DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27701

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

Secretariat: **DIN**

Voting begins on:
2023-01-04

Voting terminates on:
2023-03-29

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 27701:2023(E)

Documents
Document Sharing Hub
© ISO/IEC 2023

Full document details: ISO_IEC DIS 27701 _2023

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC DIS 27701 _2023

Contents

Page

Foreword ..... **vii**
Introduction ..... **viii**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviations **1**
4 General **2**
4.1 Structure of this document 2
4.2 Application of ISO/IEC 27001:202x requirements 2
4.3 Application of ISO/IEC 27002:2022 guidelines 3
4.4 Customer 3
5 PIMS-specific requirements related to ISO/IEC 27001 ..... **4**
5.1 General 4
5.2 Context of the organization 4
5.2.1 Understanding the organization and its context 4
5.2.2 Understanding the needs and expectations of interested parties 4
5.2.3 Determining the scope of the information security management system 4
5.2.4 Information security management system 5
5.3 Leadership 5
5.3.1 Leadership and commitment 5
5.3.2 Policy 5
5.3.3 Organizational roles, responsibilities and authorities 5
5.4 Planning 5
5.4.1 Actions to address risks and opportunities 5
5.4.2 Information security objectives and planning to achieve them 6
5.4.3 Planning of changes 6
5.5 Support 6
5.5.1 Resources 6
5.5.2 Competence 6
5.5.3 Awareness 6
5.5.4 Communication 7
5.5.5 Documented information 7
5.6 Operation 7
5.6.1 Operational planning and control 7
5.6.2 Information security risk assessment 7
5.6.3 Information security risk treatment 7
5.7 Performance evaluation 7
5.7.1 Monitoring, measurement, analysis and evaluation 7
5.7.2 Internal audit 7
5.7.3 Management review 7
5.8 Improvement 8
5.8.1 Continual improvement 8
5.8.2 Nonconformity and corrective action 8
6 PIMS-specific guidance related to ISO/IEC 27002 ..... **8**
6.1 General 8
6.2 Organizational controls 8
6.2.1 Policies for information security 8
6.2.2 Internal security roles and responsibilities 8
6.2.3 Segregation of duties 9
6.2.4 Management responsibilities 9
6.2.5 Contact with authorities 9
6.2.6 Contact with special interest groups 9
6.2.7 Threat intelligence 9

AVA Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: ISO_IEC DIS 27701 _2023

6.2.8 Information security in project management 9
6.2.9 Inventory of information and other associated assets 9
6.2.10 Acceptable use of information and other associated assets 9
6.2.11 Return of assets 10
6.2.12 Classification of information 10
6.2.13 Labelling of information 10
6.2.14 Information transfer 10
6.2.15 Access control 10
6.2.16 Identity management 10
6.2.17 Authentication information 11
6.2.18 Access rights 11
6.2.19 Information security in supplier relationships 11
6.2.20 Addressing information security within supplier agreements 11
6.2.21 Managing information security in the ICT supply chain 12
6.2.22 Monitoring, review and change management of supplier services 12
6.2.23 Information security for use of cloud services 12
6.2.24 Information security incident management planning and preparation 12
6.2.25 Assessment and decision on information security events 12
6.2.26 Response to information security incidents 12
6.2.27 Learning from information security incidents 14
6.2.28 Collection of evidence 14
6.2.29 Information security during disruption 14
6.2.30 ICT readiness for business continuity 14
6.2.31 Legal, statutory, regulatory and contractual requirements 14
6.2.32 Intellectual property rights 15
6.2.33 Protection of records 15
6.2.34 Privacy and protection of PII 15
6.2.35 Independent review of information security 15
6.2.36 Compliance with policies, rules and standards for information security 15
6.2.37 Documented operating procedures 16
6.3 People controls 16
6.3.1 Screening 16
6.3.2 Terms and conditions of employment 16
6.3.3 Information security awareness, education and training 16
6.3.4 Disciplinary procedures 16
6.3.5 Responsibilities after termination or change of employment 16
6.3.6 Confidentiality or non-disclosure agreements 16
6.3.7 Remote working 16
6.3.8 Information security event reporting 17
6.4 Physical controls 17
6.4.1 Physical security perimeters 17
6.4.2 Physical entry 17
6.4.3 Securing offices, rooms and facilities 17
6.4.4 Physical security monitoring 17
6.4.5 Protecting against physical and environmental threats 17
6.4.6 Working in secure areas 17
6.4.7 Clear desk and clear screen 17
6.4.8 Equipment siting and protection 17
6.4.9 Security of assets off-premises 17
6.4.10 Storage media 17
6.4.11 Supporting utilities 18
6.4.12 Cabling security 18
6.4.13 Equipment maintenance 18
6.4.14 Secure disposal or re-use of equipment 18
6.5 Technological controls 19
6.5.1 User endpoint devices 19
6.5.2 Privileged access rights 19
6.5.3 Information access restriction 19

AVA Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: ISO_IEC DIS 27701 _2023

6.5.4 Access to source code 19
6.5.5 Secure authentication 19
6.5.6 Capacity management 19
6.5.7 Protection against malware 19
6.5.8 Management of technical vulnerabilities 19
6.5.9 Configuration management 19
6.5.10 Information deletion 19
6.5.11 Data masking 19
6.5.12 Data leakage prevention 20
6.5.13 Information backup 20
6.5.14 Redundancy of information processing facilities 20
6.5.15 Logging 20
6.5.16 Monitoring activities 21
6.5.17 Clock synchronization 21
6.5.18 Use of privileged utility programs 21
6.5.19 Installation of software on operational systems 21
6.5.20 Networks security 21
6.5.21 Security of network services 21
6.5.22 Segregation of networks 22
6.5.23 Web filtering 22
6.5.24 Use of cryptography 22
6.5.25 Secure development life cycle 22
6.5.26 Application security requirements 22
6.5.27 Secure system architecture and engineering principles 23
6.5.28 Secure coding 23
6.5.29 Security testing in development and acceptance 23
6.5.30 Outsourced development 23
6.5.31 Separation of development, testing and production environments 23
6.5.32 Change management 23
6.5.33 Test information 24
6.5.34 Protection of information systems during audit testing 24

7 Additional ISO/IEC 27002 guidance for PII controllers 24
7.1 General 24
7.2 Conditions for collection and processing 24
7.2.1 Identify and document purpose 24
7.2.2 Identify lawful basis 24
7.2.3 Determine when and how consent is to be obtained 25
7.2.4 Obtain and record consent 25
7.2.5 Privacy impact assessment 26
7.2.6 Contracts with PII processors 26
7.2.7 Joint PII controller 27
7.2.8 Records related to processing PII 27
7.3 Obligations to PII principals 28
7.3.1 Determining and fulfilling obligations to PII principals 28
7.3.2 Determining information for PII principals 28
7.3.3 Providing information to PII principals 29
7.3.4 Providing mechanism to modify or withdraw consent 29
7.3.5 Providing mechanism to object to PII processing 30
7.3.6 Access, correction or erasure 30
7.3.7 PII controllers' obligations to inform third parties 30
7.3.8 Providing copy of PII processed 31
7.3.9 Handling requests 31
7.3.10 Automated decision making 32
7.4 Privacy by design and privacy by default 32
7.4.1 Limit collection 32
7.4.2 Limit processing 32
7.4.3 Accuracy and quality 33
7.4.4 PII minimization objectives 33

AVA Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: ISO_IEC DIS 27701 _2023

7.4.5 PII de-identification and deletion at the end of processing ... 34
7.4.6 Temporary files ... 34
7.4.7 Retention ... 34
7.4.8 Disposal ... 35
7.4.9 PII transmission controls ... 35
7.5 PII sharing, transfer and disclosure ... 35
7.5.1 Identify basis for PII transfer between jurisdictions ... 35
7.5.2 Countries and international organizations to which PII can be transferred ... 35
7.5.3 Records of transfer of PII ... 36
7.5.4 Records of PII disclosure to third parties ... 36

8 Additional ISO/IEC 27002 guidance for PII processors ... 36
8.1 General ... 36
8.2 Conditions for collection and processing ... 36
8.2.1 Customer agreement ... 37
8.2.2 Organization's purposes ... 37
8.2.3 Marketing and advertising use ... 37
8.2.4 Infringing instruction ... 38
8.2.5 Customer obligations ... 38
8.2.6 Records related to processing PII ... 38
8.3 Obligations to PII principals ... 38
8.3.1 Obligations to PII principals ... 39
8.4 Privacy by design and privacy by default ... 39
8.4.1 Temporary files ... 39
8.4.2 Return, transfer or disposal of PII ... 39
8.4.3 PII transmission controls ... 40
8.5 PII sharing, transfer and disclosure ... 40
8.5.1 Basis for PII transfer between jurisdictions ... 40
8.5.2 Countries and international organizations to which PII can be transferred ... 41
8.5.3 Records of PII disclosure to third parties ... 41
8.5.4 Notification of PII disclosure requests ... 41
8.5.5 Legally binding PII disclosures ... 41
8.5.6 Disclosure of subcontractors used to process PII ... 42
8.5.7 Engagement of a subcontractor to process PII ... 42
8.5.8 Change of subcontractor to process PII ... 43

