SECURITY IN THE GOVERNMENT SECTOR

DEPARTMENT OF THE PRIME MINISTER AND CABINET

2002

Table of Contents

Prime Minister

FOREWORD

The government requires that official information receives appropriate protection where it is in the national or the public interest to do so. This includes situations where unauthorised disclosure would damage national security, prejudice the interests of the New Zealand Government, endanger the safety of New Zealand citizens, obstruct the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of New Zealanders.

This manual, Security in the Government Sector, issued by the Interdepartmental Committee on Security sets out protective security policies, principles and procedures. Further guidance and more detail about procedures are provided in supplementary manuals produced by the New Zealand Security Intelligence Service and the Government Communications Security Bureau. Together they provide updated guidance on safeguarding government functions, resources and information from any sources of harm. Potential sources of harm include: theft, burglary or other criminal activities; individuals or groups seeking unlawfully to access economically or commercially valuable material or intellectual property; actions by disaffected staff; groups involved in politically motivated violence; or foreign intelligence services.

The heads of government departments and agencies are responsible for implementing effective protective security arrangements within their organisations and all public service staff are responsible for complying with these requirements.

Helen Clark
Prime Minister

PREFACE

This manual is issued by the Interdepartmental Committee on Security in accordance with its terms of reference. It replaces the manual "Security in Government Departments" issued in 1994, and incorporates the revised security classification system approved by Cabinet on 18 December 2000.

The manual takes into account the Australian/New Zealand Standard AS/NZS ISO/IEC 17799:2001 "*Information Technology – Code of Practice for Information Security Management*". Although the Standard is primarily directed to information technology, its principles are equally relevant to protecting from compromise the integrity and availability of information in all its forms. "Security in the Government Sector" takes a wider perspective and considers the protective security of both information and equipment – comprising physical, personnel, document, information technology and communication security measures. A cross reference has been provided to enable a check to be made against the Standard.

Some of the manual content is based on or drawn from similar overseas publications - in particular, Australia's "*Commonwealth Protective Security Manual*", and the United Kingdom's "*Manual of Protective Security*".

The manual is mandatory for government departments, ministerial offices, the NZ Police, the NZ Defence Force, the NZ Security Intelligence Service and the Government Communications Security Bureau. It is also made available to State Owned Enterprises and Crown Entities to assist them in meeting their obligations under the Official Information Act 1982 and the Privacy Act 1993.

"Security in the Government Sector" is designed to help government departments and agencies, State Owned Enterprises and Crown Entities develop their security instructions based on a framework that is consistent throughout the Government sector. While chief executives are responsible for developing, implementing and maintaining standards of protective security within their organisations using a risk management approach, there are certain minimum standards which must be met. These are detailed in this manual.

It would not be practical to attempt to include all detailed advice on matters of security in one manual. The New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB) have produced supplementary manuals and documents intended for the guidance of Departmental Security Officers. These are the NZSIS "Protective Security Manual" (PSM) and the GCSB "New Zealand Security in Information Technology" (NZSIT) series.

Within these guidelines it is expected that each organisation will develop security policies and instructions that are applicable to the circumstances of that organisation and its risk assessment. Once security instructions are adopted they should be mandatory for all staff.

Table of Contents

Chapter 1: Security Policy

Policy Statement

1. The Government requires that information important to its functions, its official resources and its classified equipment is adequately safeguarded to protect the public and national interests and to preserve personal privacy. This policy addresses the protection of the Confidentiality[1], Integrity[2] and Availability[3] of all official information. Official information includes information that is produced, transmitted, and stored in electronic form. This policy also addresses the classified equipment used to produce, transmit and store official information.

2. Chief Executives and heads of government departments and agencies, State Owned Enterprises and Crown Entities are responsible for implementing and managing effective security arrangements within their organisations. They must create and maintain appropriate security environments to adequately protect official information and classified equipment. The level of protection must correspond to the assessed level of risk.

3. Protective security usually incorporates the following measures:

   - personnel security
   - physical security
   - communications security
   - computer security
   - technical security.

4. These measures may be expensive to implement and have an impact on the operations of the organisation. However, security decisions are no different from other administrative decisions; they must be formulated on a sound factual, financial, lawful and ethical basis. Most importantly, they must be based on an assessment of risk.

5. The environment conducive to good security is not necessarily secret. In fact, the decision-making process must be as transparent as possible. This will ensure accountability to the New Zealand public.

Security Framework

6. This manual provides general guidance and broad advice on protective security matters. Government organisations responsible for providing security advice may produce their own documentation to supplement this manual.

---

1. Confidentiality - information must not be made available or disclosed to unauthorised individuals, entities, or processes.
2. Integrity - data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes.
3. Availability - information must be accessible and useable on demand by authorised entities.

7. An appropriate security environment requires a systematic and co-ordinated approach. An organisation must first identify and assess its risk environment, then develop its security plan. To be effective, planning for the management of security risks should become part of an organisation's culture. Security should be integrated into the organisation's philosophy, practices and plans. It should not be treated as a separate activity. All managers should be encouraged to recognise that risk management and good security practices are a fundamental part of management.

8. While each organisation's security plan will relate directly to its culture, environment, geographic location, function and corporate structure, all government organisations must demonstrate a commitment to the Government's security policy, principles and minimum standards.

9. A security classification system has been developed for official information held by or shared between government organisations. This system ensures that information is protected according to the degree of harm that could result from its unauthorised disclosure. When official information has a security classification, the minimum standards for its handling and protection must be followed. The decision to classify information must be based solely on the guidelines in Chapter 3: Information Classification.

10. To access certain classified information or equipment, a person must receive security clearance from the Chief Executive or head of a government organisation on behalf of the Government as a whole. For the personnel security clearance system to operate efficiently and effectively, the authority granting a security clearance must adhere to minimum standards found in Chapter 5: Personnel Security.

11. Minimum standards also apply to the physical environments that store classified information or equipment. These standards are found in Chapter 7: Physical and Environmental Security.

Risk Management

12. Regardless of an organisation's functions or security concerns, the key messages for managing security risks remain the same:

    - security risk management is everyone's business
    - risk management, including security risk management, is part of day-to-day business
    - the process for managing security risk is logical and systematic, and should become a habit.

13. Part of the organisation's risk management strategy is to decide on how much protection is required. The methodology should be based on the principles of general risk analysis and risk management found in the Australian/New Zealand Standards *AS/NZS 4360:1999 - Risk Management* and *AS/NZS ISO/IEC 17999:2001 - Information Technology Code of Practice for Iinformation Security Management*.

14. The New Zealand Security Intelligence Service (NZSIS) has provided more detail about security risk management in the *Protective Security Manual*.

Business Continuity Management

15. There should be a managed process in place for developing and maintaining business continuity throughout the organisation. This manual discusses only the business continuity related to the security of IT systems.

16. A Business Continuity Plan (BCP) should be developed for each site or system. This will assist in a managed recovery of processing facilities and databases from a major disaster or system failure. The BCP should:

    - include measures to identify and manage risks
    - limit the consequences when a problem occurs
    - ensure that essential operations are quickly resumed.

17. For further guidance on the development of a BCP, see *Chapter 9 of NZ Security of Information and Technology Publication (NZSIT) 101*.

Responsibility for Security

18. Each government department or agency, State Owned Enterprise or Crown Entity is responsible for its own protective security arrangements. The success of this system depends on:

    - effective security arrangements within each organisation
    - inter-organisational agreement on security policy and common minimum standards
    - access by organisations to security intelligence records and specialist advice on specific security problems.

19. To help organisations meet this responsibility, a number of security agencies and committees decide security policy, provide advice and offer guidance. These agencies and committees analyse policy issues on security matters, generate ideas, achieve consensus and make policy recommendations to Government.

Security Agencies

New Zealand Security Intelligence Service (NZSIS)

www.nzsis.govt.nz

20. The NZSIS establishes personnel and physical security standards for the protection of national security information, as authorised by the NZSIS Act 1969 (including amendments).

21. The NZSIS informs the Government about matters of concern exposed by intelligence-gathering operations.

22. The NZSIS advises government departments and agencies, State Owned Enterprises and Crown Entities on personnel and physical security relating to the protection of national security information.

23. On the request of government organisations, NZSIS vets personnel requiring security clearances for access to classified material.

Government Communications Security Bureau (GCSB)

www.gcsb.govt.nz

24. The GCSB is the national authority for Information Systems Security (INFOSEC). INFOSEC, in the government context, is the protection of official information against unauthorised disclosure, manipulation, destruction or alteration. This embraces Communications Security (COMSEC), Technical Security (TECSEC), and Computer Security (COMPUSEC).

25. GCSB's responsibilities include:

    - Promulgating national INFOSEC doctrine and standards for government
    - advising government organisations on applying national INFOSEC policy and standards
    - providing INFOSEC inspection service for government
    - providing an INFOSEC education and training programme for governmnet personnel.

Interdepartmental Security Committees

Officials Committee for Domestic and External Security Co-ordination (ODESC)

26. The Officials Committee for Domestic and External Security Co-ordination (ODESC) is the committee of government officials charged with giving the Prime Minister strategic policy advice on domestic and external security matters. The committee reports to the Prime Minister and is chaired by the Chief Executive of the Department of the Prime Minister and Cabinet, with membership being drawn from Chief Executives of appropriate government agencies.

27. One of the functions of ODESC is to maintain oversight of security within government departments and agencies, including the setting of appropriate security standards.

Interdepartmental Committee on Security (ICS)

28. All government organisations must follow common minimum standards of security so that information can be passed knowing that each party handles it with equal care. The ICS is responsible for formulating and co-ordinating the application of all aspects of security policy and common minimum standards of security and protection. The ICS Terms of Reference are detailed at Annex A to this Chapter.

The Government Communications Security Committee (GCSC)

29. The GCSC is responsible for formulating and reviewing New Zealand's COMSEC doctrine and standards. The core committee membership of the GCSC comes from the GCSB, MFAT, NZDF and NZSIS. Additional representatives may be co-opted from other government departments where necessary. The GCSC Terms of Reference are detailed at Annex B to this Chapter.

The Departmental Committee on Computer Security (DCCS)

30. The DCCS is responsible for formulating national COMPUSEC doctrine and standards for protecting classified official information stored or processed in government or contracted private computer systems. The DCCS is chaired by the GCSB. The core membership of the DCCS comes from the GCSB, MFAT, NZDF, NZSIS, NZ Police, Customs, and the State Services Commission. The DCCS Terms of Reference are detailed at Annex C to this Chapter.

Annex A—Terms of Reference: Interdepartmental Committee on Security

1. The Government requires that official information be given appropriate protection. All Government departments and agencies, State Owned Enterprises and Crown Entities and any other organisations or bodies which receive or hold information that is classified in accordance with the prescriptions in Cabinet Directive CO (01) 10 of 31 July 2001 are to apply common security standards and meet specified personnel requirements to ensure that the information is not improperly disclosed to a person or persons who are not authorised to receive that information.

2. To ensure that the Government's security requirements are met, the Interdepartmental Committee on Security will:

    - Provide to Government and other organisations or bodies which receive or hold classified information, detailed advice on the policies and administrative procedures which are necessary to apply in a consistent manner the prescribed system of security classifications and protect classified material from unauthorised disclosure

    - Advise the Government, through the ODESC, on those aspects of security policy where it considers action to be required, and at frequent intervals, review and update the manual entitled "Security in the Government Sector", in which the Committee shall prescribe standards necessary to ensure the proper handling of classified material and the application of appropriate personnel security criteria and standards. In doing so the Committee will take account of any changes in the threats to New Zealand interests, and developments or changes in the security standards applied by friendly countries which provide classified or other sensitive information to New Zealand. It shall be responsible for the publication and promulgation to relevant organisations and bodies of agreed amendments to the "Security in the Government Sector" manual.

3. The Committee shall also provide guidance on the use of endorsement marks, which may be used to identify the nature of the information being protected and the security standards required to protect the information.

4. The Committee shall not be responsible for the implementation and maintenance of security standards in Government and other relevant organisations. That shall remain the responsibility of the appropriate Chief Executive or Head.

5. The ICS is a sub-committee of the ODESC. The Chairman of the Committee shall report regularly to the ODESC.

Composition and Servicing of the Committee

6. The composition of the Committee shall be changed only with the approval or direction of the ODESC. It shall meet under the chairmanship of, and be serviced by, the Department of the Prime Minister and Cabinet. Its membership currently includes representatives of the MOD, MFAT, SSC, NZDF, NZ Police, Cabinet Office, NZSIS and GCSB.

Annex B—Terms of Reference: Government Communications Security Committee

1. The Government Communications Security Committee (GCSC) is established as a sub-committee of the Officials Committee for Domestic and External Security Co-ordination (ODESC).

2. The Committee comprises suitably qualified representatives representing MFAT, NZDF and NZSIS and is chaired by the Director, GCSB or his/her representative. The Committee may co-opt additional representatives from other Government organisations where necessary.

3. The GCSC is responsible to the ODESC for formulating and reviewing New Zealand's COMSEC doctrine and standards and for advice on the measures necessary to ensure the effectiveness of COMSEC, including:

    - the security of cryptographic systems, principles and procedures
    - the physical security of cryptographic materials and equipment
    - personnel security standards applicable to cryptographic and allied duties
    - emanations security standards
    - the COMSEC aspects of practices and procedures used in government communications and information systems generally.

Annex C—Terms of Reference: Departmental Committee on Computer Security

1. The Departmental Committee on Computer Security (DCCS) is established as a sub-committee of the Officials Committee for Domestic and External Security Co-ordination (ODESC).

2. The Committee will comprise suitably qualified representatives of NZSIS, NZDF, NZ Police, MFAT, NZ Customs Service and the SSC and is chaired by the Director, GCSB or his/her representative. The Committee may co-opt additional representatives from other government organisations where necessary.

