DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27552

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2018-12-26

Voting terminates on:
2019-03-20

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27552:2018(E)

© ISO/IEC 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword vii

0 Introduction viii
0.1 General viii
0.2 Compatibility with other management system standards viii

1 Scope 1

2 Normative references 1

3 Terms, definitions and abbreviations 1
3.1 Terms and definitions 1
3.2 Abbreviations 2
3.3 Alternative terms 2

4 General 2
4.1 Structure of this document 2
4.2 Application of ISO/IEC 27001:2013 requirements 3
4.3 Application of ISO/IEC 27002:2013 guidelines 3
4.4 Customer 4

5 PIMS-specific requirements related to ISO/IEC 27001 5
5.1 General 5
5.2 Context of the organization 5
5.2.1 Understanding the organization and its context 5
5.2.2 Understanding the needs and expectations of interested parties 5
5.2.3 Determining the scope of the information security management system 5
5.2.4 Information security management system 6
5.3 Leadership 6
5.3.1 Leadership and commitment 6
5.3.2 Policy 6
5.3.3 Organizational roles, responsibilities and authorities 6
5.4 Planning 6
5.4.1 Actions to address risks and opportunities 6
5.4.2 Information security objectives and planning to achieve them 7
5.5 Support 7
5.5.1 Resources 7
5.5.2 Competence 7
5.5.3 Awareness 7
5.5.4 Communication 8
5.5.5 Documented information 8
5.6 Operation 8
5.6.1 Operational planning and control 8
5.6.2 Information security risk assessment 8
5.6.3 Information security risk treatment 8
5.7 Performance evaluation 8
5.7.1 Monitoring, measurement, analysis and evaluation 8
5.7.2 Internal audit 8
5.7.3 Management review 8
5.8 Improvement 9
5.8.1 Nonconformity and corrective action 9
5.8.2 Continual improvement 9

6 PIMS-specific guidance related to ISO/IEC 27002 9
6.1 General 9
6.2 Information security policies 9

© ISO/IEC 2018 – All rights reserved

6.2.1 Management direction for information security 9
6.3 Organization of information security 10
6.3.1 Internal organization 10
6.3.2 Mobile devices and teleworking 10
6.4 Human resource security 11
6.4.1 Prior to employment 11
6.4.2 During employment 11
6.4.3 Termination and change of employment 11
6.5 Asset management 12
6.5.1 Responsibility for assets 12
6.5.2 Information classification 12
6.5.3 Media handling 12
6.6 Access control 13
6.6.1 Business requirements of access control 13
6.6.2 User access management 14
6.6.3 User responsibilities 15
6.6.4 System and application access control 15
6.7 Cryptography 15
6.7.1 Cryptographic controls 15
6.8 Physical and environmental security 16
6.8.1 Secure areas 16
6.8.2 Equipment 16
6.9 Operations security 17
6.9.1 Operational procedures and responsibilities 17
6.9.2 Protection from malware 18
6.9.3 Backup 18
6.9.4 Logging and monitoring 19
6.9.5 Control of operational software 20
6.9.6 Technical vulnerability management 20
6.9.7 Information systems audit considerations 20
6.10 Communications security 20
6.10.1 Network security management 20
6.10.2 Information transfer 20
6.11 Systems acquisition, development and maintenance 21
6.11.1 Security requirements of information systems 21
6.11.2 Security in development and support processes 21
6.11.3 Test data 23
6.12 Supplier relationships 23
6.12.1 Information security in supplier relationships 23
6.12.2 Supplier service delivery management 24
6.13 Information security incident management 24
6.13.1 Management of information security incidents and improvements 24
6.14 Information security aspects of business continuity management 26
6.14.1 Information security continuity 26
6.14.2 Redundancies 26
6.15 Compliance 26
6.15.1 Compliance with legal and contractual requirements 26
6.15.2 Information security reviews 27

7 Additional ISO/IEC 27002 guidance for PII controllers 28
7.1 General 28
7.2 Conditions for collection and processing 28
7.2.1 Identify and document purpose 28
7.2.2 Identify lawful basis 28
7.2.3 Determine when and how consent is to be obtained 29
7.2.4 Obtain and record consent 29
7.2.5 Privacy impact assessment 30
7.2.6 Contracts with PII processors 30
7.2.7 Joint PII controller 31
7.2.8 Records related to processing PII 31