Annex A (normative) **PIMS-specific reference control objectives and controls (PII Controllers) ... 44**

Annex B (normative) **PIMS-specific reference control objectives and controls (PII Processors) ... 48**

Annex C (informative) **Mapping to ISO/IEC 29100 ... 51**

Annex D (informative) **Mapping to the General Data Protection Regulation ... 54**

Annex E (informative) **Mapping to ISO/IEC 27018 and ISO/IEC 29151 ... 57**

Annex F (informative) **How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002 ... 59**

Annex G (informative) **Correspondence with ISO/IEC 27701:2019 ... 61**

Bibliography ... 67

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27701:2019), which has been editorially revised. This second edition references the structure and content of ISO/IEC 27001:202x and ISO/IEC 27002:2022. Clause 5 has been editorially revised to match the structure of ISO/IEC 27001:202x. Clause 6 and Annexes D and E have been editorially revised to match the structure and content of ISO/IEC 27002:2022. Internal cross-references have been revised as necessary. The complete correspondence with the first edition can be found in Annex G.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

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 legislation or regulation all over the world.

The information security management system (ISMS) defined in ISO/IEC 27001 is designed to permit the addition of sector specific requirements, without the need to develop a new management system. ISO management system standards, including the sector specific ones, are designed to be able to be implemented either separately or as a combined management system.

Requirements and guidance for PII protection vary depending on the context of the organization, in particular where national legislation or regulation exists. 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;

— ISO/IEC 27018;

— ISO/IEC 29151; and

— the EU General Data Protection Regulation.

However, these can be interpreted to take into account local legislation or regulation.

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 subcontractors 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 can 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.

This document was initially developed as ISO/IEC 27552.

0.2 Compatibility with other management system standards

This document applies the framework developed by ISO to improve alignment among its management system standards.

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

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

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.

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 or PII processors processing PII within an ISMS.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:202x, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

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

3 Terms, definitions and abbreviations

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
joint PII controller
PII controller that determine the purposes and means of the processing of PII jointly with one or more other PII controllers

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

3.2
privacy information management system
PIMS
information security management system which addresses the protection of privacy as potentially affected by the processing of PII

4 General

4.1 Structure of this document

This is a sector-specific document related to ISO/IEC 27001:202x and to ISO/IEC 27002:2022.

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 27001:202x. This document extends the requirements of ISO/IEC 27001:202x to take into account the protection of privacy of PII principals as potentially affected by the processing of PII, in addition to information security. For a better understanding, implementation guidance and other information regarding the requirements is included.

Clause 5 gives 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.

NOTE 1 For completeness, Clause 5 contains a subclause for each of the clauses containing requirements in ISO/IEC 27001:202x, even in cases where there are no PIMS-specific requirements or other information.

Clause 6 gives 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.

NOTE 2 For completeness, Clause 6 contains a subclause for each of the clauses containing controls in ISO/IEC 27002:2022, even in cases where there is no PIMS-specific guidance or other information.

Clause 7 gives additional ISO/IEC 27002 guidance for PII controllers, and Clause 8 gives additional ISO/IEC 27002 guidance for PII processors.

Annex A lists the PIMS-specific controls for an organization acting as a PII controller (whether it employs a PII processor or not, and whether acting jointly with another PII controller or not).

Annex B lists the PIMS-specific controls for an organization acting as a PII processor (whether it subcontracts the processing of PII to a separate PII processor or not, and including those processing PII as subcontractor to PII processors).

Annex C contains a mapping to ISO/IEC 29100.

Annex D contains a mapping of the controls in this document to the European Union General Data Protection Regulation.

Annex E contains a mapping to ISO/IEC 27018 and ISO/IEC 29151.

Annex F explains how ISO IEC 27001 and ISO/IEC 27002 are extended to the protection of privacy when processing PII.

