

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 32

(03/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

ITU-T X.1058 – Code of practice for personally identifiable information protection for telecommunications organizations

ITU-T X-series Recommendations – Supplement 32



International
Telecommunication
Union

Documents
Document Sharing Hub

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 ledger 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.

Supplement 32 to ITU-T X-series Recommendations

ITU-T X.1058 – Code of practice for personally identifiable information protection for telecommunications organizations

Summary

Supplement 32 to X-series Recommendations aims to complement the information provided in ITU-T X.1058 by providing additional implementation guidance for personally identifiable information (PII) protection, which are not described in ITU-T X.1058, but should further be applicable to telecommunications organizations to address PII protection.

The number of telecommunications organizations processing PII is on the rise. Accordingly, expectations for the protection of PII are also increasing.

The protection of PII is driving the need for a set of additional controls and implementation guidance for PII protection, which are applicable to telecommunications organizations. The guidance presented in this Supplement are additions to those described in ITU-T X.1058.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 32	2018-03-29	17	11.1002/1000/13593

Keywords

Controls, implementation guidance, personally identifiable information, telecommunications organizations.

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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/>.

© ITU 2018

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Terms and Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Supplement	2
	3.3 Abbreviations and acronyms	2
4	Overview.....	2
	4.1 Introduction	2
	4.2 Objective of this Supplement	3
	4.3 Structure and intent of this Supplement	3
5	Information security policies	3
	5.1 Management directions for information security	3
6	Organization of information security.....	3
	6.1 Internal organization.....	3
	6.2 Mobile devices and teleworking.....	4
7	Human resource security	4
	7.1 Prior to employment	4
	7.2 During employment.....	5
	7.3 Termination and change of employment	5
8	Asset management	5
	8.1 Responsibility for assets	5
	8.2 Information classification.....	6
	8.3 Media handling.....	6
9	Access control.....	6
	9.1 Business requirement of access control.....	6
	9.2 User access management	6
	9.3 User responsibilities	7
	9.4 System and application access control	7
10	Cryptography	7
	10.1 Cryptographic controls	7
11	Physical and environmental security	8
	11.1 Secure areas	8
	11.2 Equipment.....	8
12	Operations security	9
	12.1 Operational procedures and responsibilities.....	9
	12.2 Protection from malware	9
	12.3 Backup	9



Documents

Document Sharing Hub

X series – Supplement 32 (03/2018)

iii

	Page
12.4 Logging and monitoring	9
12.5 Control of operational software	10
12.6 Technical vulnerability management	10
12.7 Information systems audit considerations	10
13 Communications security	10
13.1 Network security management	10
13.2 Information transfer	10
14 System acquisition, development and maintenance	11
14.1 Security requirements of information systems	11
14.2 Security in development and support processes	11
14.3 Test data.....	11
15 Supplier relationships	11
15.1 Information security in supplier relationships	11
15.2 Supplier service delivery management.....	11
16 Information security incident management	11
16.1 Management of information security incidents and improvements	11
17 Information security aspects of business continuity management	12
17.1 Information security continuity	12
17.2 Redundancies.....	12
18 Compliance	12
18.1 Compliance with legal and contractual requirements	12
18.2 Information security reviews	12
Appendix I – Extended control set for PII protection	13
I.1 General policies for the use and protection of PII.....	13
I.2 Consent and choice	13
I.3 Purpose legitimacy and specification	13
I.4 Collection limitation	13
I.5 Data minimization	13
I.6 Use, retention and disclosure limitation	13
I.7 Accuracy and quality	14
I.8 Openness, transparency and notice.....	14
I.9 PII principal participation and access.....	14
I.10 Accountability	14
I.11 Information security	15
I.12 Privacy compliance	15
Appendix II – Privacy principles in ISO/IEC 29100	16
Bibliography.....	17

Supplement 32 to ITU-T X-series Recommendations

ITU-T X.1058 – Code of practice for personally identifiable information protection for telecommunications organizations

1 Scope

This Supplement provides additional implementation guidance for Personally Identifiable Information (PII) protection, to those described in [ITU-T X.1058], which should further be applicable to telecommunications organizations when addressing PII protection.

When addressing PII protection, it is intended that telecommunications organizations should use the associated implementation guidance described in this Supplement as well as those described in [ITU-T X.1058].

This Supplement is applicable to telecommunications organizations which collect, use, and transfer PII as part of their information processing.

2 References

[ITU-T X.1058] Recommendation ITU-T X.1058 (2017) | ISO/IEC 29151:2017, *Information technology – Security techniques – Code of practice for personally identifiable information protection*.

3 Terms and Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 cloud service customer [b-ISO/IEC 19944]: Party which is in a business relationship for the purpose of using cloud services.

3.1.2 cloud service provider [b-ISO/IEC 19944]: Party which makes cloud services available.

3.1.3 control [b-ISO/IEC 27000]: Measure that is modifying risk.

NOTE 1 – Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 – Controls may not always exert the intended or assumed modifying effect.

3.1.4 de-identification process [ITU-T X.1058]: Process of removing the association between a set of identifying data and the data principal, using de-identification techniques.

3.1.5 management [b-ISO 9000]: Coordinated activities to direct and control an organization.

3.1.6 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.

NOTE – To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

3.1.7 PII controller [b-ISO/IEC 29100]: Privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes.

NOTE – A PII controller sometimes instructs others (e.g., PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

3.1.8 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".

3.1.9 PII processor [b-ISO/IEC 29100]: Privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller.

3.1.10 policy [b-ISO/IEC 27000]: Intentions and direction of an organization, as formally expressed by its top management.

3.1.11 privacy principles [b-ISO/IEC 29100]: Set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems.

3.1.12 processing of PII [b-ISO/IEC 29100]: Operation or set of operations performed upon personally identifiable information (PII).

NOTE – Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, de-identification, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

3.1.13 sensitive PII [b-ISO/IEC 29100]: Category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal.

NOTE – In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that might be defined as sensitive.

3.1.14 telecommunications organizations [b-ITU-T X.1051]: Business entities who provide telecommunications services in order to meet the demand of others.

3.1.15 telecommunications service customer [b-ITU-T X.1051]: Person or organization who enters into a contract with telecommunications organizations to be offered telecommunications services by them.

3.1.16 telecommunications services [b-ITU-T X.1051]: Communications using telecommunications facilities, or any other means of providing communications either between telecommunications service users or telecommunications service customers.

3.2 Terms defined in this Supplement

This Supplement defines the following term:

3.2.1 PII protection policy: Overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting.

3.3 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

PII Personally Identifiable Information

4 Overview

4.1 Introduction

This Supplement is structured in a format similar to [ITU-T X.1058]. In cases where objectives and controls specified in [ITU-T X.1058] are applicable without the need for additional information,