 © ISO/IEC 2018 – All rights reserved

7.3 Obligations to PII principals 32
7.3.1 Determining and fulfilling obligations to PII principals 32
7.3.2 Determining information for PII principals 32
7.3.3 Providing information to PII principals 33
7.3.4 Provide mechanism to modify or withdraw consent 33
7.3.5 Provide mechanism to object to PII processing 34
7.3.6 Access, correction and/or erasure 34
7.3.7 PII controllers' obligations to inform third parties 34
7.3.8 Providing copy of PII processed 35
7.3.9 Handling requests 35
7.3.10 Automated decision making 36
7.4 Privacy by design and privacy by default 36
7.4.1 Limit collection 36
7.4.2 Limit processing 36
7.4.3 Accuracy and quality 37
7.4.4 PII minimization and de-identification objectives 37
7.4.5 PII de-identification and deletion at the end of processing 38
7.4.6 Temporary files 38
7.4.7 Retention 38
7.4.8 Disposal 38
7.4.9 PII transmission controls 39
7.5 PII sharing, transfer, and disclosure 39
7.5.1 Identify basis for PII transfer between jurisdictions 39
7.5.2 Countries and international organizations to which PII might be transferred 39
7.5.3 Records of transfer of PII 40
7.5.4 Records of PII disclosure to third parties 40

8 Additional ISO/IEC 27002 guidance for PII processors 40
8.1 General 40
8.2 Conditions for collection and processing 40
8.2.1 Cooperation agreement 40
8.2.2 Organization's purposes 41
8.2.3 Marketing and advertising use 41
8.2.4 Infringing instruction 42
8.2.5 Customer obligations 42
8.2.6 Records related to processing PII 42
8.3 Obligations to PII principals 42
8.3.1 Obligations to PII principals 42
8.4 Privacy by design and privacy by default 43
8.4.1 Temporary files 43
8.4.2 Return, transfer or disposal of PII 43
8.4.3 PII transmission controls 44
8.5 PII sharing, transfer, and disclosure 44
8.5.1 Basis for PII transfer between jurisdictions 44
8.5.2 Countries and international organizations to which PII might be transferred 45
8.5.3 Records of PII disclosure to third parties 45
8.5.4 Notification of PII disclosure requests 45
8.5.5 Legally binding PII disclosures 45
8.5.6 Disclosure of subcontractors used to process PII 46
8.5.7 Engagement of a subcontractor to process PII 46
8.5.8 Change of subcontractor to process PII 47

Annex A (normative) **PIMS specific reference control objectives and controls (PII Controllers) 48**

Annex B (normative) **PIMS specific reference control objectives and controls (PII Processors) 53**

Annex C (informative) **Mapping to the General Data Protection Regulation 56**
C.1 Mapping ISO/IEC 27552 structure to GDPR articles 56

Annex D (informative) **Mapping to ISO/IEC 29100 ..... 60**
D.1 Mapping for PII controllers 60
D.2 Mapping for PII processors 61

© ISO/IEC 2018 – All rights reserved

Annex E (informative) **Mapping to ISO/IEC 27018 and ISO/IEC 29151** **63**

Annex F (informative) **Terms and alternative terms** **66**

Annex G (informative) **How to apply ISO/IEC 27552 to ISO/IEC 27001 and ISO/IEC 27002** **67**

G.1 How to apply this standard **67**

G.2 Example of refinement of security standards **68**

Bibliography **71**

 © ISO/IEC 2018 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27552 was prepared by Technical Committee ISO/TC JTC1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

© ISO/IEC 2018 – All rights reserved

0 Introduction

0.1 General

Almost every organization processes Personally Identifiable Information (PII). Further, the quantity and types of PII processed is increasing, as is the number of situations where an organization needs to cooperate with other organizations regarding the processing of PII. Protection of privacy in the context of the processing of PII is a societal need, as well as the topic of dedicated laws and regulations all over the world.

The Information Security Management System (ISMS) defined in ISO IEC 27001 was designed to permit the addition of sector specific requirements, without the need to develop a new Management System. ISO Management System standards, including those that are sector specific, are designed to be able to be implemented either separately or as a combined Management System.