Annex G shows the correspondence between the controls in this edition of ISO/IEC 27701 and the previous 2019 edition.

4.2 Application of ISO/IEC 27001:202x requirements

Table 1 gives the location of PIMS-specific requirements in this document in relation to ISO/IEC 27001.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:202x

Clause in ISO/IEC 27001:202x	Title	Subclause in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

NOTE The extended interpretation of "information security" according to 5.1 always applies even when there are no PIMS-specific requirements.

4.3 Application of ISO/IEC 27002:2022 guidelines

Table 2 gives the location of PIMS-specific guidance in this document in relation to ISO/IEC 27002.

Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2022

Clause in ISO/IEC 27002:2022	Title	Subclause in this document	Remarks
5	Organizational controls	6.2	Additional guidance
6	People controls	6.3	Additional guidance
7	Physical controls	6.4	Additional guidance
8	Technological controls	6.5	Additional guidance

NOTE The extended interpretation of "information security" according to 6.1 always applies even when there is no PIMS-specific guidance.

4.4 Customer

Depending on the role of the organization (see 5.2.1), "customer" can be understood as either:

a) an organization who has a contract with a PII controller (e.g. the customer of the PII controller);

NOTE 1 This can be the case of an organization which is a joint PII controller.

NOTE 2 An individual person in a business to consumer relationship with an organization is referred to as a "PII principal" in this document.

b) a PII controller who has a contract with a PII processor (e.g. the customer of the PII processor); or

c) a PII processor who has a contract with a subcontractor for PII processing (e.g. the customer of the subcontracted PII processor).

NOTE 3 Where "customer" is referred to in Clause 6, the related provisions can be applicable in contexts a), b), or c).

NOTE 4 Where "customer" is referred to in Clause 7 and Annex A, the relation provisions are applicable in context a).

NOTE 5 Where "customer" is referred to in Clause 8 and Annex B, the relation provisions can be applicable in contexts b) or c).

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

5 PIMS-specific requirements related to ISO/IEC 27001

5.1 General

The requirements of ISO/IEC 27001:202x mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of PII.

NOTE In practice, where "information security" is used in ISO/IEC 27001:202x, "information security and privacy" applies instead (see Annex F).

5.2 Context of the organization

5.2.1 Understanding the organization and its context

A requirement additional to ISO/IEC 27001:202x, 4.1 is:

The organization shall determine its role as a PII controller (including as a joint PII controller) or a PII processor.

The organization shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include:

— applicable privacy legislation;

— applicable regulations;

— applicable judicial decisions;

— applicable organizational context, governance, policies and procedures;

— applicable administrative decisions;

— applicable contractual requirements.

Where the organization acts in both roles (i.e. a PII controller and a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.

NOTE The role of the organization can be different for each instance of the processing of PII, since it depends on who determines the purposes and means of the processing.

5.2.2 Understanding the needs and expectations of interested parties

A requirement additional to ISO/IEC 27001:202x, 4.2 is:

The organization shall include among its interested parties those parties having interests or responsibilities associated with the processing of PII, including the PII principals.

NOTE 1 Other interested parties can include customers (see 4.4), supervisory authorities, other PII controllers, PII processors and their subcontractors.

NOTE 2 Requirements relevant to the processing of PII can be determined by legal and regulatory requirements, by contractual obligations and by self-imposed organizational objectives. The privacy principles set out in ISO/IEC 29100 provide guidance concerning the processing of PII.

NOTE 3 As an element to demonstrate compliance to the organization's obligations, some interested parties can expect that the organization is in conformity with specific standards, such as the management system specified in this document, or any relevant set of specifications. These parties can call for independently audited compliance to these standards.

5.2.3 Determining the scope of the information security management system

A requirement additional to ISO/IEC 27001:202x, 4.3 is:

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

When determining the scope of the PIMS, the organization shall include the processing of PII.

NOTE The determination of the scope of the PIMS can require revising the scope of the information security management system, because of the extended interpretation of "information security" according to 5.1.

5.2.4 Information security management system

A requirement additional to ISO/IEC 27001:202x, 4.4 is:

The organization shall establish, implement, maintain and continually improve a PIMS in accordance with the requirements of ISO/IEC 27001:202x Clauses 4 to 10, extended by the requirements in Clause 5.

