guidance

SMTOs should install and use control systems for mobile storage devices to minimize information leakage via these mobile storage devices. Furthermore, SMTOs should encourage employees to register all of their mobile storage devices to minimize easy duplicability and maximize detectability.

8.3.2 Disposal of media

Control

Media should be disposed securely when no longer required, using formal procedures.

SMTO implementation guidance

If necessary SMTOs could outsource destruction of mobile storage devices to external professional firms/institutes.

8.3.3 Physical media transfer

Control and the contents from 8.3.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9 Access control

9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access control policy

Control

An access control policy should be established, documented and reviewed based on business and information security requirements.

SMTO implementation guidance

SMTOs should have a documented policy to implement access control rules to maintain appropriate information security level.

The policy should take into account the following:

a) access controls should be implemented based on security requirements for the business for organization;

b) procedures for accessing sensitive data and PII should be clearly defined;

c) access rights should be granted through the SMTOs' approval process;

d) records of access rights granted should be maintained to support security audits.

9.1.2 Access to networks and network services

Control and the contents from 9.1.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

9.2.1 User registration and de-registration

Control

A formal user registration and de-registration process should be implemented to enable assignment of access rights.

SMTO implementation guidance

SMTOs should manage user IDs to identify user activities.

Unique IDs should be used for each user to ensure access audit. Shared IDs should only be allowed if they can trace user activities.

SMTO should disable user IDs when they are no longer necessary.

Other information for SMTO

Unique IDs are required for each user to ensure access audit, but shared IDs are allowed if they can trace user activities. User access logs should be stored for a certain period for monitoring and auditing to detect security incidents. (See clause 12.4 for further information.)

9.2.2 User access provisioning

Control

A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.

SMTO implementation guidance

If SMTOs find that the risk related to access rights are low enough, they could choose to implement a verbal explanation and acceptance statement, rather than a written document.

Other information for SMTO

Regardless of above situations, SMTOs should keep in mind that in a court of law these practices could need more evidence to be accepted/acknowledged than written documents in accordance with the legislation or the regulations of the country or region.

9.2.3 Management of privileged access rights

Control

The allocation and use of privileged access rights should be restricted and controlled.

SMTO implementation guidance

Privileges should be allocated to users with a special mandate, such as system administrators, business managers, etc.

9.2.4 Management of secret authentication information of users

Control and the contents from 9.2.4 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9.2.5 Review of user access rights

Control and the contents from 9.2.5 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9.2.6 Removal or adjustment of access rights

Control and the contents from 9.2.6 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9.3 User responsibilities

Objective: To make accountable for safeguarding their authentication information.

9.3.1 Use of secret authentication information

Control and the contents from 9.3.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

9.4.1 Information access restriction

Control and the contents from 9.4.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9.4.2 Secure log-on procedures

Control and the contents from 9.4.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9.4.3 Password management system

Control and the contents from 9.4.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9.4.4 Use of privileged utility programs

Control and the contents from 9.4.4 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

9.4.5 Access control to program source code

Control and the contents from 9.4.5 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

10 Cryptography

10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Policy on the use of cryptographic controls

Control

A policy on the use of cryptographic controls for protection of information should be developed and implemented.

SMTO implementation guidance

Due to the specialized nature of cryptographic controls and technologies, SMTOs may need to seek expert advice when developing a cryptographic policy. For example, specialized advice is important when considering selection criteria from encryption algorithms which have already been implemented.

SMTOs should seek advice on the legal aspects of using cryptographic technologies in the various parts of the world in which they have business arrangements and contracts.

10.1.2 Key management

Control

A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.

SMTO implementation guidance

Due to the specialized nature of cryptographic controls and key management, SMTOs may need to seek expert advice when considering the various key management protocols and implementations that are possible to support a cryptographic policy.

