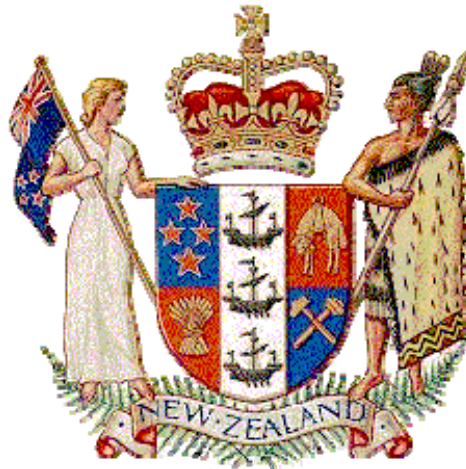


UNCLASSIFIED



Introduction to the NZSIT 400 Document Series

NZSIT 400:2008

Government Communications Security Bureau

February 2008

UNCLASSIFIED

© Government Communications Security Bureau

The NZSIT 400 document series contains information from the publication Australian Government Information and Communications Technology Security Manual (ACSI-33) which is copyright of the Commonwealth of Australia. With the agreement of the Government of Australia, relevant information has been adopted for New Zealand use.

The content of the NZSIT 400 document series is subject to Crown copyright protection unless otherwise indicated. Where security requirements permit, the Crown copyright protected material may be downloaded, displayed, printed and reproduced free of charge for non-commercial use in any format or media without requiring specific permission, provided that it is reproduced accurately in unaltered form, and that the source and copyright status of the material is acknowledged. Apart from any use as permitted under the Copyright Act 1994, all other rights are reserved.

The permission to reproduce Crown copyright protected material does not extend to any material that is identified as being the copyright of the Commonwealth of Australia or a third party. Authorisation to reproduce such material must be obtained from the copyright holders concerned.

Director Information Assurance
Government Communications Security Bureau
PO Box 12-209
WELLINGTON
liaison@gcsb.govt.nz

Foreword

1. The NZSIT 400 document series is issued under the authority of the Director, Government Communications Security Bureau as delegated from Security in the Government Sector (SIGS). The series sets out New Zealand Government policies, practices and procedures essential to the protection of information and communications technology (ICT) in the New Zealand Government and is supported for Personnel and Physical Security aspects by the Protective Security Manual (PSM).
2. The NZSIT 400 document series is published in two versions. The NZSIT 401 IN-CONFIDENCE document is available to those individuals or organisations that deal with nationally classified information of CONFIDENTIAL and above and are considered to have a need-to-know. The NZSIT 402 UNCLASSIFIED document (previously known as the NZSIT 400) is available to all other government agencies.
3. The NZSIT 401 provides implementation guidance designed to enable government agencies operating information systems processing **CONFIDENTIAL**, **SECRET** and **TOP SECRET** information to achieve an assured information technology security environment. The NZSIT 402 provides guidance designed to enable agencies operating information systems processing **UNCLASSIFIED** information to achieve an assured information technology environment.
4. The New Zealand Government must share information – between agencies, with the public and with industry – to function effectively. Yet that sharing, vital though it may be, poses risks to sensitive Government information. These risks must be managed carefully and consistently across government. This manual provides guidance to government departments, agencies and commercial service providers for managing those risks.
5. The structure and content of the NZSIT 400 document series was developed from the Australian Commonwealth Government's Australian Communications Security Instruction 33 (ACSI 33). GCSB acknowledges and thanks the author agency, the Defence Signals Directorate, for allowing NZ Government use of ACSI 33. Users familiar with ACSI 33 should note, however, that there are variations between the Australian and New Zealand documents in line with the two countries' different laws, policies and strategies.
6. Users of the NZSIT 400 document series are encouraged to provide feedback on its utility and content so that it may evolve to meet the new and emerging business requirements of government departments and agencies. As required, new versions of the NZSIT 400 document series will be issued to keep pace with the needs of NZ Government.

Overview

Introduction

1.1. This document NZSIT 400 contains important information about the NZSIT 400 document series and how it relates to the security of government Information Technology (IT) systems, including:

- How to use manuals effectively,
 - important definitions, and
 - the authority by which the standards and requirements within these manuals are set.
-

Contents

1.2. This document contains the following topics:

Topic	See block reference
Using the NZSIT 400 Document Series	2.1.
Sources of Additional Information	3.1.