5.3 Leadership

5.3.1 Leadership and commitment

The requirements stated in ISO/IEC 27001:202x, 5.1 along with the interpretation specified in 5.1, apply.

5.3.2 Policy

The requirements stated in ISO/IEC 27001:202x, 5.2 along with the interpretation specified in 5.1, apply.

5.3.3 Organizational roles, responsibilities and authorities

The requirements stated in ISO/IEC 27001:202x, 5.3 along with the interpretation specified in 5.1, apply.

5.4 Planning

5.4.1 Actions to address risks and opportunities

5.4.1.1 General

The requirements stated in ISO/IEC 27001:202x, 6.1.1 along with the interpretation specified in 5.1, apply.

5.4.1.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:202x, 6.1.2 apply with the following refinements:

ISO/IEC 27001:202x, 6.1.2 c) 1) is refined as follows:

The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.

The organization shall apply a privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.

The organization shall ensure throughout the information security and privacy risk assessment processes that the relationship between information security and PII protection is appropriately managed.

NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII.

ISO/IEC 27001:202x, 6.1.2 d) 1) is refined as follows:

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

The organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified in ISO/IEC 27001:202x, 6.1.2 c) as refined above, were to materialize.

5.4.1.3 Information security risk treatment

The requirements stated in ISO/IEC 27001:202x, 6.1.3 apply with the following additions:

ISO/IEC 27001:202x, 6.1.3 c) is refined as follows:

The controls determined in ISO/IEC 27001:202x 6.1.3 b) shall be compared with the controls in Annex A or Annex B and ISO/IEC 27001:202x, Annex A to verify that no necessary controls have been omitted.

When assessing the applicability of controls from ISO/IEC 27001:202x Annex A for the treatment of risks, the controls shall be considered in the context of both risks to information security as well as risks related to the processing of PII, including risks to PII principals.

ISO/IEC 27001:202x, 6.1.3 d) is refined as follows:

Produce a Statement of Applicability that contains:

— the necessary controls [see ISO/IEC 27001:202x, 6.1.3 b) and c)];

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— the justification for excluding any of the controls in Annex A or Annex B and ISO/IEC 27001:202x, Annex A according to the organization's determination of its role (see 5.2.1).

Not all the controls listed in the annexes need to be included in a PIMS implementation. Justification for exclusion can include where the controls are not deemed necessary by the risk assessment, and where they are not required by (or are subject to exceptions under) the legislation or regulation including those applicable to the PII principal.

5.4.2 Information security objectives and planning to achieve them

The requirements stated in ISO/IEC 27001:202x, 6.2 along with the interpretation specified in 5.1, apply.

5.4.3 Planning of changes

The requirements stated in ISO/IEC 27001:202x, 6.3 along with the interpretation specified in 5.1, apply.

5.5 Support

5.5.1 Resources

The requirements stated in ISO/IEC 27001:202x, 7.1 along with the interpretation specified in 5.1, apply.

5.5.2 Competence

The requirements stated in ISO/IEC 27001:202x, 7.2 along with the interpretation specified in 5.1, apply.

5.5.3 Awareness

The requirements stated in ISO/IEC 27001:202x, 7.3 along with the interpretation specified in 5.1, apply.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

5.5.4 Communication

The requirements stated in ISO/IEC 27001:202x, 7.4 along with the interpretation specified in 5.1, apply.

5.5.5 Documented information

5.5.5.1 General

The requirements stated in ISO/IEC 27001:202x, 7.5.1 along with the interpretation specified in 5.1, apply.

5.5.5.2 Creating and updating

The requirements stated in ISO/IEC 27001:202x, 7.5.2 along with the interpretation specified in 5.1, apply.

5.5.5.3 Control of documented information

The requirements stated in ISO/IEC 27001:202x, 7.5.3 along with the interpretation specified in 5.1, apply.

5.6 Operation

5.6.1 Operational planning and control

The requirements stated in ISO/IEC 27001:202x, 8.1 along with the interpretation specified in 5.1, apply.

5.6.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:202x, 8.2 along with the interpretation specified in 5.1, apply.

5.6.3 Information security risk treatment

The requirements stated in ISO/IEC 27001:202x, 8.3 along with the interpretation specified in 5.1, apply.

5.7 Performance evaluation

5.7.1 Monitoring, measurement, analysis and evaluation

The requirements stated in ISO/IEC 27001:202x, 9.1 along with the interpretation specified in 5.1, apply.