11 Physical and environmental security

11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

11.1.1 Physical security perimeter

Control

Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

SMTO implementation guidance

SMTOs should consider and implement the following guidelines for physical security perimeters, where appropriate:

a) telecommunication operation rooms/centres should be equipped with adequate physical trespasser detection systems;

b) facilities for telecommunication services, e.g., transmission facilities, switching facilities and telecommunication infrastructure, should be located away from other facilities (e.g., customer facilities in managed data centres); and

c) physical barriers should be effectively installed, with all local security policies rigorously enforced to ensure the protection of SMTO assets at all times. If a physical barrier is malfunctioning or a policy is not followed, it is imperative that the issue be resolved immediately by management with the appropriate level of responsibility.

11.1.2 Physical entry controls

Control

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

SMTO implementation guidance

SMTOs should consider the following guidelines:

a) operation rooms/control rooms to operate telecommunication facilities should be protected by adequate entry controls, such as providing barriers or walls. Such entry controls should be equipped at least by means of physical access control.

b) upon entry, visitor's information should be correctly recorded to protect visitor's information against unauthorized access.

11.1.3 Securing offices, rooms and facilities

Control and the contents from 11.1.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

11.1.4 Protecting against external and environmental threats

Control and the contents from 11.1.4 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

11.1.5 Working in secure areas

Control

Procedures for working in secure areas should be designed and applied.

SMTO implementation guidance

SMTOs should remind security guidance for working in security area to all employees before entering into the security perimeters. The entrance record with signature can be used as a confirmation. Additional guidance for working in security area should be considered to manage every activity to be controlled. Devices such as camera, mobile devices, and external storage devices should have security check to avoid security incident.

11.1.6 Delivery and loading areas

Control

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

SMTO implementation guidance

SMTO should have guidance to avoid unauthorized access to restricted area from delivery and loading area. Security check should be considered to proceed in an isolated area before using in a restricted area so as not be affected from security incident. The result of security check should be updated in the asset record for audit reference.

11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

11.2.1 Equipment siting and protection

Control

Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

SMTO implementation guidance

The telecommunication-specific implementation guidance from [ITU-T X.1051] clause 11.2.1 applies.

11.2.2 Supporting utilities

Control

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

SMTO implementation guidance

In SMTOs, it is preferable to provide an uninterruptible power supply with capacity for all loading, and capable of withstanding primary power supply failures for the duration of likely outages. If that is impossible due to a lack of resources, a mechanism to provide uninterruptible power to critical equipment should be installed. Batteries may need to be augmented with a private electric generator, especially in isolated areas.

11.2.3 Cabling security

Control and the contents from 11.2.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

11.2.4 Equipment maintenance

Control

Equipment should be correctly maintained to ensure its continued availability and integrity.

SMTO implementation guidance

For SMTOs, equipment maintenance may be carried out by outsourcing these services to external firms/institutes with a service contract and signed security agreement.

11.2.5 Removal of assets

Control

Equipment, information or software should not be taken off-site without prior authorization.

SMTO implementation guidance

It is essential for SMTOs to establish the removal procedures, including prior authorization for assets that SMTOs retain. The implementation guidance from [ISO/IEC 27002] clause 11.2.5 should be considered.

11.2.6 Security of equipment and assets off-premises

Control and the contents from 11.2.6 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

11.2.7 Secure disposal or re-use of equipment

Control and the contents from 11.2.7 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

11.2.8 Unattended user equipment

Control and the contents from 11.2.8 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

11.2.9 Clear desk and clear screen policy

Control and the contents from 11.2.9 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

12 Operations security

12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

12.1.1 Documented operating procedures

Control

Operating procedures should be documented and made available to all users who need them.

SMTO implementation guidance

SMTOs that remain small in size should arrange documentation of operation procedures with easy access to users who need them.

12.1.2 Change management

Control

Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

SMTO implementation guidance

A change in management of an SMTO's operation system and application software requires management approval, with a short decision-making and communication process.

12.1.3 Capacity management

Control

The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

SMTO implementation guidance

SMTOs with insufficient funds should plan the minimum (optimal) system structure with the assistance of an external professional.

12.1.4 Separation of development, testing and operational environments

Control

Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

SMTO implementation guidance

SMTOs can outsource telecommunication service testing to external firms/institutes to conduct reliable verification of service when necessary.

