AS 27701:2022

Australian STANDARD®

STANDARDS Australia

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (ISO/IEC 27701:2019, MOD)

AS 27701:2022

This Australian Standard® was prepared by IT-012, Information security, cybersecurity and privacy protection. It was approved on behalf of the Council of Standards Australia on 21 January 2022.

This Standard was published on 11 February 2022.

The following are represented on Committee IT-012:

Australian Computer Society
Australian Industry Group
Australian Information Industry Association
Australian Information Security Association
Australian Payments Network
Australian Property Institute
Australian Security Industry Association
Business Continuity Institute Australasia
Consumers Federation of Australia
Cyber Security Cooperative Research Centre
Department of Defence (Australian Government)
Energy Networks Australia
Engineers Australia
ISACA Melbourne
Joint Accreditation System of Australia & New Zealand
National Retail Association Australia
Office of the Victorian Information Commissioner
University of Wollongong

This Standard was issued in draft form for comment as DR AS 27701:2021.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76113 654 2

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (ISO/IEC 27701:2019, MOD)

First published as AS 27701:2022.

Preface

This Standard was prepared by the Standards Australia Committee IT-012, Information security, cybersecurity and privacy protection.

After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian Standard rather than an Australian/New Zealand Standard.

The objective of this document is to specify requirements and provide guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management system (PIMS) in the form of an extension to AS ISO/IEC 27001 and AS 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 and/or PII processors processing PII within an ISMS.

This Standard is an adoption with national modifications and has been reproduced from ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* The modifications are additional guidance and are set out in Appendices ZA and ZB, which have been added at the end of the source text.

Appendix ZA provides an indicative mapping between provisions of the Australian Privacy Principles (APPs) as they apply to private sector entities, the notifiable data breach scheme (NDB Scheme) of the Australian Privacy Act 1988 (Cth) and this document. It shows how conformity to requirements and controls of this document can be relevant to fulfil obligations of private sector entities under the Australian Privacy Principles and the Privacy Act.

Appendix ZB provides an indicative mapping between provisions of the New Zealand Information Privacy Principles (IPPs), the mandatory privacy breach reporting of the New Zealand Privacy Act 2020 and this document. It shows how conformity to requirements and controls of this document can be relevant to fulfil obligations under the New Zealand Information Privacy Principles and the Privacy Act.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface ii
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 27001:2013 requirements 2
4.3 Application of ISO/IEC 27002:2013 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 5
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
5.5 Support 6
5.5.1 Resources 6
5.5.2 Competence 7
5.5.3 Awareness 7
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 Nonconformity and corrective action 8
5.8.2 Continual improvement 8
6 PIMS-specific guidance related to ISO/IEC 27002 8
6.1 General 8
6.2 Information security policies 8
6.2.1 Management direction for information security 8
6.3 Organization of information security 9
6.3.1 Internal organization 9
6.3.2 Mobile devices and teleworking 10
6.4 Human resource security 10
6.4.1 Prior to employment 10
6.4.2 During employment 10

6.4.3 Termination and change of employment 11
6.5 Asset management 11
6.5.1 Responsibility for assets 11
6.5.2 Information classification 11
6.5.3 Media handling 12
6.6 Access control 12
6.6.1 Business requirements of access control 12
6.6.2 User access management 13
6.6.3 User responsibilities 14
6.6.4 System and application access control 14
6.7 Cryptography 14
6.7.1 Cryptographic controls 14
6.8 Physical and environmental security 15
6.8.1 Secure areas 15
6.8.2 Equipment 15
6.9 Operations security 17
6.9.1 Operational procedures and responsibilities 17
6.9.2 Protection from malware 17
6.9.3 Backup 17
6.9.4 Logging and monitoring 18
6.9.5 Control of operational software 19
6.9.6 Technical vulnerability management 19
6.9.7 Information systems audit considerations 19
6.10 Communications security 19
6.10.1 Network security management 19
6.10.2 Information transfer 20
6.11 Systems acquisition, development and maintenance 20
6.11.1 Security requirements of information systems 20
6.11.2 Security in development and support processes 21
6.11.3 Test data 22
6.12 Supplier relationships 23
6.12.1 Information security in supplier relationships 23
6.12.2 Supplier service delivery management 23
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 29
7.2.3 Determine when and how consent is to be obtained 29
7.2.4 Obtain and record consent 30
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
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 Providing mechanism to modify or withdraw consent 33
7.3.5 Providing 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 35
7.3.8 Providing copy of PII processed 35
7.3.9 Handling requests 36
7.3.10 Automated decision making 36
7.4 Privacy by design and privacy by default 37
7.4.1 Limit collection 37
7.4.2 Limit processing 37
7.4.3 Accuracy and quality 37
7.4.4 PII minimization objectives 38
7.4.5 PII de-identification and deletion at the end of processing 38
7.4.6 Temporary files 38
7.4.7 Retention 39
7.4.8 Disposal 39
7.4.9 PII transmission controls 39
7.5 PII sharing, transfer, and disclosure 40
7.5.1 Identify basis for PII transfer between jurisdictions 40
7.5.2 Countries and international organizations to which PII can be transferred 40
7.5.3 Records of transfer of PII 40
7.5.4 Records of PII disclosure to third parties 41

8 Additional ISO/IEC 27002 guidance for PII processors 41
8.1 General 41
8.2 Conditions for collection and processing 41
8.2.1 Customer agreement 41
8.2.2 Organization's purposes 42
8.2.3 Marketing and advertising use 42
8.2.4 Infringing instruction 42
8.2.5 Customer obligations 42
8.2.6 Records related to processing PII 43
8.3 Obligations to PII principals 43
8.3.1 Obligations to PII principals 43
8.4 Privacy by design and privacy by default 43
8.4.1 Temporary files 44
8.4.2 Return, transfer or disposal of PII 44
8.4.3 PII transmission controls 44
8.5 PII sharing, transfer, and disclosure 45
8.5.1 Basis for PII transfer between jurisdictions 45
8.5.2 Countries and international organizations to which PII can be transferred 45
8.5.3 Records of PII disclosure to third parties 46
8.5.4 Notification of PII disclosure requests 46
8.5.5 Legally binding PII disclosures 46
8.5.6 Disclosure of subcontractors used to process PII 46
8.5.7 Engagement of a subcontractor to process PII 47
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) 52**

Annex C (informative) **Mapping to ISO/IEC 29100 55**

Annex D (informative) **Mapping to the General Data Protection Regulation 57**

Annex E (informative) **Mapping to ISO/IEC 27018 and ISO/IEC 29151 60**

Annex F (informative) **How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002 63**

Bibliography 65

Appendix ZA (informative) **Mapping to the Australian Privacy Principles and Notifiable Data Breach Scheme of the *Privacy Act 1988* (Cth)** **66**

Appendix ZB (informative) **Mapping to the Information Privacy Principles and Notifiable Privacy Breaches regime of the New Zealand *Privacy Act 2020*** **72**

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*.

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.

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 and/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 and/or regulation exist. 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 need to be interpreted to take into account local legislation and/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.

Australian Standard®

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (ISO/IEC 27701:2019, MOD)

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 and/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 27001:2013, *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, *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 http://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

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