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

This is a preview. Click here to purchase the full publication.

    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

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

This is a preview. Click here to purchase the full publication.

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 is a preview. Click here to purchase the full publication.

This Standard is identical with, 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

This is a preview. Click here to purchase the full publication.

This is a preview. Click here to purchase the full publication.

This is a preview. Click here to purchase the full publication.

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

This is a preview. Click here to purchase the full publication.

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.

This is a preview. Click here to purchase the full publication.

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.