12.2 Protection from malware

Objective: To ensure that information and information-processing facilities are protected against malware.

12.2.1 Controls against malware

Control

Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

SMTO implementation guidance

The damages caused by malware directly affect SMTOs' business. Therefore, SMTOs should control malware by applying automated managing tools within their organization, with the support of external professional services. Furthermore, SMTOs should develop specific procedures for security incident responses and distribute them throughout the organization. (See clause 16.)

12.3 Backup

Objective: To protect against loss of data.

12.3.1 Information backup

Control

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

SMTO implementation guidance

SMTOs should establish procedures to backup information stored in organization's assets.

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1 Event logging

Control and the contents from 12.4.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

12.4.2 Protection of log information

Control and the contents from 12.4.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

12.4.3 Administrator and operator logs

Control

System administrator and system operator activities should be logged and the logs protected and regularly reviewed.

SMTO implementation guidance

In the case of SMTOs, typically one person carries out the duties of system administrator and manager at the same time. It is therefore necessary for SMTOs to establish a work monitoring system and implement an activity for raising awareness of information security.

12.4.4 Clock synchronisation

Control and the contents from 12.4.4 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

Control

Procedures should be implemented to control the installation of software on operational systems.

SMTO implementation guidance

The control of operational software is both a technical and specialized activity, and one for which SMTOs need to have staff available with the right expertise and knowledge to carry out the necessary tasks involved. To minimize the risk and impact due to corruption to operational systems, SMTOs should pay particular attention to the implementation guidance from [ISO/IEC 27002] clause 12.5.1 related to the control of changes to operational software:

If applications and operating system software are to be implemented in sensitive systems such as a switching facility, a test should be carried out with a full coverage of path.

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

Control and the contents from 12.6.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

12.6.2 Restrictions on software installation

Control

Rules governing the installation of software by users should be established and implemented.

SMTO implementation guidance

To restrict users' arbitrary software installation, SMTOs should grant the least privilege necessary. If it is difficult to apply the principle of least privilege, SMTOs should establish and document the policy on software installation including disciplinary rules when users violate the policy.

12.7 Information systems audit considerations

Objective: To minimize the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

Control and the contents from 12.7.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

13 Communications security

13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities**.**

13.1.1 Network controls

Control and the contents from 13.1.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

13.1.2 Security of network services

Control

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

SMTO implementation guidance

SMTOs can use a security monitoring service which is provided by external professional institutes when necessary, based on the size of the organization.

13.1.3 Segregation in networks

Control

Groups of information services, users and information systems should be segregated on networks.

SMTO implementation guidance

SMTOs should divide their networks into separate logical network domains using security gateways (e.g., firewalls).

If SMTOs have public web servers or e-mail relay servers, they should be deployed to a public segment such as a demilitarized zone (DMZ) separated from the internal network.

13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

13.2.1 Information transfer policies and procedures

Control

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

SMTO implementation guidance

SMTOs should adopt a safe means of exchanging information, considering security issues.

13.2.2 Agreements on information transfer

Control

Agreements should address the secure transfer of business information between the organization and external parties.

SMTO implementation guidance

SMTOs that collaborate frequently with a large enterprise (parent company) should clearly define the kind of information to be shared, the method and system of sharing information, and specific sharing procedures, etc.

13.2.3 Electronic messaging

Control and the contents from 13.2.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

13.2.4 Confidentiality or non-disclosure agreements

Control and the contents from 13.2.4 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

14.1.1 Information security requirements analysis and specification

Control

The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.

SMTO implementation guidance

If it is difficult for SMTOs to specify the requirements for controls due to limited budgets and human resources, they have the option of using independently evaluated and certified products, such as information technology (IT) products that have been evaluated in accordance with [b-ISO/IEC 15408-1], [b-ISO/IEC 15408-2] and [b-ISO/IEC 15408-3], or other evaluation or certification standards, as appropriate. Another option for SMTOs is to seek the services of external consultancy companies or organizations that specifically provide advice to small medium enterprises (SMEs).