This document defines additional requirements and provides guidance for the protection of privacy as potentially affected by the processing of PII, enabling the organizations' overall Management System to be extended to cover both the general requirements for information security (an Information Security Management System (ISMS)) and the more specific requirements for PII protection, both together constituting a Privacy Information Management System (PIMS). These additional requirements and guidance are written in such a way that they are practically usable for PII protection by organizations of all sizes and cultural environments.

Requirements and guidance for PII protection vary depending upon the context of the organization, in particular where national laws and regulations are applicable. ISO/IEC 27001 requires that this context be understood and taken into account. This document includes mapping to the privacy framework and principles defined in ISO/IEC 29100; also to ISO/IEC 27018, ISO/IEC 29151 and the EU General Data Protection Regulation. However these might need to be interpreted to take into account local laws and regulations.

This document can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as sub-contractors to PII processors).

An organization complying with the requirements in this document will generate documentary evidence of how it handles the processing of PII. Such evidence can be used to facilitate agreements with business partners where the processing of PII is mutually relevant. This might also assist in relationships with other stakeholders. The use of this document in conjunction with ISO/IEC 27001 can, if desired, provide independent verification of this evidence, although compliance with this document cannot be taken as compliance with laws and regulations.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment amongst its International Standards for Management Systems.

This document enables an organization to align or integrate its PIMS with the requirements of other Management System standards.

© ISO/IEC 2018 – All rights reserved

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

1 Scope

This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

In particular, this document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

Excluding any of the requirements specified in Clause 5 of this document is not acceptable when an organization claims conformity to this document.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2018*, Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013*, Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013*, Information technology — Security techniques — Code of practice for information security controls*

ISO/IEC 29100:2011*, Information technology — Security techniques — Privacy framework*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and ISO/IEC 29100 and the following apply.

3.1.1
joint PII controller
two or more PII controllers that jointly determine the purposes and means of the processing of PII

© ISO/IEC 2018 – All rights reserved

3.1.2
privacy information management system
PIMS
information security management system which addresses the protection of privacy as potentially affected by the processing of PII

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

ISMS Information Security Management System

PII Personally Identifiable Information

PIMS Privacy Information Management System

3.3 Alternative terms

The protection of PII is subject to laws and regulations in many jurisdictions. In some cases, those laws and regulations use terminology which has both similarities and differences to the terminology used in this document.

The mapping between the terminology used in this document and that used in some laws and regulations is shown in Annex F.

4 General

4.1 Structure of this document

This is a sector-specific document related to ISO/IEC 27001:2013 and to ISO/IEC 27002:2013.

This document focuses on PIMS-specific requirements. Compliance with this document is based on adherence to these requirements and with the requirements in ISO/IEC 27001:2013. This document extends the requirements of ISO/IEC 27001:2013 to take into account, in addition to information security, the protection of privacy of PII principals as potentially affected by the processing of PII. For a better understanding, implementation guidance and other information regarding the requirements is included.

PIMS-specific requirements and other information regarding the information security requirements in ISO/IEC 27001 appropriate to an organization acting as either a PII controller or a PII processor are given in Clause 5.

NOTE 1 For completeness, clause 5 of this document contains a sub-clause for each of the clauses containing requirements in ISO/IEC 27001:2013, even in cases where there are no PIMS-specific requirements or other information.

PIMS-specific guidance and other information regarding the information security controls in ISO/IEC 27002 and PIMS-specific guidance for an organization acting as either a PII controller or a PII processor are given in Clause 6.

NOTE 2 For completeness, clause 6 of this document contains a sub-clause for each of the clauses containing objectives or controls in ISO/IEC 27002:2013, even in cases where there is no PIMS-specific guidance or other information.

Additional ISO/IEC 27002 guidance for PII controllers is given in Clause 7, and additional ISO/IEC 27002 guidance for PII processors is given in Clause 8.

The PIMS specific control objectives and controls for an organization acting as a PII controller are listed in Annex A (whether it employs a PII processor or not, and whether acting jointly with another PII controller or not).

© ISO/IEC 2018 – All rights reserved