3. The DCCS is responsible to the ODESC for the co-ordination of governmental input into the formulation of national COMPUSEC doctrine and standards to ensure the protection of classified Government information which is:

   - stored and/or processed in government-owned computer systems
   - stored and/or processed in government-controlled private sector computer systems
   - transmitted through data networks.

4. The DCCS will provide a forum for discussion of other matters of national COMPUSEC as ODESC may direct or members may wish to raise.

5. The Chairman of the DCCS is to provide an annual report to ODESC.

Table of Contents

Chapter 2: Security Organisation

Security Structure within Government Organisations

Security Policy Document

1. Management should approve, promulgate and implement a security policy that sets out management's approach and commitment to security.

The policy should:

- state management’s commitment to security
- set out the organisation’s approach to managing security
- include security measures for information systems.

2. The policy's security framework should:
   - be based on robust risk analysis
   - meet the organisation’s operational purpose
   - be practical and useable while providing adequate security
   - be cost effective.

3. The organisation’s security policy should include:
   - general guidance on security roles and responsibilities
   - clear definitions of responsibility for the protection of classified material, whether electronic or hard copy
   - clear definitions of security processes
   - where necessary, more detailed guidance for specific sites, systems or services
   - an ongoing programme of user awareness and education.

4. The policy may be implemented through the organisation’s security instructions. For a suggested outline of security instructions, see Annex A to this Chapter.

5. For additional advice on INFOSEC policy development, see the GCSB publication, *NZSIT 101, Information Technology Security Policy Handbook*.

Review and Evaluation

6. A nominated owner is responsible for maintaining and reviewing the policy according to a defined process.

7. The policy review process should be triggered by any changes affecting the basis of the original risk assessment. For example, after:
    - significant security incidents
    - the introduction of new vulnerabilities
    - changes to the organisational or technical infrastructure.
8. Schedule periodic reviews of:
    - the policy's effectiveness, gauged by the nature, number and impact of recorded security incidents
    - the cost and impact on the policy of controls on efficiency
    - effects on the policy of changes to technology
    - level of user compliance.

Management Security Forum

9. While all members of the management team share responsibility for the security of official information, consider establishing a management security forum. The forum may operate independently or as part of an existing management body. Its purpose is to ensure clear direction and visible management support for security initiatives.
10. The forum should promote security within the organisation through appropriate commitment and adequate resourcing. The forum may:
    - monitor significant changes in the exposure of information to threats
    - review and monitor security incidents
    - review and approve security policy and overall security responsibilities
    - approve major security enhancement initiatives.

Security Co-ordination

11. Make one manager responsible for all security-related activities. In a large organisation, a cross-functional group of management representatives from relevant parts of the organisation may be necessary to co-ordinate security controls.
12. The security manager or management group should:
    - agree on specific roles and responsibilities for security across the organisation
    - agree specific methodologies and processes for security, such as risk-assessment procedures and security-classification systems
    - devise and support organisation-wide security initiatives, such as awareness programmes
    - ensure that security is incorporated into the planning process

- assess and co-ordinate the implementation of specific security controls for new systems or services
- review security incidents and recommend appropriate process improvments
- promote the visibility of business support for security throughout the organisation.

Allocation of Security Responsibilities

13. The security arrangements of government entities should be designed to ensure that government security policy is translated into effective and uniform practice throughout the organisation.

14. Each organisation is required to have a proper security infrastructure with clear allocation of responsibility for all aspects of security. The form of this will depend upon the size of the organisation and the amount of classified material to be handled and protected.

15. Organisations handling a substantial quantity of classified material should establish a specialist security unit. This unit should work in close association with the personnel and administrative staffs to ensure that security requirements are treated appropriately.

16. Where a specialist security unit is not justified the organisation's personnel and administrative staffs are responsible for personnel and physical security. In all cases there should be a clear allocation of responsibilities for security.

17. Overall responsibility for security rests with a manager, designated as Departmental Security Officer (DSO).

18. The DSO is answerable to, and should have free access to, the Chief Executive or Head on security related matters.

19. The DSO should be known to all staff members.

20. Within government organisations, the DSO's responsibilities include:
    - Promulgating and implementing security policy
    - providing guidance in security matters
    - managing and reporting security incidents.

21. The DSO should ensure that senior management, IT staff and system users appreciate the importance of applying and monitoring information system security (INFOSEC). While technological measures lessen many risks, an effective protection system requires all staff to consider INFOSEC measures as part of their day-to-day routine.

Duties of the Departmental Security Officer

22. Under the delegated authority of the Chief Executive or head, the DSO's duties include:

    - formulating and implementing general security policy within the organisation
    - serving as liaison with the Secretary of the ICS, the NZSIS, and the GCSB for any specialist advice
    - applying common minimum standards for security from the ICS
    - issuing instructions on security, and ensuring that the instructions are followed
    - arranging for routine security inspections
    - arranging for security education and training
    - investigating breaches of security.

23. For specific DSO responsibilities, see Annex B to this Chapter.

Education and Training

24. For good protective security, all staff must accept their individual responsibilities to maintain security alertness and adhere to established rules and procedures. This can be achieved through effective ongoing education and training.

25. Since security is a managerial responsibility at all levels, managers should be involved in identifying education and training needs. In particular:

    - managers should ensure that staff understand and comply with all relevant security regulations
    - managers should participate in security training
    - line managers should co-operate fully with the DSO and other security staff to identify education and training needs
    - line managers should ensure that their staff can attend security courses and presentations.

Security Education

26. Security education should:

    - be ongoing
    - be provided for all staff
    - be designed to promote a sense of personal responsibility for effective security, regardless of position, rank, grade or level of access
    - help counter threats through a basic knowledge of security principles.

Security Training

27. Security training should:

    - be provided to staff with specific security responsibilities
    - be designed to impart a sound knowledge and understanding of the organisation's security rules and procedures, appropriate to specific responsibilities
    - provide staff with the knowledge so they can effectively perform their security duties.

28. For details on preparing and implementing an effective security training and education programme, see the NZSIS *Protective Security Manual*.

29. The GCSB offers a range of introductory and specialised courses on INFOSEC topics.

Specialist Security Advice

30. Many organisations require specialist advice on security. Ideally, an experienced in-house security adviser, not necessarily the DSO, can provide this advice. Otherwise, a person should be appointed to co-ordinate in-house security knowledge and experience to ensure consistency in security decision-making.

31. Security advisers should be tasked with providing advice on all aspects of security.

32. Security advisers should have access to suitable external advisers for specialist advice outside their own expertise.

33. Security advisers should have direct access to management, since their assessment of security risks and advice on security controls may determine the effectiveness of the organisation's security policy.

34. Consult the security adviser as soon as possible after a suspected security incident or breach. Although most internal security investigations are carried out under management control, the security adviser may advise, lead or conduct the investigation.

Information Systems Security Manager

35. Organisations with significant information system resources should also appoint an Information Systems Security Manager (ISSM).

36. To oversee a range of technically complex security issues, the ISSM must:

    - understand the structure and architecture of the organisation's information systems
    - have a detailed knowledge of the system's security features, operating systems, access control, and auditing facilities

- be familiar with security strategies in general and INFOSEC in particular
- provide advice on INFOSEC to the DSO
- have ready access to senior management on security issues.

37. Those responsible for INFOSEC in an organisation must also have the authority to enforce information system security policy.

Travel Advice

38. For advice to government employees travelling overseas, see the NZSIS *Protective Security Manual.*

Security Briefings

39. Appropriate security briefings are available for staff visiting or being posted to certain overseas posts. Contact the NZSIS well in advance to allow time for suitable briefing arrangements.

Centre for Critical Infrastructure Protection (CCIP)

40. The Centre for Critical Infrastructure Protection (CCIP) is established within the GCSB to provide advice and support in protecting New Zealand's critical infrastructure from cyber threats. 'Critical infrastructure' is the infrastructure required to provide those services that, if interrupted, would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population and would require immediate reinstatement.

41. The aim of the CCIP is to be a co-ordination point for protection from and reaction to major computer and communications based attacks such as hacking, viruses, and denial-of-service attacks on elements of the critical infrastructure. The CCIP has three main roles:

    - provide 24-hour 7-day 'watch and warn' advice regarding the Internet and critical infrastructure threats and incidents
    - analyse and investigate cyber-threats in order to improve New Zealand's protection
    - assist owners of critical infrastructure to identify and understand their vulnerabilities and to provide advice in protecting critical infrastructure. This includes an outreach programme and facilitation of IT security training.

42. The CCIP has relationships with counterpart organisations overseas, including the National Infrastructure Security Coordination Centre (NISCC) in the UK, the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) in Canada, and the National Infrastructure Protection Center (NIPC) in the United States.

43. Although the CCIP provides advice and support, each organisation is responsible for security of its own systems and services.

Computer Emergency Response Teams

44. There are a number of international Computer Emergency Response Teams (CERTs) that produce advisory notices and alerts detailing vulnerabilities, exploits, and suggested fixes for vendor operating systems and software. It is recommended that organisations subscribe to such a service.

Security Incidents

Reporting Security Incidents

45. Report all personnel, physical, IT and information systems security incidents through appropriate channels as quickly as possible.

46. This may include reporting the circumstances of any contact with people or organisations seeking to obtain information, which they do not have a need to know, through unauthorised means.

47. Establish a formal reporting and incident response procedure.

48. Make all staff aware of their responsibilities and the procedure for reporting security incidents.

49. For advice on actions to be taken following breaches of security, see the NZSIS *Protective Security Manual.*

Reporting Security Weaknesses

50. Staff should be required to note and report any observed or suspected security weaknesses or threats to procedures, policies, systems or services. They should report these matters to the appropriate authority as quickly as possible.

51. Staff should be aware that they should not, in any circumstances, attempt to prove a suspected weakness before reporting. This is for their own protection, as testing weaknesses might be interpreted as a potential misuse of the system.

Learning from Incidents

52. There should be procedures in place to quantify and monitor the types, volumes and costs of incidents and malfunctions. This information should be used to:

    - identify recurring or high-impact incidents or malfunctions
    - indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences
    - inform the security policy review process.

Disciplinary Process

53. There should be a formal disciplinary process for employees who have violated the organisation's security policies and procedures. The disciplinary process can:

    - act as a deterrent to staff who might otherwise be inclined to disregard security procedures
    - ensure correct, fair treatment for staff who are suspected of committing serious or persistent breaches of security.

54. Staff should be made aware of the disciplinary process as part of a security education programme.

Other Security Organisations and Legislation

New Zealand Security Association Inc (NZSA)

55. The NZSA is an independent organisation established to promote a professional security industry. NZSA:

    - sets minimum standards for its members, published in its *Codes of Practice*, which is available to non-members
    - develops security education and training programmes
    - fosters contact with similar international organisations.

56. NZSA members provide a wide range of security services, including advice on the protection of information.

57. Advice from NZSA may be followed as long as it does not conflict with the provisions of Chapter 3 in this manual. For advice on protecting national security information which is classified CONFIDENTIAL and above, consult the NZSIS.

National Supervisory Council for Security Systems (NSCSS)

58. The NSCSS Inc is an independent, non-profit organisation established to raise the standards of intrusion-detection systems in New Zealand. NSCSS aims to ensure that equipment has been tested, approved, and installed safely and correctly. See also Chapter 7 paragraph 21.

NZ Computer Society Special Interest Group on Security (NZCS SigSec)

59. The New Zealand Computer Society's Special Interest Group on Security is a forum for networking with others with an interest in IT security from within and outside Government. It is Wellington-based and meets quarterly for a presentation and networking. For more details contact the Computer Society's Wellington office or go to the NZCS web site, www.nzcs.org.nz.

Government Information Systems Manager's Forum (GOVIS) Security Group

60. The GOVIS Security forum has similar objectives to the NZCS SigSec but is restricted to Government employees only. Meetings are approximately quarterly and there is an e-mail group for posting questions or discussing items of interest. For more details see the GOVIS web site, www.govis.org.nz.

Private Investigators and Security Guards Act 1974

61. The Private Investigators and Security Guards Act 1974 provides for the licensing of security companies and individuals in the commercial security sector. It also defines private investigators and security guards to include anyone who installs, sells or advises on alarm systems, locks or cameras.

62. The licensing procedure requires a Police vetting check. Annual renewals ensure that checks are up to date. Note, however, that the vetting check does not ensure competence.

63. Government departments and agencies, State Owned Enterprises and Crown Entities employing or contracting commercial security companies should verify that the company and the contracting staff are licensed under the act. This can be done either by contacting the PISG Registrar c/- Auckland District Court or by inspecting the relevant certificates.

Annex A—Suggested Outline for Security Instructions

Introduction

Definition of security

The threat, with particular reference to the work of the department

Aims of protective security

Organisation of Protective Security within the Department

Responsibility for security

Security organisation

Security duties

Security education and training

Classification and Markings

The classification system

Importance of correct grading

The classifications

Interpretation of the definitions

Authority to apply classifications

Methods of applying classifications

General rules of classification

The classification of typewriter or printer ribbons

The classification of magnetic and optical storage media

Arrangements for regrading and declassifying

Other endorsement markings

Control of Classified Documents and Similar Material

Objective

The “need to know” principle

Preparation of classified documents

Reference and copy numbers

Page numbering

Accountable documents

The control of TOP SECRET and SECRET documents and files

Removal of classified documents from the premises (including Homeworking)

Spot checks

The “need to retain”

Transmission of Classified Documents and Similar Material

Approved methods of transmission (boxes, pouches, enveloping)

Sealing

Document and package receipts

Movement:

- Within the organisation
- To other government organisations or addresses within New Zealand
- To addresses abroad
- Personal carriage overseas by officials

Electronic transfer

Security of Communications

Rules for passing classified information by telephone, computer, data links, facsimile and any other form of electronic transmission.

Electronic Processing of Classified Information

Rules for the protection and use of:

- information and technology systems
- photocopying machines
- other electronic office equipment.

Storage of Classified Documents

Minimum standards as applied to the department

Destruction

Handling of classified waste

Arrangements for destruction

Records of destruction

Precautions within Buildings

Room security

Precautions against eavesdropping and overview

Dictating machines and tape recorders

Room checks at close of work

Conferences and meetings

Arrangements in secure rooms or areas (if any)

Ancillary staff

Patrol arrangements and duties of patrols

Security of Keys and Combination Lock Settings

Definition of security keys

Compromise—warning

Arrangements for issue and recording of security keys

Safe custody of security keys and duplicates

Replacement of lost keys

Action when security key is lost or compromised

Combination lock settings—security measures

Security of Access Control Devices

Custody of blank cards

Replacement of lost cards

Reprogramming of cards

Changing of combinations

Return of cards

Control of Entry to Departmental Buildings

Control arrangements: staff, visitors, ancillary staff, duties of doorkeepers, receptionists, supervision of cleaners, etc.

Staff responsibility for safeguarding passes

Visitors to secure areas

Identification of staff keeping unusual hours

External Building Security

Site security

Building exterior security

Secure Behaviour

Responsibility of the individual for security

Telephone security

Duty to report known or suspected breaches of security

Disclosure of classified information to persons outside the government service

Social contracts with foreign officials

Personal correspondence

Indiscreet conversations

Overseas travel

Microfilming

Removal of classified documents from the office

Arrangements for taking classified documents to meetings or home

Classified documents in public places

Security Incidents

Management of security incidents

Identification

Reporting

Review and recommendations for improvements

Annex

The security classifications with definitions and examples of the correct use of the classifications based on the work of the department.

Annex B—Specific Responsibilities of the DSO

Personnel Security

1. In consultation with the Chief Executive, determine which posts within the organisation involve access to classified material and what level of security clearance is required for each.

2. Regularly review the list of posts that involve access to classified material.

3. Perform pre-vetting procedures in the organisation.

4. Arrange for the vetting of staff in posts that involve access to classified material.

5. Arrange for the security education of staff doing classified work. Ongoing training should include:

    - the need for protective security
    - the requirements of protective security
    - personal responsibility for security, including the need to report any incident that may have a bearing on security.

6. Advise on the supervision of staff doing classified work.

7. Advise on measures to ensure that security incidents are immediately reported to the Chief Executive or DSO.

8. Arrange for keeping "out of normal hours" attendance records, as needed.

Education and Training

9. Arrange ongoing security training to ensure that staff with specific security responsibilities:

    - have a clearly defined role and function
    - know what organisational and individual resources are available
    - can competently perform the correct security procedures for their current and future responsibilities.

10. The DSO should:

    - identify the organisation's security education and training needs
    - formulate a policy to meet the organisation's security education and training needs
    - brief line managers on security education and training needs and policy
    - supervise the security education and training programme, in agreement with the responsible managers

- liaise with personnel management to identify the security education and training needs of staff, especially new recruits and those taking on new posts and duties
- liaise with security staff to identify their particular education and training needs and carry out programmes to meet those needs
- liaise with the NZSIS on security education and training matters.

Protection of Classified Information

11. In consultation with the appropriate staff, prepare and issue internal instructions for safeguarding classified information and equipment, including:

- the "need to know" principle
- preparation, control, transmission, housing and destruction of classified documents
- restrictions on the use of photocopying machines
- removal of documents from the office
- protection of security keys and combination settings of containers (pouches, satchels, etc.) used for transmitting classified material
- handling of classified waste.

Building Security

- Oversee site security and building exterior security.

Precautions within Buildings

- Secure areas and planning of accommodation from the security standpoint.
- Measures to guard against the risk of eavesdropping and overview.
- Room security and room checks at close of work.
- Visitors to areas where classified information is handled and/or discussed.
- Conferences and meetings.
- Supervision/control of ancillary staff.

Control of Entry to Buildings

- Access control - pass system and control of entry cards and passes.
- Supervision of security staff including issue of instructions to security guards and door control staff.
- Inspections including night visits of security guards.
- Physical obstacles to prevent unauthorised entry, such as: doors, locks, windows, skylights, ducts, fencing, vehicle barriers, and outer perimeter lighting.

- Formulation of security procedures in event of emergency.

Communications and Electronic Processing of Classified Information

12. Prepare and issue internal guidelines on the use of:
    - office equipment
    - data processing equipment
    - communications systems for processing and/or transmitting classified information.
13. Oversee all communications and computer security arrangements. Specifically:
    - liaise with the COMSEC officer and communications staff, to ensure that communications equipment and systems are procured and used in accordance with National COMSEC standards
    - advise staff on the security of telephone conversations
    - create computer security practices for the organisation
    - advise users of personal computers, word processors and electronic or electric typewriters on the special precautions required to process classified information.

Security Instructions

14. Prepare security instructions for the organisation.
15. Prepare security notes for staff doing classified work.

Security Inspections

16. Inspect personnel, physical and document security. Include checks on entry, pass and document control.

Breaches of Security

17. Arrange to be informed of all breaches of security.
18. Maintain records of all breaches of security.
19. Ensure that breaches of security are brought to the attention of those concerned.
20. Ensure action is taken to investigate, minimise damage done and prevent recurrence.

Table of Contents

Chapter 3: Information Classification

Classified Material

1. For this manual, “classified material” means:
    - classified information in hard copy
    - classified information in electronic form
    - classified equipment.

Inventory of Classified Material

2. Compiling an inventory of classified information and equipment is an important part of risk management. The level of protection required is determined by the importance of the material in the inventory.

3. Generally, the value of material matches its security classification. However, some material without a security classification may have value in terms of time, cost or effort in replacing if lost or corrupted.

Classification Guidelines

General

4. “Official information” is any information developed, received or collected by or on behalf of the Government. As a valuable official resource, official information must be:
    - handled carefully, according to authorised procedures
    - made available only to people who have a legitimate “need to know”, to fulfil their official duties
    - released only in accordance with the policies, legislative requirements and directives of the Government and the courts.

Official Information Act

5. The system of classification for the protection of official information is based on:
    - the Official Information Act 1982
    - the principle that official information should be made available to the public unless there are good reasons to withhold it.

6. Classifications alone do not justify withholding official information. All requests for information, regardless of classification, must be considered using the criteria in the Official Information Act 1982.

7. Information that does not need to be classified is referred to as “unclassified”.

8. Generally, staff must not disclose or make use of information unless authorised by:
    - the Official Information Act 1982, for official information
    - the Privacy Act 1990, for personal information.

Purpose of Classification

9. A security classification specifies how people must protect the information and equipment that they handle. The classification system limits access to that information and equipment through a series of procedural and/or physical barriers.

10. In general, information to be protected is either:
    - **"Policy and Privacy"** information, for which compromise does not threaten the security of the nation, but rather the security or interests of individuals, groups, commercial entities, government business and the community.
    - **"National Security"** information, for which compromise could affect the security or defence of New Zealand or the international relations of the Government of New Zealand.

11. Other, unclassified official information may still need protection and management. For example, information hosted on government websites especially needs protection and management to assure authenticity and prevent tampering.

Security Classifications

12. The security classification system for government organisations follows the Cabinet decision of December 2000[1]. The guidelines are not prescriptive—they are to help classify material, based on risk assessment of how much damage or prejudice would result from compromising specific content. For more information on risk assessment as part of security risk management, see the NZSIS *Protective Security Manual*.

Policy and Privacy Information

13. Security classifications for material that needs to be protected because of public interest or personal privacy are:
    - IN CONFIDENCE (see Annex A to this Chapter)
    - SENSITIVE (see Annex B to this Chapter).

[1] CAB(00) M42/4G(4)

National Security Information

14. Security classifications for material that needs to be protected because of national security are:

    - RESTRICTED (see Annex C to this Chapter)
    - CONFIDENTIAL (see Annex D to this Chapter)
    - SECRET (see Annex E to this Chapter)
    - TOP SECRET (see Annex F to this Chapter).

Endorsement Markings

15. Endorsement markings may be used along with security classifications to identify protected information. Endorsement markings may indicate:

    - the specific nature of information
    - temporary sensitivities
    - limitations on availability
    - how recipients should handle or disclose information.

16. Use endorsement markings only when there is a clear need for special care. For a list of standard endorsements and their meanings, see Annex G to this Chapter.

Authority to Classify

17. Chief Executives and heads of government departments and agencies, State Owned Enterprises and Crown Entities are vested with the authority to classify material using the approved classifications.

18. Chief Executives and heads may delegate authority to classify to senior staff, but sparingly. In particular, only appropriate senior staff should be given authority to classify material SECRET or TOP SECRET. It is important to avoid unwarranted application of these classifications by less experienced staff.

Importance of Correct Classification

19. Selecting the most appropriate classification is critical because:

    - under-classifying can have the direct and obvious consequences of inadequately protected material
    - over-classifying can mean unnecessary, expensive protection for material and loss of properly classified material among improperly classified material.

20. Over-classifying may stem from:

    - genuine doubt about the classification prescriptions
    - personal uncertainty
    - a tendency to play safe.

Guidance to Staff

21. The most effective measure to prevent over-classification is issuing detailed guidance on the correct use of classifications.

22. Each organisation should supplement the standard definitions with up-to-date examples of the correct and incorrect use of classifications, drawn from its own field of activity. The definitions of the security classifications together with the examples should be given to all staff who classify information.

23. Security training should stress the importance of selecting the most appropriate classification. Staff should be reminded that the likely damage caused by unauthorised disclosure is included in the definition of a classification.

Measures to Reduce Over-Classification

24. Where appropriate and practical, organisations should:

    - encourage staff to challenge questionable classifications
    - have line managers check classifications routinely
    - in security instructions, clearly define how the Chief Executive or head delegates authority for classification
    - in complex documents such as books, reports, memoranda or minutes of meetings, separately classify each chapter, section, page or paragraph; this can be indicated by inserting the appropriate classification in parentheses immediately following the section or paragraph number or in the sideline if unnumbered
    - avoid rules for automatic classification, as they can result in documents bearing classifications higher than warranted.

Classification of Committee Papers

25. The following general principles apply to the classification of committee papers:

    - classification of papers is the responsibility of the chairperson
    - each item of the minutes and each paper should be classified according to their contents.

Classifications Originating Overseas

26. The New Zealand Government has international obligations and statutory responsibilities to maintain the security of classified material received from allies, friendly nations and international organisations. Material must be classified at a level not less than that in force in the country or organisation of origin.

27. To help identify overseas information when the source is not obvious on the document, the recipient should annotate the document with the country of origin.

28. When using classified information from another country or an international organisation to create new information, safeguard it to a level equal to or greater than that applied by the originator. To ensure appropriate protection, annotate such documents to show that they contain classified information originating from external sources.

Classifications Originating Outside the Organisation

29. Upon receiving classified information from another organisation within New Zealand, safeguard it to a level equal to or greater than that applied by the originator.

Downgrading Classifications

30. Organisations should institute systems of review for downgrading classified material. This especially applies to material in current use. The security instructions for material should include details about downgrading.

31. Adopt the following broad principles:

    - concentrate on recent documents, which may be still current
    - after use, return material classified SECRET or TOP SECRET to the point of origin
    - for authority to downgrade or declassify, refer material classified SECRET or TOP SECRET to the point of origin
    - destroy or declassify surplus classified material.

32. Before deciding to declassify any documents, media or equipment, assess the risk of disclosure.

33. Consider the following steps:

    - automatically downgrade information that becomes generally known after an event such as operations, moves, conferences, constitutional changes or visits
    - review accumulated material for downgrade, or destroy surplus material that is not required for records, after an operation or sequence of events
    - review files, media and contents for regrading when they are taken out of or brought back into current use
    - review accountable documents for regrading when they are mustered for periodical checks
    - review technical or scientific reports for regrading when they are over five years old, or some other specified period.

Annex A—Management of Material Classified as IN CONFIDENCE

IN CONFIDENCE	Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens.
Guidelines:	• Prejudice the maintenance of law, including the prevention, investigation and detection of offences, and the right to a fair trial. • Affect adversely the privacy of natural persons, including that of deceased natural persons. • Disclose a trade secret or unreasonably to prejudice the commercial position of the person who supplied or is the subject of the information. • Disclose information which is subject to an obligation of confidence or which any person has been or could be compelled to provide under the authority of any enactment, where the making available of the information would be likely to prejudice the supply of similar information, or information from the same source, and it is in the public interest that such information should continue to be supplied; or be likely otherwise to damage the public interest. • Prejudice measures protecting the health or safety of members of the public. • Prejudice the substantial economic interests of New Zealand. • Prejudice measures that prevent or mitigate material loss to members of the public. • Breach the constitutional conventions for the time being which protect: the confidentiality of communications by or with the Sovereign or Her representative; collective and individual ministerial responsibility; the political neutrality of officials; and the confidentiality of advice tendered by ministers of the Crown and officials. • Impede the effective conduct of public affairs through: the free and frank expression of opinion by or between or to Ministers of the Crown or officers and employees of any department or organisation in the course of their duty; the protection of such Ministers, officers and employees from improper pressure or harassment. • Breach legal professional privilege. • Impede a Minister of the Crown or any Department or organisation holding the information to carry out, without prejudice or disadvantage, commercial activities. • Lead to the disclosure or use of official information for improper gain or advantage.

Principles and Clearance Levels	• Information for official use, with consideration of "need to know" principle. *Note: Information held internally by an organisation that is classified IN CONFIDENCE might not always be labelled as such. It should be so marked, however, whenever it is passed outside the organisation to ensure that it is afforded appropriate protection.*
Electronic Transmission	• An appropriate statement should accompany all IN CONFIDENCE information transmitted via e-mail or fax. • It should outline legal responsibilities and notification/destruction instructions if the incorrect party receives it. • IN CONFIDENCE data can be transmitted across external or public networks but the level of information contained should be assessed before using clear text. • Username/Password access control and/or encryption may be advisable (with the aim of maintaining public confidence in public agencies). • All IN CONFIDENCE information (including data) should clearly identify the originating government agency and date.
Electronic Storage	• Electronic files (including databases) should be protected against illicit internal use or intrusion by external parties through two or more of the following mechanisms: • user challenge and authentication (username/password or digital ID/Certificate) • logging use at level of individual • firewalls and intrusion-detection systems and procedures; • server authentication • OS-specific/application-specific security measures.
Electronic Disposal	• Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Manual Transmission	• May be carried by ordinary postal service or commercial courier firm as well as mail delivery staff in a single closed envelope[2]. • The envelope must clearly show a return address in case delivery is unsuccessful. In some cases involving privacy concerns, identifying the originating department may be inappropriate and a return PO Box alone should be used.

[2] Where there is a concern that the envelope may be opened by a person not authorised to access the material, for example in a registry, it may be prudent to double envelope the material with the inner envelope addressed to an individual by name and title and indicating that it contains material with an IN CONFIDENCE classification.

Manual Storage	• IN CONFIDENCE information can be secured using the normal building security and door-swipe card systems that aim simply to keep the public out of administrative areas of government departments.
Manual Disposal	• Disposed of by departmental arrangements.

Annex B—Management of Material Classified as SENSITIVE

SENSITIVE	Compromise of information would be likely to damage the interests of New Zealand or endanger the safety of its citizens.
Guidelines:	• Endanger the safety of any person. • Damage seriously the economy of New Zealand by disclosing prematurely decisions to change or continue Government economic or financial policies relating to: – exchange rates or the control of overseas exchange transactions – the regulation of banking or credit – taxation – the stability, control, and adjustment of prices of goods and services, rents and other costs, and rates of wages, salaries and other incomes – the borrowing of money by the Government of New Zealand – the entering into of overseas trade agreements. • Impede a Minister of the Crown or a department organisation holding the information to carry on without prejudice or disadvantage, negotiations (including commercial and industrial negotiations).
Principles and Clearance Levels	• Information classified as SENSITIVE should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the department to access SENSITIVE level or above are authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	• All SENSITIVE information transmitted across public networks within New Zealand or across any networks overseas must by encrypted using a system approved by the GCSB.
Electronic Storage	• Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: – user challenge and authentication (username/password or digital ID/Certificate) – logging use at level of individual – firewalls and intrusion-detection systems and procedures; server authentication – OS-specific/application-specific security measures.

Electronic Disposal	• Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Manual Transmission	• **Within a single physical location**. As determined by the Chief Executive or Head of the organisation. • **Transfer between establishments within or outside New Zealand.** – May be carried by ordinary postal service or commercial courier firms, provided the envelope/package is closed and the word SENSITIVE is not visible. – The outer envelope should be addressed to an individual by name and title. SENSITIVE mail for/from overseas posts should be carried by diplomatic airfreight through MFAT. – The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.
Manual Storage	• In an office environment, SENSITIVE material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	• Disposed of or destroyed in a way that makes reconstruction highly unlikely.

Annex C—Management of Material Classified as RESTRICTED

RESTRICTED	Compromise of information would be likely to affect the national interests in an adverse manner.
Guidelines:	• Affect diplomatic relations adversely. • Hinder the operational effectiveness or security of New Zealand or friendly forces. • Affect the internal stability or economic well-being of New Zealand or friendly countries adversely.
Principles and Clearance Levels	• Information classified as RESTRICTED should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the department to access RESTRICTED level or above is authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	• All RESTRICTED information transmitted across public networks within New Zealand or across any networks overseas must be encrypted using a system approved by the GCSB.
Electronic Storage	• Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: – user challenge and authentication (username/password or digital ID/Certificate) – logging use at level of individual – firewalls and intrusion-detection systems and procedures; server authentication – OS-specific/application-specific security measures.
Electronic Disposal	• Electronic files should be disposed of in a way that makes reconstruction highly unlikely.

Manual Transmission	• **Within a single physical location**. As determined by the Chief Executive or Head of the organisation. • **Transfer between establishments within or outside New Zealand.** – May be carried by ordinary postal service or commercial courier firms, provided the envelope/package[3] is closed and the word RESTRICTED is not visible. – The outer envelope should be addressed to an individual by name and title. RESTRICTED mail for/from overseas posts should be carried by diplomatic airfreight via MFAT. – The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating department may be inappropriate and a return PO Box alone should be used.
Manual Storage	• In an office environment, RESTRICTED material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	• Disposed of or destroyed in a way that makes reconstruction highly unlikely.

3. Where there is a concern that the envelope may be opened by a person not authorised to access the material, for example in a registry, it may be prudent to double envelope the material with the inner envelope addressed to an individual by name and title and indicating that it contains material with a SENSITIVE classification.

Annex D—Management of Material Classified as CONFIDENTIAL

CONFIDENTIAL	Compromise of information would damage national interests in a significant manner.
Guidelines:	• Materially damage diplomatic relations (ie cause formal protest or other sanctions). • Cause damage to the operational effectiveness or security of New Zealand or friendly forces or to the continuing effectiveness of valuable security or intelligence operations. • Damage the internal stability of New Zealand or friendly countries. • Disrupt significant national infrastructure.
Principles and Clearance Levels	• Information classified as CONFIDENTIAL must be held, processed, transmitted and destroyed with levels of security commensurate with the significant damage to national interest that compromise would incur. • Only staff cleared by the department for CONFIDENTIAL access or above is authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	• All CONFIDENTIAL information transmitted across any networks within New Zealand or overseas must be encrypted using a system approved by the GCSB.
Electronic Storage	• Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: – user challenge and authentication (username/password or digital ID/Certificate) – logging use at level of individual – firewalls and intrusion-detection systems and procedures; server authentication – OS-specific/application-specific security measures.
Electronic Disposal	• Media that has held CONFIDENTIAL information must be declassified by degaussing, overwriting or destroying iaw GCSB guidelines contained in *NZSIT 207*.

Manual Transmission	• **Within a single physical location.** Single opaque envelope that indicates the classification, with a receipt at the discretion of the originator, and either: – despatched through a department's own transit system; or – distributed within a building or part of a building that has been declared a specially protected area; otherwise – must be double enveloped and sealed with approved seals in accordance with Chapter 4 paragraph 104 and carried by authorised messengers. • **Transfer between establishments within New Zealand.** CONFIDENTIAL material should be double enveloped and sealed with approved seals in accordance with Chapter 4 paragraph 104 and: – carried by an authorised messenger or safe-hand courier with "By Hand" stamped on the outer envelope; or – where no authorised messenger or safe-hand courier service exists CONFIDENTIAL material may be sent by registered post[4]. In this case, receipts must be obtained. • **Transfer between establishments outside New Zealand.** CONFIDENTIAL material must be double enveloped with "By Hand" stamped on the outer envelope and sealed with approved seals in accordance with Chapter 4 paragraph 104 with a receipt form included inside the inner envelope and: – carried by the Diplomatic safe-hand bag service operated by MFAT to or between posts; or – where no safe-hand courier service exists material may be sent by registered post within Australia, Canada and the United States of America between New Zealand posts situated in respective countries; or – in exceptional circumstances CONFIDENTIAL material may be transmitted by registered mail between New Zealand diplomatic posts or other New Zealand agencies situated in the United Kingdom, Canada, Australia and the United States of America, or by Diplomatic air freight bag between MFAT and New Zealand official missions in Niue and Tarawa. For further advice contact NZSIS.
	• **COMSEC material.** To be handled in accordance with procedures advised by GCSB from time to time.

4. NZ Post will deliver registered post to a physical address only, not a PO Box or Private Bag.

Manual Storage	• Must be locked in an approved security container when not in use. See Chapter 7 paragraph 54. • The minimum acceptable storage arrangements are a combination of the protection afforded by the security container itself, the position or site and the use of approved security equipment.
Manual Disposal	• If accountable, the destruction should be recorded by marking the record of accountable documents or the file index sheet where these are used. See Chapter 4 paragraph 68. • Destroy by burning, pulping, shredding or dry maceration.

Annex E—Management of Material Classified as SECRET

SECRET	Compromise of information would damage national interests in a serious manner.
Guidelines:	• Raise international tension. • Damage seriously relations with friendly governments. • Cause serious damage to the operational effectiveness or security of New Zealand or friendly forces or the effectiveness of valuable security or intelligence operations. • Seriously damage the internal stability of New Zealand or friendly countries. • Shut down or substantially disrupt significant national infrastructure.
Principles and Clearance Levels	• Information classified as SECRET must be held, processed, transmitted and destroyed with levels of security commensurate with the serious damage to national interest that compromise would incur. • Only staff cleared by the department for SECRET access or above are authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	• All SECRET information transmitted across any network within New Zealand or overseas must be encrypted using a system approved by the GCSB.
Electronic Storage	• Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: – user challenge and authentication (username/password or digital ID/Certificate) – logging use at level of individual – firewalls and intrusion-detection systems and procedures; server authentication – OS-specific/application-specific security measures.
Electronic Disposal	• Media that has held SECRET information must be declassified by degaussing, overwriting or destroying iaw GCSB guidelines contained in *NZSIT 207*.

Manual Transmission	• **Within a single physical location.** Material should be double enveloped and sealed with approved seals in accordance with Chapter 4 paragraph 104 and: – despatched through a department's own transit system with hand-to-hand receipts at each stage of the journey; or – distributed within a building or part of a building that has been declared a specially protected area; otherwise – carried by authorised messengers. • **Transfer between establishments within New Zealand.** SECRET material should be double enveloped with "By Hand" stamped on the outer envelope and sealed with approved seals in accordance with Chapter 4 paragraph 104 and carried by an authorised messenger or safe-hand courier. • **Transfer between establishments outside New Zealand.** SECRET material must be double enveloped with "By Hand" stamped on the outer envelope and sealed with approved seals in accordance with Chapter 4 paragraph 104 with a receipt form included inside the inner envelope and carried by the Diplomatic safe-hand bag service operated by MFAT. • **COMSEC material.** To be handled in accordance with procedures advised by GCSB from time to time.
Manual Storage	• Must be locked in an approved security container when not in use. See Chapter 7 paragraph 54. • The minimum acceptable storage arrangements are a combination of the protection afforded by the security container itself, the position or site and the use of approved security equipment.
Manual Disposal	• If accountable the destruction should be recorded by marking the record of accountable documents or the file index sheet where these are used. See Chapter 4 paragraph 68. • Destroy by burning, pulping, shredding or dry maceration.

Annex F—Management of Material Classified as TOP SECRET

TOP SECRET	Compromise of information would damage national interests in an exceptionally grave manner.
Guidelines:	• Threaten directly the internal stability of New Zealand or friendly countries. • Lead directly to widespread loss of life. • Cause exceptionally grave damage to the operational effectiveness or security of New Zealand or friendly forces or the effectiveness of extremely valuable security or intelligence operations. • Cause exceptionally grave damage to relations with other governments. • Cause severe long-term damage to significant national infrastructure.
Principles and Clearance Levels	• Information classified as TOP SECRET must be held, processed, transmitted and destroyed with levels of security commensurate with the exceptionally grave damage to national interest that compromise would incur. • Only staff cleared by the department for TOP SECRET access is authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	• All TOP SECRET information transmitted across any network within New Zealand or overseas must be encrypted using a system approved by the GCSB.
Electronic Storage	• Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: – user challenge and authentication (username/password or digital ID/Certificate) – logging use at level of individual – firewalls and intrusion-detection systems and procedures server authentication OS specific/application-specific security measures
Reproduction	• TOP SECRET documents should only by photocopied on the written request of an authorised employee. The photocopying of TOP SECRET documents must be recorded, showing the subject, reference number, number of copies made and authority for copying.
Electronic Disposal	• Media that has held TOP SECRET information cannot be declassified and must be destroyed in accordance with GCSB guidelines contained in *NZSIT 207*.

Manual Transmission	• **Within a single physical location.** Material should be double enveloped with "By Hand" stamped on the outer envelope and sealed with approved seals in accordance with Chapter 4 paragraph 104 and: – despatched through a department's own transit system with hand-to-hand receipts at each stage of the journey; or – distributed within a building or part of a building that has been declared a specially protected area; otherwise – carried by authorised messengers within an approved circulating box or pouch. • **Transfer between establishments within New Zealand.** TOP SECRET material should be double enveloped with "By Hand" stamped on the outer envelope and sealed with approved seals in accordance with Chapter 4 paragraph 104 and carried by an authorised messenger or safe-hand courier. • **Transfer between establishments outside New Zealand.** TOP SECRET material must be double enveloped and sealed with approved seals in accordance with Chapter 4 paragraph 104 with a receipt form included inside the inner envelope and carried by the Diplomatic safe-hand bag service operated by MFAT. • **COMSEC material.** To be handled in accordance with procedures advised by GCSB from time to time.
Manual Storage	• Must be locked in an approved security container when not in use. See Chapter 7 paragraph 54. • The minimum acceptable storage arrangements are a combination of the protection afforded by the security container itself, the position or site and the use of approved security equipment.
Manual Disposal	• Before destruction all pages and enclosures must be verified as present. • The destruction must be supervised and witnessed and should be recorded by filing a note of destruction in the place of the document or by marking the relevant entry on the file index sheet where these are authorised. See Chapter 4 paragraph 68. • Destroy by burning, pulping, shredding or dry maceration.

Annex G—Endorsements that may be Applied with any Security Classification

Appointments	Actual or potential appointments that have not yet been announced and the deliberation during the recommendation/approval process
Budget	Proposed or actual measures for the Budget prior to their announcement by the Treasurer
Cabinet	Contains material which will be presented to, and/or, require decisions by, Cabinet or Cabinet Committee
Commercial	Sensitive commercial processes, negotiations of affairs
Evaluative	Material relating to competitive evaluations such as interview records and tender assessments
Honours	The actual or potential award of an honour before the announcement of the award and the deliberations during the recommendation/approval process or the consideration of honours policy matters involving the exercise of the Royal prerogative
Medical	Medical reports, records and other material related to them
Staff	References to named or identifiable staff. Also for use by staff in entrusting personal confidences to management
Policy	Proposals for new or changed government policy before publication
New Zealand Eyes Only	This material is not to be viewed by any person who is not a New Zealand national
[Department(s)] Use Only	For use only within the specified department(s)
Addressee Only	Material that is only to be seen by the person to whom it is addressed
Embargoed for Release	Prior to the designation time at which an announcement will be made, an address made or information will be disseminated
To be Reviewed on	A designated time at which the classification of the information is to be reviewed

Table of Contents

Chapter 4: Control of Classified Material

General

1. Classified material must be controlled to:
   - prevent unauthorised and improper access
   - assist investigations into any breach of security
   - reinforce the "need to know" principle.

2. Control is best maintained by an orderly system of paper keeping. This lets an organisation know:
   - what classified material it has
   - where it should be found
   - whether it is where it should be
   - who has or had access to it.

3. For one organisation to entrust its classified material to another, confident that it will be protected the same way, there must be a common standard of control.

"Need to Know" Principle

4. Fundamental to all aspects of security is that the only people who receive classified information are those who need it to complete the business in hand. Thus, employees receive access to classified information:
   - only because they "need to know" it to complete their duties
   - not because it would be convenient for them to know
   - not by virtue of their status, position, rank or level of authorised access.

5. Adherence to the "need to know" principle helps protect the employee as well as the classified material.

6. The "need to know" principle applies both within an organisation and when dealing with people outside it.

7. If in any doubt whether or not a proposed recipient is authorised for access to a particular classification, staff must consult their supervisor or the DSO.

8. Security briefings and security education should make staff fully aware of their personal responsibility to apply the "need to know" principle.

9. Standard distribution lists are a useful aid in applying the "need to know" principle. Government organisations should keep the number of recipients on a distribution list and the number of copies distributed to a minimum.

10. The distribution of SECRET and TOP SECRET material should be strictly controlled under arrangements clearly defined in the organisation's security instructions.

11. Avoid including unnecessary, classified information in widely distributed documents. When a highly classified document covers a number of topics, produce it in sections if possible, so that the whole document is not distributed to those concerned with only part of it.

12. Carefully control the issue of classified documents from registries and libraries, on a "need to know" basis.

"Need to Retain" Principle

13. Only retain classified documents, especially circulated drafts, while they are in use. Once a classified document or draft is no longer needed, either return it to the originator or destroy it.

14. Security instructions on the "need to retain" principle should include:

    - keeping all holdings of loose classified material to a minimum
    - annual reviews of holdings of loose classified material
    - how to return or dispose of unneeded classified material
    - regular, for example six-monthly, reviews of all holdings of TOP SECRET material, to find what can be returned or destroyed
    - storing TOP SECRET or SECRET documents, that need to be retained long-term, in numbered or otherwise identifiable folders, subject to the minimum control and storage standards for their classification.

15. For classified committee papers, also consider:

    - staff with no direct interest in or need to retain copies should return them to the originator as soon as possible
    - staff or branches of organisations with access to master sets, held in registries or in the original master record, should surrender spare copies
    - committee secretaries should set a maximum period for retaining copies and advise committee members to return or destroy them when the period is over.

Workplace Procedures

Working in Secure Zones

16. Within the same building, different levels of security may be needed. Consider concentrating offices doing classified work in a separate, secure zone.

17. Allow only authorised personnel into secure zones.

18. Different levels of security may be needed within a secure zone. Consider barriers to control physical access between areas with different security needs.

19. For more advice on physical protection for secure zones, see Chapter 7 of this manual, and the NZSIS *Protective Security Manual*.

Room Security

20. During normal working hours, if classified documents are not protected in locked security containers, individual staff and their supervisors are responsible for ensuring that the documents cannot be read, handled or removed by unauthorised personnel.

21. Chief Executives and heads of government departments and agencies, State Owned Enterprises and Crown Entities must decide how to protect material that is classified IN CONFIDENCE, SENSITIVE or RESTRICTED in their organisation.

22. All material classified CONFIDENTIAL or above should be secured whenever not in use.

23. Material classified CONFIDENTIAL or above, including classified waste, should be locked in security containers whenever a room in a secure zone is unoccupied for over thirty minutes or as detailed in the organisation's security instructions.

24. Lock doors and close and secure windows when a room in a secure zone is unoccupied for less than the time specified in paragraph 23 and the classified material is not secured.

25. Make sure that all classified documents cannot be read from outside the room.

26. When cleaners or other ancillary staff may have access to a secure room, lock away all classified material when the room is unoccupied.

27. The need to protect material such as internal telephone directories varies by organisation and is at the discretion of the Chief Executive or head.

Open-Plan Offices

28. It may be hard to enforce "need to know" procedures in open-plan offices. Before working on classified material in open-plan offices, take precautions to prevent overlooking and eavesdropping by unauthorised people. Pay particular attention to the location of discussion areas and equipment such as computer monitors, printers, photocopiers and other reprographic systems.

Overhearing and Eavesdropping

29. Under normal working conditions, ordinary speech is not intelligible beyond a range of 15 metres; although in exceptionally quiet conditions, or where building structural anomalies or technical aids could conduct sound waves, the range may be greater.

30. In considering the risk of overhearing (as distinct from eavesdropping by technical means) in "sensitive" rooms, note any sounds that may mask speech.

31. The risk of overhearing is obviously greater when windows are open, especially at or close to ground level.

32. Avoid dictating TOP SECRET material. Dictation is more easily overheard than ordinary conversation. Take special precautions with dictation to prevent overhearing or eavesdropping.

33. Consult the GCSB if the organisation has concerns about overhearing or eavesdropping.

Overviewing from Adjacent Buildings

34. Telephotography can be used to photograph documents from any position at an angle greater than 15 degrees above horizontal. The effective range depends on the equipment used and the environmental conditions.

35. Consider all windows of rooms used for classified work as vulnerable to telephotography. Net curtains or opaque glass may provide protection, but this may be compromised by artificial light. To be safe, draw all curtains and blinds, including venetian blinds.

36. Consult the NZSIS if the organisation has concerns about overviewing.

Ancillary Staff

37. Just because ancillary staff (such as guards, receptionists, cleaners, maintenance workers, or canteen staff) are security vetted does not mean that physical security measures and the "need to know" principle are no longer necessary.

38. Use protective measures and security education to prevent ancillary staff from accessing classified material or overhearing discussions involving classified matters.

Clear Desk and Clear Screen Policy

39. Consider adopting:

    - a clear desk policy for papers and removable storage media
    - a clear screen policy for information processing facilities.

40. A clear desk and clear screen policy will greatly reduce the risk of unauthorised access, loss of, or damage to information. The policy should take into account security classifications and the organisation's risk assessment.

41. Apply the following guidelines:

- Where appropriate, store paper and computer media in suitable containers when not in use, even during working hours.
- Lock away classified material when not needed, especially when the office is unoccupied.
- Log off personal computers, computer terminals and printers when unattended.
- Protect personal computers, computer terminals and printers by key locks, passwords or other controls when not in use.
- Protect incoming and outgoing mail points and unattended fax and telex machines.
- Lock photocopiers outside of normal working hours (or protect from unauthorised use in some other way).
- Clear classified information from printers immediately.

End of Day Procedures

42. Line managers should be responsible for developing and implementing adequate procedures to protect classified material outside of working hours. This could include having all rooms checked at the end of the working day.

Identification of Staff Keeping Unusual Hours

43. Organisations holding classified material should keep a record of staff leaving the office late or coming in at unusual hours. Record the name of the employee, their branch and time of entry or departure.

44. Each organisation should decide what constitutes “working late” or “unusual hours”. Generally, an hour and a half before or after normal working hours or any time on days the office is closed for normal business may be considered “unusual hours”.

45. This record will help protect against unauthorised copying or removal of classified material, and will also protect the employee. While there may not be anything sinister in an employee working unusual hours, line managers and the DSO ought to know which staff members make a habit of this.

46. If an employee with access to classified material is regularly keeping unusual hours for no obvious reason, the DSO should make discreet inquiries to find out why. If no satisfactory reason is found, consult the NZSIS.

Removal of Classified Material from the Office

47. Classified material should only be removed from the office when:

- the material is needed for a declared purpose
- the employee removing the material has specific permission.

48. For specific requirements for storage and transmission of classified material, see Chapter 3 Annexes A to F.

Homeworking

49. Some organisations may have staff who work on official and classified information from home. For guidance on the security aspects of homeworking, see the NZSIS *Protective Security Manual*.

Conference Security

50. Guidelines on security at conferences, see the NZSIS *Protective Security Manual*.

Information Preparation and Handling

General

51. To protect classified information, an effective system of control is essential. Such a system must allow government organisations to know:

- what classified material is held
- what level of protection it needs
- where it is held
- who is authorised to see or use it; and, at the higher levels of classification, who has had access to or has used it in the past.

52. The system of control should apply to the following aspects of handling information:

- preparation
- marking
- registration and filing
- copying
- custody review
- spot checks
- microform
- destruction.

Preparation

53. Classified documents must be handled—prepared, copied, delivered, etc.—only by authorised personnel. Regularly review security arrangements for production and copying. Consider the following:

    - establish separate production and copying facilities for classified documents
    - number copies as they are produced or copied
    - as soon as possible, dispose of spoilt copies as classified waste
    - hold spare copies in secure storage, and dispose of as classified waste as soon as it is clear that they are surplus and no longer needed
    - familiarise staff with precautions against unauthorised use of reproduction equipment such as photocopiers, printers and facsimiles; this includes making only the authorised number of copies
    - make sure that instructions for handling, destroying and disposing of classified material are specific, practical and effective.

54. Treat the following as classified documents:

    - cylinders
    - discs
    - tapes
    - shorthand notebooks
    - preliminary sketches
    - working notes or sketches
    - photographs
    - negatives
    - stencils
    - carbon papers
    - all magnetic and optical storage media used to record classified material.

55. Script on a cotton typewriter or printer ribbon is sometimes legible until typed over four or five times. Nylon ribbons are more resistant to indentation. While elaborate precautions with ribbons used to type classified documents are not necessary, consider the following:

- remove used ribbons before typewriters or printers are sent for repair
- treat single-use ribbons, such as acetate and other ribbons on certain makes of electric typewriters, as classified, consistent with the level of classification used on the typed document
- remove ribbons after working hours and whenever not in use; store accordingly; and destroy as classified waste as soon as they are completely used
- use similar procedures for correcting tape.

56. Print or stamp security classifications on documents clearly and distinctively, in the centre of the top and bottom of each page.

57. Colour coding makes it easy to identify classifications; and higher classifications clearly stand out. The accepted colour coding is:

- TOP SECRET: red
- SECRET: blue
- CONFIDENTIAL: green
- RESTRICTED, SENSITIVE and IN CONFIDENCE: black

58. When classification markings must be typed or printed in the same lettering as the text, consider using:

- wider spacing
- distinctive boxes
- underlining.

59. Print or stamp the overall classification of non-permanently bound books or files in the centre of the top and bottom of:

- the front and back covers
- the title page.

60. Classify all subsequent pages and insertions, such as maps, photographs or drawings, according to their contents.

61. For magnetic media, such as floppy discs, and optical storage media, such as CD-ROMs and DVDs, clearly and prominently mark the highest security classification on both the front of the disc and on its case.

62. For guidance on marking other classified material such as books, maps and films, see the NZSIS *Protective Security Manual*.

Registration

63. For documents classified higher than RESTRICTED, include a reference to the originator and the date of origin.

64. For documents issued in a series, such as committee papers, include a sequential number, to make it obvious when one is missing.

65. For documents classified CONFIDENTIAL and above, include page numbers.

66. For TOP SECRET and SECRET documents, include page numbers and total number of pages, to make it easy to check for completeness.

67. For TOP SECRET and SECRET documents in wide circulation, number each copy. This helps to record distribution and narrow investigation if necessary.

Making Documents "Accountable"

68. When a classified document is made "accountable", its holder must check and certify its safe custody at stated intervals, normally every six months.

69. All TOP SECRET documents must be accountable.

70. The originator of a document determines:

    - whether it is accountable (if lower than TOP SECRET)
    - marks that distinguish it as accountable
    - frequency of checking and certifying.

Minimum Standards for Controlling TOP SECRET and SECRET Material

71. The minimum standards for controlling TOP SECRET and SECRET material are:

    - record its location on preparation, arrival into the organisation, in use and in storage
    - record its disposal or destruction
    - keep these records for at least five years.

72. For further guidance on controlling TOP SECRET and SECRET material, see the NZSIS *Protective Security Manual*.

Automated Document Accounting Systems (ADAS)

73. ADAS may be used in place of manual systems to account for classified material. Computerising a manual system does not in itself enhance security. However, an ADAS may:

    - increase security awareness
    - tighten security
    - improve efficiency as part of a larger electronic office project.

74. For further information on ADAS systems, see the NZSIS *Protective Security Manual*.

Copying, Printing and Facsimile Machines

75. To prevent unauthorised use, strictly control access to copying machines and printers, including microfilming equipment, and facsimile machines that are not protected by COMSEC systems.

76. Control depends on the circumstances and types of machines. When a machine is used to copy or print substantial quantities of classified material, control its use during working hours and immobilise it at all other times.

77. For guidance on additional control measures, including those to be taken when repairing or disposing of reprographic machinery, see the NZSIS *Protective Security Manual*.

Laptop Computers

78. See Chapter 9.

Custody

79. Only registry staff should issue classified files and return them to registries.

80. If a classified file is passed directly to another person in an emergency, the person passing the file should:

    - inform registry staff as soon as possible
    - inform their supervisor or an appropriate superior why it was necessary to pass the file directly.

81. Return all classified files not under current action to the appropriate registry.

Review

82. In addition to routine document destruction, organisations should periodically hold special destruction exercises. These exercises should:

    - ruthlessly cull unwanted copies of classified documents, especially when master sets or originals exist, for example at head office
    - take care, however, not to destroy original documents of historical value (see paragraph 126).

Spot Checks

83. Spot checks deter taking TOP SECRET and SECRET documents out of the office for unauthorised purposes.

84. Line managers should carry out spot checks:

    - without warning
    - at frequent but irregular intervals
    - during normal working hours.

85. To prevent spot checks from degenerating to a tiresome chore:

    - check only TOP SECRET and SECRET documents
    - check only a few documents at a time.

86. For further advice on spot checks, see the NZSIS *Protective Security Manual*.

Microform

87. Classified documents may be recorded on microfilm, microfiche or microform, as long as:

    - information is recorded by persons cleared to access it
    - reproductions are subject to the same security procedures as the originals
    - continuous reels of recorded material are classified according to the highest classification they contain
    - classified documents that are subject to special security procedures are recorded separately
    - when continuous reels contain both TOP SECRET and lower-classified documents, steps are taken to safeguard the TOP SECRET documents when people without access to them are viewing the lower-classified material.

Custody of Classified Material

General

88. Chief Executives or heads of government departments and agencies, State Owned Enterprises and Crown Entities determine the security arrangements for storing IN CONFIDENCE, SENSITIVE and RESTRICTED material.

89. CONFIDENTIAL, SECRET and TOP SECRET material must be locked in security containers when not in use.

90. CONFIDENTIAL, SECRET and TOP SECRET material should not be stored together with UNCLASSIFIED material.

91. IN CONFIDENCE, SENSITIVE and RESTRICTED material may be stored together with UNCLASSIFIED material.

92. When storing material of different classifications together, use the security standard of the highest-classified item.

Minimum Standards for Holding Material Classified CONFIDENTIAL or Above

93. Minimum standards for holding material classified CONFIDENTIAL have been established. They are based on:

    - the security container and its lock
    - the position or site of the container
    - the use of approved security equipment.

94. For more on the relationships between security classifications, container sites, container groups and categories of locks and the list of approved equipments, see the NZSIS *Protective Security Manual*.

Transporting Classified Material

95. During transit, classified material is at risk from accidental or deliberate compromise.

96. To protect classified material when in transit:

    - use reliable means of transport
    - use robust packaging
    - conceal the attractiveness, identity and source of the material, under plain cover.

97. With higher levels of classification, use an audit system to track the material and reveal any actual or attempted tampering.

98. Protect classified material in transit:

- within and between sites and establishments in New Zealand
- between New Zealand and countries overseas
- within and between countries overseas.

Overseas Safe Hand Service

99. Most official material sent to, from, and between New Zealand government posts overseas is handled by the diplomatic mail service controlled and operated by MFAT. This service provides for:

- the regular dispatch of classified material by diplomatic safe hand bag in the care of a diplomatic courier
- the regular dispatch of unclassified material by unaccompanied diplomatic airfreight bag.

100. If classified material must be transferred overseas, seek advice from MFAT on how best to send it.

Commercial Postal and Courier Services

101. Material classified up to CONFIDENTIAL may be carried by commercial courier or post within New Zealand as long as the originators find the risk of compromise acceptable. Use the packaging and sealing provisions in Chapter 3 Annexes A to D.

102. Material classified SECRET must not be posted. It may be carried, only within New Zealand, by a commercial courier who is approved for the purpose by NZSIS. The courier must be contracted to follow procedures outlined in NZSIS *Protective Security Manual.*

103. Material classified TOP SECRET must not be posted nor carried by commercial courier under any circumstances.

Minimum Requirements for Transmission and Transport

Level	Classified Information	Classified Equipment
IN CONFIDENCE	Handle, use and transmit with care. See Chapter 3 Annex A.	Control, use and transport with care.
SENSITIVE or RESTRICTED	Handle, use and transmit with care. Take basic precautions against accidental compromise or opportunist attack. See Chapter 3 Annex B and C.	Control, use and transport with care. Take basic precautions against accidental compromise or opportunist attack.
CONFIDENTIAL	Handle, use and transmit to make accidental and deliberate compromise unlikely. Where possible, make actual or attempted compromise unlikely. Where possible, make actual or attempted compromise likely to be detected. See Chapter 3 Annex D.	Control, use and transport to make accidental compromise unlikely. Offer a degree of resistance to deliberate compromise. Control knowledge of planned movements. Make actual or attempted compromise likely to be detected.
SECRET	Handle, use and transmit to minimise the chance of accidental compromise. Offer a degree of resistance to deliberate compromise by a professional attack. Where possible, detect actual or attempted compromise and help identify those responsible. See Chapter 3 Annex E.	Control, use and transport to minimise the possibility of accidental compromise. Offer a degree of resistance to deliberate compromise by a professional attack. Limit knowledge of planned movements. Detect actual or attempted compromise and help identify those responsible.

Level	Classified Information	Classified Equipment
TOP SECRET	Handle, use and transmit to prevent accidental compromise. Offer a degree of resistance to compromise by a sustained and sophisticated attack. Where possible, detect actual or attempted compromise and make it likely that those responsible will be identified. See Chapter 3 Annex F.	Control, use and transport with every possible precaution against accidental damage. Offer a degree of resistance to deliberate compromise by a sustained and sophisticated attack. Strictly limit knowledge of planned movements to those with a "need to know". Detect actual or attempted compromise and make it likely that those responsible will be identified.

Tamper-Evident Seals, Tapes and Envelopes

104. Envelopes containing classified documents for distribution outside a specially protected area must be adequately sealed. For details on currently approved sealing material and methods, see the NZSIS *Protective Security Manual*.

Mechanical Document Transfer Systems (MDT)

105. MDT systems use rails, tracks or pneumatic tubes to carry documents within and between buildings. Before installing an MDT system, assess the security implications for each site.

106. For more about MDT systems, see the NZSIS *Protective Security Manual*.

Destruction of Classified Material

107. Until classified material has been reduced to a state where it cannot be read or reconstituted, it retains its classification. Procedures for handling, recording, transmitting, and destroying classified waste are the same as for any material with that classification.

108. For more about types and standards of destruction, see the NZSIS *Protective Security Manual*.

Record of Destruction

109. Keep a record of the destruction of TOP SECRET and accountable documents.

110. Some organisations may also wish to keep a record of the destruction of certain other classified documents or material.

111. Records of destruction should include:

- the date
- the signature of the person carrying out the destruction
- the authority for the destruction
- for TOP SECRET material, the signature of a second witness to the destruction.

112. Before destroying any file, folder or document, first verify that all TOP SECRET and accountable pages and enclosures are present and complete.

113. Record the destruction of individual TOP SECRET items in files by:

- filing a note of the destruction in place of the document
- marking the relevant entry in the file index sheet.

114. Record the destruction of unfiled TOP SECRET documents by marking the relevant entry in the incoming-document record.

115. Record the destruction of accountable documents by marking their records.

116. Record the destruction of TOP SECRET files/folders by marking their indexes. The destruction of each TOP SECRET document in a file/folder does not have to be separately recorded.

117. For documents bearing an endorsement marking, take care to follow relevant instructions.

118. Certain categories of documents may not be destroyed by the holder, but instead must be returned to the originator or appropriate controller for destruction.

119. Retain records of the destruction of TOP SECRET material for as long as possible—as a general rule, aim for at least five years.

Minimum Requirements for Destruction

120. Classified waste is a potential source of information. Before it is destroyed, hold it in an appropriate container, separate from other waste. Security controls adopted by organisations for classified waste must meet the following levels:

Level	Classified Information	Classified Equipment
IN CONFIDENCE	Make compromise highly unlikely	Dispose of with care to make compromise highly unlikely
SENSITIVE or RESTRICTED	Make reconstruction highly unlikely	Dispose of with care or destroy to make reconstitution unlikely
CONFIDENTIAL	Make retrieval and reconstitution unlikely. Make actual or attempted compromise likely to be detected.	Make retrieval and reconstitution highly unlikely. Make actual or attempted compromise likely to be detected.
SECRET	Make retrieval or reconstruction highly unlikely. Detect actual or attempted compromise and help identify those responsible.	Make reconstitution highly unlikely. Prevent identification of constituent parts. Detect actual or attempted compromise and help identify those responsible.
TOP SECRET	Do everything necessary to: • prevent retrieval or reconstitution • detect actual or attempted compromise and make it likely that those responsible will be identified	Do everything necessary to: • prevent reconstitution • detect actual or attempted compromise and make it likely that those responsible will be identified

Methods of Destruction

121. However material is destroyed, it should done by or under the strict supervision of a staff member with appropriate security clearance. The responsible staff member should:

    - accompany the material to the point of destruction
    - ensure that destruction is complete
    - give or witness a destruction certificate, as necessary.

122. Before destruction, all tapes, discs and similar magnetic and optical storage media which have been used to record classified information should be erased.

123. For details on approved methods of destruction of classified documents and other material, see the NZSIS *Protective Security Manual*.

124. For advice on the destruction of magnetic and electronic media, see the GCSB's *NZSIT 207, Declassification of Storage Media*.

Emergency Destruction

125. Although a need to plan for emergency destruction of classified material may appear unlikely, such a possibility should not be ignored. Where appropriate, consider the following contingency precautions:

    - Keep highly classified material in storage to an absolute minimum. Unless there is an essential need to retain it, consider destroying classified material when action on it is complete.
    - Establish an order of priorities for destruction. Keep the list in a location that staff know and can access without delay in an emergency.
    - Prepare a plan that uses all available destruction equipment. Periodically check that the equipment is serviceable and that staff know how to operate it.
    - Consider alternative destruction facilities in the event of power failure. For example, adapt paper shredders for manual operation or use an emergency incinerator.

National Archives

126. The Archives Act 1957:

- establishes a repository known as the National Archives
- transfers to the National Archives all "public archives"—public records, with certain exceptions, at least 25 years old, no longer in use, and worthy of permanent preservation
- lets the minister of a government organisation defer transfer of classified records
- lets an organisation make conditions on public archives transferred to the National Archives, including how they can be accessed
- requires the Chief Archivist (not the organisations) to authorise destroying records that are no longer useful to the organisation and not valuable enough to warrant their continued preservation.

127. Before transferring papers to the National Archives, an organisation normally subjects them to a process of scrutiny. This may include seeking help from the Chief Archivist. If the Chief Executive or head of the organisation holding the records agrees, the Chief Archivist or a duly delegated and suitably security-cleared representative may inspect classified records.

128. Records transferred to the National Archives may be withheld from the public because:

- the organisation that transferred them wants public access restricted; in this case, a person may request access to the records from the organisation, under the provisions of the Official Information Act 1982
- the Minister of Internal Affairs has directed the Chief Archivist to withhold access to a record or class of record, to satisfy the public policy of the New Zealand Government or that of another country
- the record is in a specified class of records transferred from the New Zealand Police or the Ministry of Justice, which require written authorisation from the respective minister
- the record is fragile or undergoing description, repair or other treatment.

Table of Contents

Chapter 5: Personnel Security

1. Personnel security has three major elements, which depend on or complement one another:

   - personnel screening, for suitability for employment in government departments or agencies where there is routine access to official information
   - granting specific authority to access official and classified material or sensitive sites
   - the security clearance system.

Security in Job Definition and Resourcing

Security in Job Descriptions

2. Security roles and responsibilities should be defined in the organisation's security policy and stated in job descriptions. The job descriptions should explain:

   - general responsibilities to implement or maintain security policy
   - specific responsibilities to protect official information.

Management Responsibilities

3. Managers' responsibilities should include:

   - ensuring that official information is protected
   - ensuring that there are appropriate levels of assurance about the trustworthiness of people whose posts require access to, knowledge of or custody of classified material
   - consulting line managers when post-holders change or the security clearances are due for review about whether the levels of assurance, or security clearances, are still required.

Terms and Conditions of Employment

4. Terms and conditions of employment should include:

   - the employee's responsibility for information security
   - action to be taken if the employee disregards security requirements
   - the employee's legal rights and responsibilities.

5. Where appropriate, these responsibilities should continue for a defined period after employment ends.

Confidentiality Agreements

6. Confidentiality and non-disclosure agreements, signed by employees as part of their terms and conditions of employment, can specify the need to protect information.

7. Casual staff and third-party users, not already covered by a contract that includes the confidentiality agreement, may be required to sign a confidentiality agreement before being given access to official information.

Personnel Screening

8. When a person is first employed, transferred or promoted, and the new job requires access to official information, the organisation must determine whether the initial appointment checks provide enough assurance that the employee can be entrusted with that information.

9. Screening does not, on its own, provide a guarantee of integrity and trustworthiness. Since individuals and their circumstances change, personnel screening is only as good as the investigations done at the time.

10. Personnel security must continue after initial approval. Any new information or concerns that may affect an employee's reliability must be advised promptly to the appropriate authority. Continuing personnel security includes after-care and review.

Pre-Employment Checking

11. When a person applies for a permanent staff position, checks should include:

    - the availability of satisfactory character referees
    - the completeness and accuracy of the curriculum vitae, including qualifications.

12. When a candidate is selected, but not yet appointed, additional checks should be conducted:

    - confirmation of both identity and character through referees
    - a criminal history check with either NZ Police or the Department for Courts.

13. Temporary staff should be similarly checked. When temporary staff come through an agency, the agency contracts should clearly specify responsibilities for screening, and for notification procedures to be followed if screening is not complete or reveals cause for concern.

Authority to Access

14. Access to some official information is needed for most government jobs. Chief Executives or heads would normally obtain sufficient assurance about their permanent staff through:

    - pre-employment checks
    - periodic reviews
    - approval procedures
    - sound terms and conditions of employment.

15. The "need to know" rule must still apply.

Access to "Sensitive" Sites

16. Some sites are "sensitive" because of the type, quantity and level of material handled or stored or discussed there. Examples include defence establishments, police stations and the parliamentary complex. There may be a higher chance of staff or visitors having indirect or inadvertent exposure to classified information or equipment.

17. The organisation controlling the site makes the decision to grant regular access. It is usually effected by the issue of a pass or access or identity card.

18. A "Basic Check" may give a level of assurance, beyond that of normal pre-employment checking, about staff or contractors who require regular access to sensitive sites.

Basic Check

19. The subject of a basic check must be informed that it is to be done. The originating organisation then:

    - arranges a criminal history check through Police or Courts, unless one has already been completed within the last 12 months
    - forwards a request to the NZSIS for checking against NZSIS records, after the criminal history check is complete.

20. The NZSIS response to a basic check will be endorsed on the original request as a marking to the effect of either:

    - "No Comment" or
    - "Separate Reply to Follow", which means the written response to be provided later will be qualified or adverse, or more information is required.

21. NZSIS will not, except in rare circumstances, refer to or base a qualified or adverse response on a candidate's criminal history or other information which is already known to the originating organisation.

22. Basic checks should be repeated every five years.

23. A basic check is not needed and should not be requested unless the staff member or contractor does not have a security clearance and needs regular access to sensitive sites. The granting of access after a basic check is not a "security clearance".

24. For more on basic checks, see the NZSIS *Protective Security Manual.*

Access to Classified Material

25. Access to all classified material must be governed by the "need to know" rule.

26. The management of organisations decide which of their staff and contractors can access RESTRICTED, SENSITIVE and IN CONFIDENCE material. The granting of such access is not a "security clearance". The decision should be based on the employee's:

    - suitability for employment
    - any relevant performance assessments
    - records of conduct.

27. Staff who need regular access to CONFIDENTIAL or higher national security material must be granted an appropriate security clearance from the Chief Executive or head of the organisation.

Security Vetting Procedures

28. Decisions to grant security clearances for access to higher level national security material are based at least in part on the outcome of the vetting process. It includes various checks and inquiries into the suitability of the staff member to have such access.

Legal Aspects to the Security Vetting Procedure

29. The Privacy Act 1993 exempts NZSIS from certain of its principles. NZSIS is entitled to collect personal information not only from vetting candidates themselves, but also from other people and organisations. Such disclosures by others of personal information about the candidate are not a breach of the Act.

30. Both the Privacy Act and the Official Information Act 1982 allow NZSIS to refuse to disclose, even to candidates, personal information which is evaluative material, if its disclosure would breach an undertaking of confidence. The information provided by referees is protected from disclosure.

31. The Human Rights Act 1993 recognises that for work involving national security, sometimes factors must be considered that might otherwise be discriminatory. The prohibition on discriminating in employment on the grounds listed below does not apply to employment in the area of national security:

    - religious or ethical belief
    - political opinion
    - psychiatric illness
    - intellectual or psychological disability
    - particular marriage partners or relatives, and
    - national origin.

32. Further, where a person is under age 20, it is not a breach of the Act to decline employment on the grounds of age if the work requires a high level security clearance.

33. However, it remains unlawful to discriminate on the grounds of:

    - sex
    - sexual orientation
    - age other than as outlined above
    - colour
    - race
    - physical disability or
    - marital status.

Assessment of Required Security Clearance Levels

34. The security clearance vetting system must not be used by departments or agencies as a general character or trustworthiness check for current or potential employees.

35. Security clearances are required only for regular access to national security information classified CONFIDENTIAL or higher. They are not required for access to RESTRICTED material, or Policy and Privacy information classified SENSITIVE or IN CONFIDENCE.

36. Before starting the security vetting process, organisations should review what level if any of security clearance is needed for a particular job or individual.

37. Clearances match the classification of material to be regularly accessed. However, in an operational emergency, chief executives may authorise staff to access national security material classified above their current clearance. There are strict limits on this "emergency access".

38. For further guidelines on assessing security clearance requirements and emergency access, see the NZSIS *Protective Security Manual*.

Guidelines for Assessing Trustworthiness

39. A Chief Executive or head should not appoint or maintain people in posts with access to classified material unless satisfied that they are trustworthy. The decision should take into account a number of variables which make up the whole person. Available and reliable information, past and present, favourable and unfavourable, should be considered.

40. For detailed guidelines, see the NZSIS *Protective Security Manual.*

Pre-Vetting

41. After determining a person's need to access particular levels of classified material, there are several steps an organisation must take before forwarding a vetting request to NZSIS. These include checks to ensure that personal data is complete and accurate and that other relevant information has been considered.

42. If pre-vetting procedures reveal that an employee is unsuitable for access to classified material, the process should stop without a vetting request being forwarded to NZSIS.

43. For more advice on pre-vetting procedures, see the NZSIS *Protective Security Manual.*

Levels of Vetting and Clearances

44. Vetting and the resulting security clearances are on an escalating scale: the breadth, depth, time and resources for inquiries, assessment and recommendation increase significantly for each step up the scale. The higher the level of clearance sought, the more intrusive on privacy is the information requested of the candidate and the inquiries made. Care must be taken that the level of clearance sought is justified by the access needed.

45. To begin the vetting process, the originating department arranges for the candidate to complete the appropriate vetting form. The candidate must declare that the information given is true and complete, and acknowledge that any false statement or deliberate omission may be grounds to deny a security clearance.

46. The candidate must also consent, on a separate form, to the Police or other people or organisations disclosing personal information to the NZSIS.

47. Before forwarding the request to NZSIS, the DSO checks the candidate's form to confirm:

    - the need for a clearance
    - the level of clearance needed
    - all relevant information known to the originating department is provided.

48. The type of inquiries that NZSIS makes depends on the level of vetting:

    - for lower levels of clearance, candidates and their immediate family are checked against police criminal history and criminal intelligence records, and NZSIS records
    - for higher levels of clearance, candidates must provide additional personal information and nominate referees to complete a questionnaire or be personally interviewed
    - for the highest levels of clearance, credit checks are done.

49. Sometimes the NZSIS will need to interview additional non-nominated referees or the candidates themselves.

50. For details about security clearance vetting procedures, see the NZSIS *Protective Security Manual.*

Referees

51. The most common causes of difficulty and delay in completing vetting inquiries are the non-availability or unsuitability of referees nominated by the candidate. Referees:

    - must have close personal knowledge of the candidate's private life and have had contact within the last 12 months
    - must not be related to the candidate or to each other
    - should be, if possible, from the candidate's own peer or age group
    - preferably should not be listed elsewhere on the vetting request form (for example, flatmates)
    - should include at most two work colleagues or professional acquaintances, and then only if they are also well-acquainted with the candidate outside work
    - must be resident in New Zealand, unless there are exceptional circumstances
    - should preferably be New Zealand citizens
    - should be contactable for at least six weeks after the form is forwarded to the NZSIS.

Adverse or Qualified Replies

52. At the end of vetting, NZSIS forwards a reply to the originating department. If the reply includes an adverse or qualified recommendation, wherever possible reasons are provided.

Decision on Granting Security Clearances

53. The departmental head or Chief Executive considers the NZSIS vetting report and all other relevant information, both favourable and unfavourable, to form an opinion as to whether a candidate can be entrusted with access to classified material. The decision must be based on knowledge of the candidate at the time, and in relation to the specific position.

54. The decision should be conservative. If there are any grounds for concern, the Chief Executive must be satisfied that there are overriding reasons to grant the clearance. See the NZSIS *Protective Security Manual*.

55. The test of suitability escalates according to the level of clearance sought.

56. If a clearance is declined, or granted at a lower level, or with qualifying conditions, based in whole or in part on the NZSIS reply, the candidate should be told. Candidates should also be advised of their right to complain to the Inspector General of Intelligence and Security if they consider they have been adversely affected by any act, omission, practice, policy or procedure of the NZSIS.

57. The NZSIS must be advised when less than a full clearance is granted, or if a security clearance is declined or withdrawn.

Records of Security Clearances

58. Departments and agencies are responsible for maintaining records of security clearances issued to their staff and contractors.

59. Organisations should establish a reliable "bring up" system so that clearances do not lapse.

Lapses and Transfers of Security Clearances

60. A security clearance lapses after five years or when the holder leaves the organisation that granted it.

61. When an employee with a clearance transfers to another government organisation, the Chief Executive of the new organisation may grant a new clearance at the same or lower level, without further vetting, if:

    - the previous clearance is less than 12 months old, and
    - the employee's duties, for which access is required, are broadly comparable to those of the position in the previous organisation.

62. When transferring a clearance, the expiry date of the new clearance should be made the same as that of the original clearance from the former organisation.

63. For advice about confirming original clearance expiry dates and other information relevant to security clearance transfers, consult the NZSIS.

After-Care and Review

64. Personnel security should continue after initial access or security clearance is approved.

65. Any new information or concerns about a person's reliability must be brought to the attention of the appropriate authority. This requires after-care and review procedures to be in place.

66. Effective personnel security depends on the support of line managers who have an ongoing responsibility to maintain standards for protecting classified material under their control, and to brief staff about those standards.

67. Line managers should be alert to potential difficulties or conflicts of interest among staff. They should report any concerns as soon as possible to the appropriate authority.

68. Effective measures also require close co-operation between the departmental security and personnel branches, including the welfare section, to ensure that information about issues of possible security concern is passed to the DSO or security branch.

69. For more information, see the NZSIS *Protective Security Manual.*

Reviews of Security Clearances

70. A security clearance reflects only that a person was considered suitable to have access to classified material at the time of the vetting. It is no guarantee of continuing suitability. Security clearances are subject to review:

    - if there is a change in the employee's personal circumstances; for example, a new relationship
    - if the employee turns 20 years old, after having been granted a clearance under special circumstances
    - at the end of a term specified when it was granted
    - every five years in all cases.

71. Organisations should begin review procedures at least three months before clearance expires.

72. When a clearance expires, the entire pre-vetting and vetting process is repeated. Since one of the assessment criteria is consistency with known or previously supplied information, there can be no reliance on personal information already "on file." New vetting forms must be submitted, with full details supplied in all areas.

Table of Contents

Chapter 6: Contractors and Other Third-Party Access

Assessment of Risk from Third-Party Access

Types of Access

1. Access given to people outside the parent organisation deserves special attention, including:

    - physical access, for example to offices, computer rooms or filing cabinets
    - logical access, for example to an organisation's databases or information systems across a network connection.

Reasons for Access

2. Physical or logical access may be granted access to off-site providers for several reasons, including the need for:

    - trading or joint-venture partners to exchange information, access information systems or share databases
    - hardware and software support staff to access system or low-level application functionality.

3. Third-party access may put information at risk without adequate security management. Where there is a business need for third-party access, a risk assessment should be carried out first to see what controls are needed. The assessment should consider:

    - types of access needed
    - value of the information
    - controls used by the third party
    - implications of access on the organisation's information security.

Protection of Classified Material

4. The contracted parties must use appropriate security controls, approved by the contracting organisation, to protect classified material from deliberate or accidental compromise. Such arrangements should ensure:

    - information or equipment used are at no greater risk than if handled by the organisation's own employees
    - minimum standards outlined in Chapter 3 of this manual are maintained.

On-Site Contractors

5. Security weaknesses may arise from on-site, temporary, third-party contractors, such as:
    - consultants
    - cleaning, catering, security guards and other outsourced support services
    - hardware and software maintenance and support staff
    - student placement
    - other casual, short-term appointments.
6. If contractors are engaged for any purpose, consider whether they need a security clearance for the information they use or the areas they access.
7. Unless contractors need to access classified material, the Chief Executive or head can usually decide their level of access based on:
    - reference checks
    - employment history checks
    - criminal history checks through Department for Courts or NZ Police
    - basic checks (see Chapter 5).
8. If a security clearance is needed, the contracting organisation should initiate the clearance process.
9. Pre-vetting procedures should still be followed as closely as possible.
10. The contract with the third party should include security requirements (see paragraph 25). For example, non-disclosure agreements should be considered to help maintain confidentiality.
11. Third parties must not have access to classified material or information-processing facilities until:
    - appropriate checks are complete
    - security clearances are granted
    - contracts, defining the terms for connection or access, are signed.

Off-Site Contractors

12. With some contract work for government organisations, non-government contractors hold or produce classified information or equipment on their own premises.

13. Contracts from government organisations must specify that the contractor protects both classified and unclassified official information, following the levels outlined in Chapter 3 of this manual. The contracting organisation must decide how best to ensure that contractors know their responsibilities.

14. Where material classified CONFIDENTIAL must be released off-site, security arrangements are best managed by the contracting organisation. Security responsibilities should be clear and reinforced by formal or legal means such as contractual conditions.

15. Depending on its complexity, the contracting organisation may wish to seek security advice from the NZSIS and/or GCSB.

16. For contracts involving classified equipment, the contracting organisation should consider separating and directly controlling the classified aspects of the work.

17. Only the minimum quantity of classified equipment should leave government control, and only then with access limited to people with a “need to know”.

Consultants

18. Often consultants work for government organisations under the terms of a specific contract. But sometimes consultants receive no direct pay from the contracting organisation, other than travel and subsistence payments; so security is not enforced by Standard Conditions of Contract.

19. When there is no direct contract, government organisations must draw up appropriate terms and conditions of appointment. These should detail the consultant’s personal responsibilities for safeguarding classified material.

20. Consultants accessing material classified CONFIDENTIAL or above must receive written guidance on the relevant security controls and procedures.

21. Before a consultant receives classified material, the DSO of the government department or agency, State Owned Enterprise or Crown Entity must ensure that :

    - the consultant is appropriately authorised
    - where necessary, the consultant holds the appropriate level of clearance
    - security measures are in place to ensure the material’s physical protection.

Outsourcing

22. When the management or control of all or some of its information systems, networks or desktop environments is outsourced, security should be outlined in a contract agreed between the parties. For example, the contract should specify:

    - how to meet legal requirements, such as data-protection legislation
    - how to ensure that all parties, including subcontractors, know their security responsibilities
    - how to maintain and test the integrity and confidentiality of operations
    - what physical and logical controls restrict and limit access to the organisation's classified and business information
    - what levels of physical security are provided for outsourced equipment
    - the right of audit.