Security requirements are identified by carrying out a risk assessment. [b-ISO/IEC 27005] provides guidance on a risk management processes and [b-ITU-T X.1055] also provides details on risk management profiles.

14.1.2 Securing application services on public networks

Control and the contents from 14.1.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.1.3 Protecting application services transactions

Control

Information involved in application service transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

SMTO implementation guidance

SMTOs should update system security every time a security event arises in order to secure safe on-line transactions (to keep security up to date).

14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Secure development policy

Control and the contents from 14.2.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.2.2 System change control procedures

Control and the contents from 14.2.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.2.3 Technical review of applications after operating platform changes

Control and the contents from 14.2.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.2.4 Restrictions on changes to software packages

Control and the contents from 14.2.4 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.2.5 Secure system engineering principles

Control and the contents from 14.2.5 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.2.6 Secure development policy

Control and the contents from 14.2.6 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.2.7 Outsourced development

Control and the contents from 14.2.7 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.2.8 System security testing

Control and the contents from 14.2.8 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.2.9 System acceptance testing

Control and the contents from 14.2.9 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

14.3 Test data

Objective: To ensure the protection of data used for testing.

14.3.1 Protection of test data

The control objective and the contents from 14.3.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

15 Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Control and the contents from 15.1.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

15.1.2 Addressing security within supplier agreements

Control and the contents from 15.1.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

15.1.3 Information and communication technology supply chain

Control and the contents from 15.1.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Monitoring and review of supplier services

Control

Organizations should regularly monitor, review and audit supplier service delivery.

SMTO implementation guidance

If the SMTO workforce does not have adequate professional knowledge, they should have thorough background knowledge on how to manage service level with a third party.

15.2.2 Managing changes to supplier services

Control and the contents from 15.2.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

16 Information security incident management

16.1 Management of information security incidents

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 Responsibilities and procedures

Control

Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

SMTO implementation guidance

SMTOs can have agreements for handling information security incidents with external service providers.

Other information for SMTO

There are various kinds of security incident response services in the market, which can help SMTOs fulfil their responsibilities.

To be prepared in case of a security incident, SMTOs should be aware of which kind of services are available and which company provides appropriate and affordable services to meet their needs.

16.1.2 Reporting information security events

Control

Information security events should be reported through appropriate management channels as quickly as possible.

SMTO implementation guidance

Depending on the impact of information security events, relationships between the response team and external parties (e.g., Computer Incident Response Team (CIRT), law enforcement organizations, other emergency authorities, customers, and business partners) should be established. If necessary, SMTOs should promptly report the incidents to the related customers through direct e-mails and/or home-page**.**

16.1.3 Reporting information security weaknesses

Control and the contents from 16.1.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

16.1.4 Assessment of and decision on information security events

Control and the contents from 16.1.4 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

16.1.5 Response to information security incidents

Control

Information security incidents should be responded to in accordance with the documented procedures.

SMTO implementation guidance

SMTOs should consider the handling of issues related to telecommunication services or their customers as high priority. For example, customer-initiated issues can be prioritized according to the criteria provided:

a) customer site is completely down or is failing to meet SLA requirements;

b) customer service degraded;

c) customer requests.

16.1.6 Learning from information security incidents

Control and the contents from 16.1.6 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

16.1.7 Collection of evidence

Control and the contents from 16.1.7 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

17 Information security aspects of business continuity management

17.1 Information security continuity

Objective: Information security continuity should be embedded in the organization's business continuity management systems.

17.1.1 Planning information security continuity

Control and the contents from 17.1.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

17.1.2 Implementing information security continuity

Control

The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

SMTO implementation guidance

The planning process should focus on the required business objectives. SMTOs should consider the inclusion of an emergency rehabilitation plan for telecommunication services and ensuring essential communications of telecommunication service customers according to the customer SLA.

17.1.3 Verify, review and evaluate information security continuity

Control and the contents from 17.1.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

17.2 Redundancies

Objective: To ensure availability of information processing facilities.