5.7.2 Internal audit

The requirements stated in ISO/IEC 27001:202x, 9.2 along with the interpretation specified in 5.1, apply.

5.7.3 Management review

The requirements stated in ISO/IEC 27001:202x, 9.3 along with the interpretation specified in 5.1, apply.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

5.8 Improvement

5.8.1 Continual improvement

The requirements stated in ISO/IEC 27001:202x, 10.1 along with the interpretation specified in 5.1, apply.

5.8.2 Nonconformity and corrective action

The requirements stated in ISO/IEC 27001:202x, 10.2 along with the interpretation specified in 5.1, apply.

6 PIMS-specific guidance related to ISO/IEC 27002

6.1 General

The guidelines in ISO/IEC 27002:2022 mentioning "information security" should be extended to the protection of privacy as potentially affected by the processing of PII.

NOTE 1 In practice, where "information security" is used in ISO/IEC 27002:2022, "information security and privacy" applies instead (see Annex F).

All controls should be considered in the context of both risks to information security as well as risks to privacy related to the processing of PII.

NOTE 2 Unless otherwise stated by specific provisions in Clause 6, or determined by the organization according to applicable jurisdictions, the same guidance applies for PII controllers and PII processors.

6.2 Organizational controls

6.2.1 Policies for information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.1 and the following additional guidance applies:

Additional implementation guidance for 5.1, Policies for information security, of ISO/IEC 27002:2022 is:

Either by the development of separate privacy policies, or by the augmentation of information security policies, the organization should produce a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation or regulation and with the contractual terms agreed between the organization and its partners, its subcontractors and its applicable third parties (customers, suppliers etc.), which should clearly allocate responsibilities between them.

Additional other information for 5.1, Policies for information security, of ISO/IEC 27002:2022 is:

Any organization that processes PII, whether a PII controller or a PII processor, should consider applicable PII protection legislation or regulation during the development and maintenance of information security policies.

6.2.2 Internal security roles and responsibilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.2 and the following additional guidance applies:

Additional implementation guidance for 5.2, Information security roles and responsibilities, of ISO/IEC 27002:2022 is:

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

The organization should designate a point of contact for use by the customer regarding the processing of PII. When the organization is a PII controller, designate a point of contact for PII principals regarding the processing of their PII (see 7.3.2).

The organization should appoint one or more persons responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII.

The responsible person should, where appropriate:

— be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks;

— be involved in the management of all issues which relate to the processing of PII;

— be expert in data protection legislation, regulation and practice;

— act as a contact point for supervisory authorities;

— inform top-level management and employees of the organization of their obligations with respect to the processing of PII;

— provide advice in respect of privacy impact assessments conducted by the organization.

NOTE Such a person is called a data protection officer in some jurisdictions, which define when such a position is required, along with their position and role. This position can be fulfilled by a staff member or outsourced.

6.2.3 Segregation of duties

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.3 applies.

6.2.4 Management responsibilities

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.4 applies.

6.2.5 Contact with authorities

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.5 applies.

6.2.6 Contact with special interest groups

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.6 applies.

6.2.7 Threat intelligence

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.7 applies.

6.2.8 Information security in project management

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.8 applies.

6.2.9 Inventory of information and other associated assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.9 applies.

6.2.10 Acceptable use of information and other associated assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.10 applies.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

6.2.11 Return of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.11 applies.

6.2.12 Classification of information

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.12 and the following additional guidance applies:

Additional implementation guidance for 5.12, Classification of Information, of ISO/IEC 27002:2022 is:

The organization's information classification scheme should explicitly consider PII as part of the scheme it implements. Considering PII within the overall classification scheme is integral to understanding what PII the organization processes (e.g. type, special categories), where such PII is stored and the systems through which it can flow.

6.2.13 Labelling of information

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.13 and the following additional guidance applies.

Additional implementation guidance for 5.13, Labelling of information, of ISO/IEC 27002:2022 is:

The organization should ensure that people under its control are made aware of the definition of PII and how to recognize information that is PII.

6.2.14 Information transfer

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.14 and the following additional guidance applies:

Additional implementation guidance for 5.14, Information transfer, of ISO/IEC 27002:2022 is:

The organization should consider procedures for ensuring that rules related to the processing of PII are enforced throughout and outside of the system, where applicable.

6.2.15 Access control

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.15 applies.