Using the NZSIT 400 Document Series

Introduction

2.1. The information in this topic will help you to use these manuals more effectively.

Replaces the NZSIT 100 and 200 series

2.2. NZSIT 400 document series replaces the NZSIT100 and NZSIT200 series of publications, which should be destroyed. Copies may be returned to the GCSB for destruction.

Classification of NZSIT 400 document series

2.3. NZSIT 400 document series is published in two versions as shown in the table below. The abbreviations for each classification are shown in square brackets.

Version/classification	System classifications covered
IN CONFIDENCE NZSIT 401	As per the Unclassified version plus: <ul style="list-style-type: none"> • CONFIDENTIAL [C], • SECRET [S], and • TOP SECRET [TS].
Unclassified NZSIT 402	Unclassified: <ul style="list-style-type: none"> • IN CONFIDENCE [IC], • SENSITIVE [Sv], and • RESTRICTED [R].

Paragraph numbering

2.4. Paragraph numbers consist of several fields separated by full stops. The fields are ordered as follows:

- Part number
- Chapter number
- Paragraph number

Readers of the NZSIT 402 Unclassified version will notice that in places the numbering is non-sequential. This is intentional and indicates that the missing text relates to classifications outside the scope of the version of the document being read.

Continued on next page

Using the NZSIT 400 Document Series, Continued

Paragraph applicability and system classifications

2.5. Readers will note that some paragraph titles include a system classification reference, shown within square brackets. Paragraph titles that do not include a classification reference indicate that the paragraph applies to all classifications.

Updates

2.6. The NZSIT 400 documents are updated regularly. It is important that agencies ensure that they are using the latest release.

You can get the latest version from:

Version	Location
IN CONFIDENCE	<ul style="list-style-type: none"> The State Services Commission's Public Service Intranet URL: www.psi.govt.nz/ (member agencies only) On CD from the GCSB See: Contacting the GCSB, block reference 1.2.6. in the NZSIT 401 / NZSIT 402 Security Manual.
Unclassified	<ul style="list-style-type: none"> The GCSB's Internet website URL: www.gcsb.govt.nz/publications/index.html

Feedback

2.7. The GCSB welcomes feedback about these manuals. Please contact the Information Assurance Division of the GCSB to suggest improvements or to advise of inaccuracies and ambiguities.

See: Contacting the GCSB, block reference 1.2.6. in the NZSIT 401 / NZSIT 402 Security Manual.

Target audience

2.8. The target audience for this manual is the people responsible for the management and security of NZ Government information and IT systems, including:

- Information and IT managers and administrators,
- IT Security Managers (ITSMs) and administrators,
- Departmental Security Officers (DSOs),
- Outsourcers and other parties providing IT or security services to Government agencies.

Continued on next page

Using the NZSIT 400 Document Series, Continued

Classification terminology

2.9. This document adopts the following information classification terms:

Term	Type of information
National Security	Information classified RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET .
Policy and Privacy	Information classified IN CONFIDENCE or SENSITIVE .
Classified	Information that is classified as either 'National Security' or 'Policy and Privacy'. Important: 'Classified' information does not include information deemed to be 'unclassified'.
Unclassified	Information that has been assessed as not containing any material that warrants a security classification.
Public domain	The unclassified information authorised for unlimited public access and circulation, such as agency publications and websites.

Keywords for requirements

2.10. The table below defines the keywords used within this document series to indicate the level of requirements. All keywords are presented in bold, upper case format.

Keyword	Interpretation
MUST	The item is mandatory. See: Waivers against " MUSTs " and " MUST NOTs ", block reference 2.11.
MUST NOT	Non-use of the item is mandatory. See: Waivers against " MUSTs " and " MUST NOTs ", block reference 2.11.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. See: Deviations , block reference 2.12.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course. See: Deviations , block reference 2.12.
RECOMMENDS RECOMMENDED	The specified body's recommendation or suggestion. Note: Agencies deviating from a RECOMMENDS or RECOMMENDED are encouraged to document the reason(s) for doing so.

Continued on next page

Using the NZSIT 400 Document Series, Continued

Waivers

2.11. Agencies deviating from a **“MUST”** or **“MUST NOT”**, **MUST** provide a waiver in accordance with the following requirements.

- A waiver may be granted to accept the risk posed by the lack of a particular control or mandated policy requirement.
 - A waiver may require special limitations on operation, additional security monitoring or other restrictions.
 - A waiver is granted only when the benefit of operation clearly outweighs any security concern raised by the shortcoming.
 - A waiver **MUST** be based on a specific national security requirement and a certification of compelling need.
 - A time period for the waiver **SHOULD** be specified.
-

Deviations

2.12. Agencies deviating from a **“SHOULD”** or **“SHOULD NOT”**, **MUST** document:

- the reasons for the deviation,
 - an assessment of the residual risk resulting from the deviation,
 - a date by which to review the decision, and
 - management’s approval.
-

Legislation and other Government policy

2.13. Government departments **MUST** comply with the requirements of these manuals subject to any obligations imposed by relevant legislation or law; and subject to any overriding Government policy instruction. While this document series contains examples of when some laws may be relevant for agencies, there is no comprehensive consideration of such issues. Accordingly, agencies should rely on their own inquiries in that regard.

Waivers

2.11. Agencies deviating from a **“MUST”** or **“MUST NOT”**, **MUST** provide a waiver in accordance with the following requirements.

- A waiver may be granted to accept the risk posed by the lack of a particular control or mandated policy requirement.
 - A waiver may require special limitations on operation, additional security monitoring or other restrictions.
 - A waiver is granted only when the benefit of operation clearly outweighs any security concern raised by the shortcoming.
 - A waiver **MUST** be based on a specific national security requirement and a certification of compelling need.
 - A time period for the waiver **SHOULD** be specified.
-

Deviations

2.12. Agencies deviating from a “**SHOULD**” or “**SHOULD NOT**”, **MUST** document:

- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- a date by which to review the decision, and
- management’s approval.

Legislation and other Government policy

2.13. Government departments **MUST** comply with the requirements of these manuals subject to any obligations imposed by relevant legislation or law; and subject to any overriding Government policy instruction. While this document series contains examples of when some laws may be relevant for agencies, there is no comprehensive consideration of such issues. Accordingly, agencies should rely on their own inquiries in that regard.

Sources of Additional Information

Where does NZSIT 400 document series fit in?

3.1. NZSIT 400 document series has a close relationship with *Security in the Government Sector (SIGS)* and *The Protective Security Manual (PSM)*. SIGS is issued by the Prime Minister through the Interdepartmental Committee on Security. Compliance to SIGS is mandatory for all government agencies. The PSM builds on SIGS in the areas of Protective Security (Personnel and Physical security). It is issued by the NZ Security Intelligence Service. NZSIT 400 document series builds on SIGS in the areas of IT Security (Computer, Communications and Technical security).

Note: These manuals use the term 'agencies' to cover all government departments, ministerial offices, the NZ Police, NZ Defence Force, and the NZSIS.

Additional information

3.2. The table below identifies the location of related information contained in other documents.

Topic	See
Classification labelling	<ul style="list-style-type: none"> • SIGS Chapter 3: Information Classification
Clearances	<ul style="list-style-type: none"> • SIGS Chapter 5: Personnel Security
Information security management	<ul style="list-style-type: none"> • ISO/IEC 27002:2007 (to replace AS/NZS ISO/IEC 17799:2001) • Information Technology–Code of Practice for Information Security Management (Standards NZ) • ISO/IEC 27001:2005 (replaced AS/NZS 7799.2:2003) • Information Security Management–Part 2: Specifications for Security Management Systems (Standards NZ)
Information security responsibilities	<ul style="list-style-type: none"> • SIGS Chapter 2: Security Organisation
Information security risk management	<ul style="list-style-type: none"> • HB 231: Information Security Risk Management Guidelines (Standards NZ) • AS/NZS 4360: Risk Management (Standards NZ)
Information security training	<ul style="list-style-type: none"> • Information Assurance Customer Training Programme (GCSB)
Management of electronic evidence	<ul style="list-style-type: none"> • HB 171: Guidelines for the Management of IT Evidence (Standards Australia). Note: use for guidance only; this is not approved as an NZ standard.
Physical security requirements	<ul style="list-style-type: none"> • SIGS • The PSM
Reporting security incidents	<ul style="list-style-type: none"> • The PSM Supplement 2: Breaches of Security
Storing and archiving govt information	<ul style="list-style-type: none"> • Public Records Act 2005 (Archives New Zealand)