17.2.1 Availability of information processing facilities

Control and the contents from 17.2.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

18 Compliance

18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

Control and the contents from 18.1.1 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

18.1.2 Intellectual property rights

Control and the contents from 18.1.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

18.1.3 Protection of records

Control and the contents from 18.1.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

18.1.4 Privacy and protection of personally identifiable information

Control and the contents from 18.1.4 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

18.1.5 Regulation of cryptographic controls

Control and the contents from 18.1.5 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with organizational policies and procedures.

18.2.1 Independent review of information security

Control

The organization's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.

SMTO implementation guidance

It is recommended for SMTOs to utilize external professional institutes or automated auditing tools for information security.

18.2.2 Compliance with security policies and standards

Control and the contents from 18.2.2 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

18.2.3 Technical compliance review

Control and the contents from 18.2.3 of [ISO/IEC 27002] and [ITU-T X.1051] apply.

Annex A

Telecommunication extended control set

(This annex forms an integral part of this Recommendation.)

TEL.9 Access control

TEL.9.5 Network access control

Objective: To prevent unauthorized access to networked services.

TEL.9.5.1 Telecommunication carrier identification and authentication by users

Control and the contents from TEL.9.5.1 of [ITU-T X.1051] apply.

TEL.11 Physical and environmental security

TEL.11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to an organization's information and information processing facilities.

TEL.11.1.7 Securing communication centres

Control and the contents from TEL.11.1.7 of [ITU-T X.1051] apply.

TEL.11.1.8 Securing telecommunication equipment room

Control and the contents from TEL.11.1.8 of [ITU-T X.1051] apply.

TEL.11.1.9 Securing physically isolated operation areas

Control and the contents from TEL.11.1.9 of [ITU-T X.1051] apply.

TEL.11.3 Security under the control of other party

Objective: To protect equipment located outside telecommunication organizations' premises (e.g., co-locations) against physical and environmental threats.

TEL.11.3.1 Equipment sited in other carriers' premises

Control and the contents from TEL.11.3.1 [ITU-T X.1051] apply.

TEL.11.3.2 Equipment sited in user premises

Control and the contents from TEL.11.3.2 [ITU-T X.1051] apply.

TEL.11.3.3 Interconnected telecommunication services

Control and the contents from TEL.11.3.3 [ITU-T X.1051] apply.

TEL.13 Communications security

TEL.13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

TEL.13.1.4 Security management of telecommunication service delivery

Control and the contents from TEL.13.1.4 [ITU-T X.1051] apply.

TEL.13.1.5 Response to spam

Control and the contents from TEL.13.1.5 [ITU-T X.1051] apply.

TEL.13.1.6 Response to DoS/DDoS attacks

Control and the contents from TEL.13.1.6 [ITU-T X.1051] apply.

TEL.18 Compliance

TEL.18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

TEL.18.1.6 Non-disclosure of communications

Control and the contents from TEL.18.1.6 [ITU-T X.1051] apply.

TEL.18.1.7 Essential communications

Control

Telecommunication organizations should, when a natural disaster, accident or any other emergency occurs, or at a risk of occurrence thereof, give priority to essential communications whose contents are necessary for the prevention of or relief or recovery from such incidents and for the maintenance of public order.

SMTO implementation guidance

SMTOs should prepare a list of public authorities needed to give priority to communication in accordance with the legislation or the regulations of the country or region where the business is registered.

TEL.18.1.8 Legality of emergency actions

Control and the contents from TEL.18.1.8 [ITU-T X.1051] apply.

Bibliography

[b-ITU-T X.1055] Recommendation ITU-T X.1055 (2008), *Risk management and risk profile guidelines for telecommunications organizations.*

[b-ITU-T X.1057] Recommendation ITU-T X.1057 (2011), *Asset management guidelines in telecommunication organizations.*

[b-ISO/IEC 15408-1] ISO/IEC 15408-1:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.

[b-ISO/IEC 15408-2] ISO/IEC 15408-2:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components*.

[b-ISO/IEC 15408-3] ISO/IEC 15408-3:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements.*

[b-ISO/IEC 27005] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018