6.2.16 Identity management

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.16 and the following additional guidance applies:

Additional implementation guidance for 5.16, Identity management, of ISO/IEC 27002:2022 is:

Procedures for registration and de-registration of users who administer or operate systems and services that process PII should address the situation where user access control for those users is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure).

The organization should not reissue to users any de-activated or expired user IDs for systems and services that process PII.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of user ID management. Such cases should be included in the documented information.

Some jurisdictions impose specific requirements regarding the frequency of checks for unused authentication credentials related to systems that process PII. Organizations operating in these jurisdictions should take compliance with these requirements into account.

6.2.17 Authentication information

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.17 applies.

6.2.18 Access rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.18 and the following additional guidance applies:

Additional implementation guidance for 5.18, Access rights, of ISO/IEC 27002:2022 is:

The organization should maintain an accurate, up-to-date record of the user profiles created for users who have authorized access to the information system and the PII contained therein. Each profile comprises the set of data about the user, including user ID, necessary to implement the identified technical controls providing authorized access.

Implementing individual user access IDs enables appropriately configured systems to identify who accessed PII and what additions, deletions or changes they made. As well as protecting the organization, users are also protected as they can identify what they have processed and what they have not processed.

In the case where the organization is providing PII processing as a service, the customer can be responsible for some or all aspects of access management. Where appropriate, the organization should provide the customer the means to perform access management, such as by providing administrative rights to manage or terminate access. Such cases should be included in the documented information.

6.2.19 Information security in supplier relationships

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.19 applies.

6.2.20 Addressing information security within supplier agreements

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.20 and the following additional guidance applies:

Additional implementation guidance for 5.20, Addressing information security within supplier agreements, of ISO/IEC 27002:2022 is:

The organization should specify in agreements with suppliers whether PII is processed and the minimum technical and organizational measures that the supplier needs to meet in order for the organization to meet its information security and PII protection obligations (see 7.2.6 and 8.2.1).

Supplier agreements should clearly allocate responsibilities between the organization, its partners, its suppliers and its relevant third parties (customers, suppliers, etc.) taking into account the type of PII processed.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

The agreements between the organization and its suppliers should provide a mechanism for ensuring the organization supports and manages compliance with all applicable legislation or regulation. The agreements should call for independently audited compliance, acceptable to the customer.

NOTE For such audit purposes, compliance with relevant and applicable security and privacy standards such as ISO/IEC 27001 or this document can be considered.

Implementation guidance for PII processors

The organization should specify in contracts with any suppliers that PII is only processed on its instructions.

6.2.21 Managing information security in the ICT supply chain

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.21 applies.

6.2.22 Monitoring, review and change management of supplier services

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.22 applies.

6.2.23 Information security for use of cloud services

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.23 applies.

6.2.24 Information security incident management planning and preparation

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.24 and the following additional guidance applies:

Additional implementation guidance for 5.24, Information security incident management planning and preparation, of ISO/IEC 27002:2022 is:

As part of the overall information security incident management process, the organization should establish responsibilities and procedures for identifying and recording breaches of PII. Additionally, the organization should establish responsibilities and procedures related to notification to relevant parties of PII breaches (including the timing of such notifications) and the disclosure to authorities, taking into account the applicable legislation or regulation.

Some jurisdictions impose specific regulations regarding breach responses, including notification. Organizations operating in these jurisdictions should ensure that they can demonstrate compliance with these regulations.

6.2.25 Assessment and decision on information security events

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.25 applies.

6.2.26 Response to information security incidents

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.26 and the following additional guidance applies:

Additional implementation guidance for 5.26, Response to information security incidents, of ISO/IEC 27002:2022 is:

Implementation guidance for PII controllers

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

An incident that involves PII should trigger a review by the organization, as part of its information security incident management process, to determine if a breach involving PII that requires a response has taken place.

An event does not necessarily trigger such a review.

NOTE 1 An information security event does not necessarily result in actual, or the significant probability of, unauthorized access to PII or to any of the organization's equipment or facilities storing PII. These can include, but are not limited to, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks and packet sniffing.

When a breach of PII has occurred, response procedures should include relevant notifications and records.

Some jurisdictions define cases when the breach should be notified to the supervisory authority, and when it should be notified to PII principals.

Notifications should be clear.

NOTE 2 Notification can contain details such as:

— a contact point where more information can be obtained;

— a description of and the likely consequences of the breach;

— a description of the breach including the number of individuals concerned as well as the number of records concerned;

— measures taken or planned to be taken.

NOTE 3 Information on the management of security incidents can be found in the ISO/IEC 27035 series.

Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory or forensic purposes, such as:

— a description of the incident;

— the time period;

— the consequences of the incident;

— the name of the reporter;

— to whom the incident was reported;

— the steps taken to resolve the incident (including the person in charge and the data recovered);

— the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify PII principals, regulatory agencies or customers.

Implementation guidance for PII processors

Provisions covering the notification of a breach involving PII should form part of the contract between the organization and the customer. The contract should specify how the organization will provide the information necessary for the customer to fulfil their obligation to notify relevant authorities. This notification obligation does not extend to a breach caused by the customer or PII principal or within system components for which they are responsible. The contract should also define expected and externally mandated limits for notification response times.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

In some jurisdictions, the PII processor should notify the PII controller of the existence of a breach without undue delay (i.e. as soon as possible), preferably, as soon as it is discovered so that the PII controller can take the appropriate actions.

Where a breach involving PII has occurred, a record should be maintained with sufficient information to provide a report for regulatory or forensic purposes, such as:

— a description of the incident;

— the time period;

— the consequences of the incident;

— the name of the reporter;

— to whom the incident was reported;

— the steps taken to resolve the incident (including the person in charge and the data recovered);

— the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII.

In the event that a breach involving PII has occurred, the record should also include a description of the PII compromised, if known; and if notifications were performed, the steps taken to notify the customer or the regulatory agencies.

In some jurisdictions, applicable legislation or regulation can require the organization to directly notify appropriate regulatory authorities (e.g. a PII protection authority) of a breach involving PII.

6.2.27 Learning from information security incidents

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.27 applies.

6.2.28 Collection of evidence

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.28 applies:

6.2.29 Information security during disruption

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.29 applies.

6.2.30 ICT readiness for business continuity

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.30 applies.

6.2.31 Legal, statutory, regulatory and contractual requirements

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.31 and the following additional guidance applies:

Additional other information for 5.31, Legal, statutory, regulatory and contractual requirements, of ISO/IEC 27002:2022 is:

The organization should identify any potential legal sanctions (which can result from some obligations being missed) related to the processing of PII, including substantial fines directly from the local supervisory authority. In some jurisdictions, International Standards such as this document can be used to form the basis for a contract between the organization and the customer, outlining their respective

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023

security, privacy and PII protection responsibilities. The terms of the contract can provide a basis for contractual sanctions in the event of a breach of those responsibilities.

6.2.32 Intellectual property rights

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.32 applies.

6.2.33 Protection of records

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.33 and the following additional guidance applies:

Additional implementation guidance for 5.33, Protection of records, of ISO/IEC 27002:2022 is:

Review of current and historical policies and procedures can be required (e.g. in the cases of customer dispute resolution and investigation by a supervisory authority).

The organization should retain copies of its privacy policies and associated procedures for a period as specified in its retention schedule (see 7.4.7). This includes retention of previous versions of these documents when they are updated.

6.2.34 Privacy and protection of PII

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.34 applies.

6.2.35 Independent review of information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.35 and the following additional guidance applies:

Additional implementation guidance for 5.35, Independent review of information security, of ISO/IEC 27002:2022 is:

Where an organization is acting as a PII processor, and where individual customer audits are impractical or can increase risks to security, the organization should make available to customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the organization's policies and procedures. A relevant independent audit, as selected by the organization, should normally be an acceptable method for fulfilling the customer's interest in reviewing the organization's processing operations, if it covers the needs of anticipated users and if results are provided in a sufficient transparent manner.

6.2.36 Compliance with policies, rules and standards for information security

The control, implementation guidance and other information stated in ISO/IEC 27002:2022, 5.36 and the following additional guidance applies:

Additional implementation guidance for 5.36, Compliance with policies, rules and standards for information security, of ISO/IEC 27002:2022 is:

As part of technical reviews of compliance with security policies and standards, the organization should include methods of reviewing tools and components related to processing PII. This can include:

— ongoing monitoring to verify that only permitted processing is taking place; or

— specific penetration or vulnerability tests (for example, de-identified datasets can be subject to a motivated intruder test to validate that de-identification methods are compliant with organizational requirements).

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC DIS 27701 _2023