AS/NZS ISO/IEC 18028.1:2008
ISO/IEC 18028-1:2006

Australian/New Zealand Standard™

Information technology—Security techniques—IT network security

Part 1: Network security management

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 28 May 2008 and on behalf of the Council of Standards New Zealand on 31 May 2008.
This Standard was published on 25 June 2008.

The following are represented on Committee IT-012:

Attorney General's Office
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Council of Small Business Organisations
Internet Industry Association
NSW Police
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 Standards may also be withdrawn.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 07261.

Australian/New Zealand Standard™

Information technology—Security techniques—IT network security

Part 1: Network security management

First published as AS/NZS ISO/IEC 18028.1:2008.

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

ISBN 0 7337 8769 X

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology.

The objective of this Standard is to provide IT professionals and general line management with detailed guidance on the planning, installation and ongoing maintenance of IT networks.

This Standard is identical with, and has been reproduced from ISO/IEC 18028-1:2006, *Information technology—Security techniques—IT network security,* Part 1: *Network security management*.

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) 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	27002	Information technology—Security Techniques—Code of practice for information security management
		AS/NZS ISO/IEC	
18028	Information technology—Security techniques—IT network security	18028	Information technology—Security techniques—IT network security
18028-2	Part 2: Network security architecture	18028.2	Part 2: Network security architecture
18028-3	Part 3: Securing communications between networks using security gateways	18028.3	Part 3: Securing communications between networks using security gateways
18028-4	Part 4: Securing remote access	18028.4	Part 4: Securing remote access
18028-5	Part 5: Securing communications across networks using virtual private networks	18028.5	Part 5: Securing communications across networks using virtual private networks
18044	Information technology—Security techniques—Information security incident management	18044	Information technology—Security techniques—Information security incident management

Any international references not listed have not been adopted as Australian or Australian/New Zealand Standards.

CONTENTS

Page

Page

INTRODUCTION

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions. A secure network should be protected against malicious and inadvertent attacks, and should meet the business requirements for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall end-to-end security solution. Thus, the purpose of ISO/IEC 18028 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in this standard to meet their specific requirements. Its main objectives are as follows:

— in ISO/IEC 18028-1, to define and describe the concepts associated with, and provide management guidance on, network security – including on how to identify and analyze the communications related factors to be taken into account to establish network security requirements, with an introduction to the possible control areas and the specific technical areas (dealt with in subsequent parts of ISO/IEC 18028);

— in ISO/IEC 18028-2, to define a standard security architecture, which describes a consistent framework to support the planning, design and implementation of network security;

— in ISO/IEC 18028-3, to define techniques for securing information flows between networks using security gateways;

— in ISO/IEC 18028-4, to define techniques for securing remote access;

— in ISO/IEC 18028-5, to define techniques for securing inter-network connections that are established using virtual private networks (VPNs).

ISO/IEC 18028-1 is relevant to anyone involved in owning, operating or using a network. This includes senior managers and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security and/or network security, network operation, or who are responsible for an organization's overall security program and security policy development.

ISO/IEC 18028-2 is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network managers, administrators, engineers, and network security officers).

ISO/IEC 18028-3 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example network managers, administrators, engineers and network security officers).

ISO/IEC 18028-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of remote access security (for example network managers, administrators, engineers, and network security officers).

ISO/IEC 18028-5 is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example network managers, administrators, engineers, and network security officers).

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology — Security techniques — IT network security —

Part 1:
Network security management

1 Scope

ISO/IEC 18028-1 provides direction with respect to networks and communications, including on the security aspects of connecting information system networks themselves, and of connecting remote users to networks. It is aimed at those responsible for the management of information security in general, and network security in particular. This direction supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, provides an introduction on how to identify appropriate control areas with respect to security associated with connections to communications networks, and provides an overview of the possible control areas including those technical design and implementation topics dealt with in detail in ISO/IEC 18028-2 to ISO/IEC 18028-5.

2 Normative references

The following referenced documents are indispensable for the application 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 18028-2:2005, *Information technology — Security techniques — IT network security — Part 2: Network security architecture*

ISO/IEC 18028-3:2005, *Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways*

ISO/IEC 18028-4:2005, *Information technology — Security techniques — IT network security — Part 4: Securing remote access*

ISO/IEC 18028-5:2006, *Information technology — Security techniques — IT network security — Part 5: Securing communications across networks using virtual private networks*

ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 18044:2004, *Information technology — Security techniques — Information security incident management*

ISO/IEC 18043:2006, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems*