



AS/NZS ISO/IEC 17799:2006
**Information technology — Security techniques
— Code of practice for information
security management**



STANDARD

AS/NZS
➔

AS/NZS ISO/IEC 17799:2006

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 23 May 2006 and on behalf of the Council of Standards New Zealand on 16 June 2006. This Standard was published on 6 July 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 Standards may also be withdrawn.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 06092.

AS/NZS ISO/IEC 17799:2006

Australian/New Zealand Standard™

**Information technology—Security
techniques—Code of practice for
information security management**

Originated as part of AS/NZS 4444:1996.
Previous edition AS/NZS ISO/IEC 17799:2001.
Second edition 2006.

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

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

ISBN 0 7337 7492 X

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology to supersede AS/NZS ISO/IEC 17799:2001.

This Standard is identical with and has been reproduced from ISO/IEC 17799:2005.

The objective of this Standard is to provide a practical guideline for developing organizational security, standards and effective security management practices and to help build confidence in inter-organizational activities.

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

CONTENTS

| | Page |
|--|-----------|
| 1 SCOPE | 1 |
| 2 TERMS AND DEFINITIONS | 1 |
| 3 STRUCTURE OF THIS STANDARD | 4 |
| 3.1 CLAUSES | 4 |
| 3.2 MAIN SECURITY CATEGORIES | 4 |
| 4 RISK ASSESSMENT AND TREATMENT | 5 |
| 4.1 ASSESSING SECURITY RISKS | 5 |
| 4.2 TREATING SECURITY RISKS..... | 5 |
| 5 SECURITY POLICY | 7 |
| 5.1 INFORMATION SECURITY POLICY | 7 |
| 5.1.1 <i>Information security policy document</i> | 7 |
| 5.1.2 <i>Review of the information security policy</i> | 8 |
| 6 ORGANIZATION OF INFORMATION SECURITY | 9 |
| 6.1 INTERNAL ORGANIZATION | 9 |
| 6.1.1 <i>Management commitment to information security</i> | 9 |
| 6.1.2 <i>Information security co-ordination</i> | 10 |
| 6.1.3 <i>Allocation of information security responsibilities</i> | 10 |
| 6.1.4 <i>Authorization process for information processing facilities</i> | 11 |
| 6.1.5 <i>Confidentiality agreements</i> | 11 |
| 6.1.6 <i>Contact with authorities</i> | 12 |
| 6.1.7 <i>Contact with special interest groups</i> | 12 |
| 6.1.8 <i>Independent review of information security</i> | 13 |
| 6.2 EXTERNAL PARTIES | 14 |
| 6.2.1 <i>Identification of risks related to external parties</i> | 14 |
| 6.2.2 <i>Addressing security when dealing with customers</i> | 15 |
| 6.2.3 <i>Addressing security in third party agreements</i> | 16 |
| 7 ASSET MANAGEMENT | 19 |
| 7.1 RESPONSIBILITY FOR ASSETS..... | 19 |
| 7.1.1 <i>Inventory of assets</i> | 19 |
| 7.1.2 <i>Ownership of assets</i> | 20 |
| 7.1.3 <i>Acceptable use of assets</i> | 20 |
| 7.2 INFORMATION CLASSIFICATION | 21 |
| 7.2.1 <i>Classification guidelines</i> | 21 |
| 7.2.2 <i>Information labeling and handling</i> | 21 |
| 8 HUMAN RESOURCES SECURITY | 23 |
| 8.1 PRIOR TO EMPLOYMENT | 23 |
| 8.1.1 <i>Roles and responsibilities</i> | 23 |

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
 - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-