STANDARDS Australia

AS/NZS ISO/IEC 27001:2006

Information technology — Security techniques — Information security management systems — Requirements

STANDARD

AS/NZS

STANDARDS NEW ZEALAND
PAEREWA AOTEAROA

AS/NZS ISO/IEC 27001:2006

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 19 May 2006 and on behalf of the Council of Standards New Zealand on 2 June 2006.
This Standard was published on 23 June 2006.

The following are represented on Committee IT-012:

Attorney General's Department
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Department of Defence
Department of Social Welfare, NZ
Government Communications Security Bureau, NZ
Internet Industry Association
NSW Police Service
New Zealand Defence Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 06091.

AS/NZS ISO/IEC 27001:2006

Australian/New Zealand Standard™

Information technology—Security techniques—Information security management systems—Requirements

Originated as part of AS/NZS 4444:1996.
Previous edition AS/NZS 7799.2:2003.
Jointly revised and redesignated as AS/NZS ISO/IEC 27001:2006.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 7497 0

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification to supersede AS/NZS 7799.2:2003, *Information security management*, Part 2: *Specification of information security management systems.*

This Standard is identical with, and has been reproduced from ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements*. It represents both an update to the existing ISMS standard (AS/NZS 7799.2:2003) and the adoption of the revised ISO numbering convention which will gather the core information security standards together into the newly allocated 27000 series.

The objective of this Standard is to specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof (see Annex B which provides informative guidance on the use of this Standard).

The ISMS is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text 'this International Standard' should read 'Australia/New Zealand Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian/New Zealand Standard*	
ISO/IEC		AS/NZS	
17799	Information technology—Security techniques—Code of practice for information security management	17799	Information technology—Code of practice for information security management

The terms 'normative' and 'informative' have been used in this Standard to define the application of the annex to which they apply. A 'normative' annex is an integral part of a Standard, whereas an 'informative' annex is only for information and guidance.

CONTENTS

Page

1 Scope 1
1.1 General 1
1.2 Application 1

2 Normative references 1

3 Terms and definitions 2

4 Information security management system 3
4.1 General requirements 3
4.2 Establishing and managing the ISMS 4
4.2.1 Establish the ISMS 4
4.2.2 Implement and operate the ISMS 6
4.2.3 Monitor and review the ISMS 6
4.2.4 Maintain and improve the ISMS 7
4.3 Documentation requirements 7
4.3.1 General 7
4.3.2 Control of documents 8
4.3.3 Control of records 8

5 Management responsibility 9
5.1 Management commitment 9
5.2 Resource management 9
5.2.1 Provision of resources 9
5.2.2 Training, awareness and competence 9

6 Internal ISMS audits 10

7 Management review of the ISMS 10
7.1 General 10
7.2 Review input 10
7.3 Review output 11

8 ISMS improvement 11
8.1 Continual improvement 11
8.2 Corrective action 11
8.3 Preventive action 12

Annex A (normative) **Control objectives and controls** 13

Annex B (informative) **OECD principles and this International Standard** 30

Annex C (informative) **Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard** 31

Bibliography 34