23. The contract should allow for expanded security requirements and procedures, based on a security management plan agreed by both parties.

24. Outsourcing contracts can pose some complex security questions. A good starting point for the structure and content of a security management plan is the controls outlined in *AS/NZS ISO/IEC 17799:2001 Information Technology—Code of Practice for Information Security Management*.

Security Requirements in Third-Party Contracts

25. Third-party access to a government organisation's information-processing facilities should be detailed in a formal contract.

26. The contract should contain or cite all requirements for complying with the organisation's security policies and standards.

27. The contract should ensure that there is no misunderstanding between the organisation and the third party. Consider putting these terms in the contract:

    - the general policy on information security
    - protection, including:
        - steps to protect official information, equipment and software
        - steps to determine whether information or data has been compromised (for example, lost or modified)
        - controls to ensure that information and equipment is returned or destroyed at a specified time after or during the contract
        - integrity and availability
        - restrictions on copying and disclosing information.
    - a description of each service offered
    - the target level of service

- unacceptable levels of service
- provision for transferring staff as appropriate
- the respective liabilities of parties to the agreement
- legal responsibilities, for example based on data-protection legislation, especially considering different national legal systems if foreign organisations are involved
- intellectual property rights (IPRs), copyright assignment and protection of any collaborative work
- control-of-access agreements to information systems, covering:
  - permitted access methods
  - the control and use of unique identifiers such as user IDs and passwords
  - an authorisation process for user access and privileges
  - an ongoing, accurate list of authorised users, specifying their rights and privileges
  - clearly defined and verifiable performance criteria, and steps for monitoring and reporting those criteria
  - the right to monitor and if necessary revoke user access
  - the right to audit or have third parties audit contractual responsibilities
  - an escalation process for problem resolution, including contingency arrangements where appropriate
  - responsibilities for installing and maintaining hardware and software
  - a clear reporting structure and agreed reporting formats
  - a clearly defined process of change management
  - physical protection controls, and mechanisms to enforce those controls
  - user and administrator training in methods, procedures and security
  - controls to protect against malicious software
  - arrangements for reporting, notifying and investigating security incidents and breaches
  - terms for third-party subcontractors.

28. People working for contractors, subcontractors and other organisations outside government have a duty of confidentiality when they are involved in handling classified or unclassified government information.

29. The duty to respect confidentiality must be clearly communicated, preferably by confidentiality agreements or contractual conditions. Contractors and subcontractors in particular should be told that their involvement in government contracts might increase the risk of their businesses being targeted for security incidents.

Table of Contents

Chapter 7: Physical and Environmental Security

"Defence in Depth"

1. Risk management allows flexibility through various levels of protection against unauthorised access to classified material.

2. Protective security uses a multi-layered approach, known as "defence in depth". Defence in depth means combining several measures to make unauthorised access difficult for an external intruder or an employee who does not "need to know". These measures should complement and support one another. They may control:

   - physical space
   - procedures
   - personnel
   - technology.

3. Physical security measures must be designed to meet the threat to security posed by the ill-intentioned person who already has authority to enter the site, building or secure zone, rather than the intruder from outside.

4. The main physical defences are those nearest the protected information. In a government organisation with much classified material, other precautions may be needed for "defence in depth" or to guard against human error. Precautions may include:

   - security keys and containers to protect classified information
   - access control measures
   - security alarm systems to detect unauthorised access and alert a response
   - physical barriers to deter, detect and delay unauthorised entry.

5. Physical measures may be complemented by procedural and personnel measures such as:

   - the "need to know" principle, limiting access to official information to people who require it to carry out their duties
   - a security classification system that identifies material that needs special protection
   - a personnel security system that ensures appropriate approval or clearance for access to official material
   - logical controls which minimise security risks to departmental IT systems
   - education or training programme.

Security Awareness

6. Good security must include the co-operation of staff who fully know their responsibilities. Managers and staff should receive security education to meet their individual responsibilities and needs.

7. For specialist advice on security awareness training, consult the NZSIS.

Planning Accommodation

8. Careful planning of the layout within a site, building or secure zone can reduce security vulnerabilities and costs.

9. For guidance on security aspects of accommodation planning, see the NZSIS *Protective Security Manual*.

Physical Security Perimeter

10. Physical protection can come from establishing several security perimeters around facilities storing classified material. A security perimeter is any physical barrier such as a wall, card-controlled entry or staffed reception desk.

11. A risk assessment will help decide the location, strength and nature of each barrier.

12. A perimeter may be:

    - natural boundaries
    - fences or walls
    - the outer walls of a building
    - divisions within a building.

13. The purpose of a perimeter is to physically, psychologically or legally deter intruders.

14. Perimeter security may be enhanced by:

    - perimeter intrusion-detection systems (PIDS)
    - security lighting
    - closed-circuit television (CCTV)
    - security guards
    - warning signs and notices.

15. For guidelines see the NZSIS *Protective Security Manual.*

Storage Facilities

16. Facilities for the storage of classified material may comprise sites containing a number of buildings, buildings standing alone or secure zones within buildings.

Surveys

17. Facilities that will store classified material should be surveyed for securing all possible means of access, including:

    - all entrances
    - ground-floor or accessible windows
    - skylights
    - personnel inspection covers and the like.

18. Surveys should be repeated at frequent intervals, preferably every 12 months or when its use or the threat level changes.

19. For guidance on securing building exteriors, see the NZSIS *Protective Security Manual.*

Security Assessment

20. In assessing security risks, facilities are rated by level of resistance to forced and surreptitious attack. The ratings are:

    - Grade I—specially designed structural barriers that deny unauthorised entry outside normal working hours
    - Grade II—structural barriers that deter unauthorised entry outside normal working hours
    - Grade III—standard building material and hardware that provide limited security.

21. Assessments should also consider security threats from neighbouring premises.

22. Facilities used to process or store classified material should:

    - be unobtrusive
    - have minimum indication of purpose
    - have no obvious signs either outside or inside suggesting the presence of classified material.

General Design Features

23. Facilities that store or process classified material should have as few access points as safety and the functions of the site allow.

24. Access points should have physical security controls such as:

    - window bars
    - grilles
    - shutters
    - security doors.

25. Controls may be enhanced by intrusion-detection systems, CCTV or guard services.

26. For more to consider when assessing security risks and appropriate countermeasures see the NZSIS *Protective Security Manual.*

Intrusion-Detection Systems

27. Intrusion-detection systems (IDS) are designed to detect actual or attempted unauthorised entry, identify its location and signal a response with an alarm. IDS can:

    - provide continuous surveillance over secure areas
    - extend coverage into areas not usually accessible to guards.

28. When selecting, installing and using IDS, take care to avoid the possibility of:

    - intruders circumventing the system
    - technical problems
    - excessive false alarms.

29. Organisations considering an IDS for areas with national security material classified CONFIDENTIAL or above must consult the guidelines in the NZSIS *Protective Security Manual.* Seek advice from NZSIS if in doubt about any aspect of a system or its installation.

Non-Governmental Standards and Agencies

30. Two New Zealand Standards and one non-governmental agency directly address intrusion-detection systems:

    - NZS 4301:Part 1:1993 Intruder Alarm Systems—applies to systems installed in client's premises, including systems which comply with occupancy class 4—national and corporate security

- NZS 4301:Part 3:1993 Intruder Alarm Systems—applies to detection devices for internal use
- National Supervisory Council for Security Systems (NSCSS)—applies to devices of any occupational class, including class 4—national and corporate security, approved by NSCSS (see Chapter 2 paragraph 58).

31. Systems or devices which comply with these standards are not approved to protect national security material classified CONFIDENTIAL or above (see paragraph 29). However, for protection of official information classified RESTRICTED or SENSITIVE and below, NSCSS approved IDS may be considered to provide a level of assurance that other systems may not provide.

Physical Entry Controls

32. Secure areas should be protected from unauthorised access by controls such as:
    - authentication controls, such as card plus PIN, to authorise and validate entry to areas with classified information, including information-processing facilities
    - a securely maintained audit trail of access
    - some form of visible identification worn by all staff
    - a policy of challenging unescorted strangers and anyone not wearing identification
    - regular review and update of access rights to secure areas
    - controls for visitors:
        - supervision or clearance for specific, authorised purposes
        - instructions on emergency procedures and security requirements
        - recording their date and time of entry and departure.

33. For more detail on using physical entry control systems, see the NZSIS *Protective Security Manual*

Visitors

34. Visitors to areas housing official information should not be allowed unrestricted movement.

35. Prior notice should be given to the guard or receptionist of expected visitors and whether they need to be escorted within the building.

36. On arrival, each visitor should be:
    - issued a pass that is clearly displayed
    - conducted either to the "host" or to a waiting room observed by a receptionist or guard.

37. Unless they have given prior notice of a visit, “hosts” should be asked by telephone if they will receive visitors.

38. If calling on more than one person, a visitor should be escorted between offices.

39. The last-visited person must make sure that a visitor leaves the building when their business is complete, and that they return any issued pass to the guard or receptionist. The last-visited person or an assigned staff member should escort the visitor to the exit.

40. Entry and exit to areas where classified material may be visible or accessible should be avoided. Visitors should be:

    - advised that no photographs or recordings of any type may be taken at any time during the visit to areas where classified information is held, processed or handled, except with specific departmental approval
    - asked, where necessary, to hand in mobile telephones and other recording and communications equipment.

41. To be effective, measures for visitor control should include a register of each visitor’s name and the staff member authorising the visit. It should also show:

    - the visitor’s department, agency or firm; or in the case of private individuals, their private address
    - the names of employees visited
    - the times of the visitor’s arrival and departure
    - the reason for the visit.

42. The visitor control record should be held at the guard or reception point, or by a designated employee if there is no guard or reception point.

43. The visitor control record should be covered to prevent visitors from seeing details of other visitors.

44. At the end of each day, all visitors’ passes should be checked, and action taken to account for any not returned.

45. The visitor register should be retained for a period of two years, to be available for any possible security investigations.

46. In organisations with a large flow of inquiries or visitors, the reception desk should be near the main entrance.

Entry by Media Representatives

47. If permission is granted for visits by media representatives to areas where classified material is used, handled or stored, the following additional procedures should be observed:

    - a designated staff member should accompany media representatives throughout the visit
    - classified material should be locked away or at least hidden
    - the media representatives must be reminded that no photographs or recordings of any type may be taken at any time during the visit, except with specific approval of their escorting staff member.

Instructions to Guards or Receptionists

48. Where guards or receptionists carry out security functions such as checking passes or maintaining records of staff entering or leaving at unusual hours, they should receive precise written instructions which should contain:

    - details on which pass holders may be admitted
    - names and telephone numbers to report incidents of security significance both during and outside working hours.

49. The instructions should be customised for every entrance to every building.

50. Close liaison between those controlling the guards or receptionists and the organisation's security personnel will ensure that:

    - the written instructions are understood, observed and updated
    - the guards or receptionists carry out their duties well.

Securing Facilities, Rooms and Offices

51. A secure zone may be a locked office, or several rooms inside a physical security perimeter, which may be locked or contain lockable cabinets or safes.

52. Consider the following controls for secure zones:

    - locate important facilities away from public access
    - lock unattended doors and windows
    - use external protection for windows, particularly at ground level
    - install intrusion-detection systems:
        - to professional standards
        - with regular testing
        - to cover all external doors and accessible windows
        - to alarm unoccupied areas at all times and other areas as needed

- locate information-processing facilities managed by the organisation in a different place than those managed by third parties
- locate support functions and equipment such as photocopiers and fax machines in a secure area so that information cannot be compromised
- restrict public access to directories and internal telephone books that identify the location of "sensitive" facilities.

Security Containers

53. The protection of classified material depends on:
    - the security container
    - the lock on the container
    - the location of the container within the site, building or secure zone.

54. For minimum requirements for locks, containers and their sites, when storing material classified CONFIDENTIAL and above, see the NZSIS *Protective Security Manual*; for a list of approved equipment for storing material classified CONFIDENTIAL or above, see Part 2, "Equipment Catalogue".

Table of Contents

Chapter 8: Communications and Systems Security Management

Configuration and Incident Management

Configuration Management

Introduction

1. Communications and Systems security management is fundamental to the protection of the Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation characteristics of information. It is also a key element in the implementation of Security Policy.

Certification and Accreditation

2. The formal validation of system security is achieved through a process of certification and accreditation.

3. All systems that handle classified information, or are particularly critical to a department's operation, will require accreditation. The establishment of departmental computer security policy and the conduct of informal system reviews should provide sufficient assurance of security for other systems.

4. Certification of an IT system is the confirmation that it meets all its stated security requirements. The certification process includes the development and maintenance of security documentation. It also involves confirmation by the system developers or administrators that the documentation is correct and complete and that the documented security architectures, mechanisms and processes have been implemented.

5. Accreditation follows on from certification. It is the process of verifying the system's security and formally authorising the system for operation. It involves an independent review of the certification documentation to ensure that the security measures meet the required level of security for the information and services managed by the system. It also involves site inspections to ensure that security has been implemented according to the documentation and appropriately for the environment. Once the verification process is complete, the accreditation authority will use the results to determine whether the system has approval to operate. The accreditation authority for a specific system is ultimately the Chief Executive of the department operating the system. However, the responsibility may be delegated to a member of the department's senior management group.

6. Configuration management or "configuration control" is a set of measures to keep system security, integrity and functionality from degrading when introducing new facilities or eliminating faults.

7. An organisations security plan may not work against new threats or ongoing changes in system configuration. Configuration management is fundamental to the continued strength of system security.

Configuration Control Board

8. Organisations should consider setting up a Configuration Control Board (CCB) to co-ordinate and approve changes to a system's baseline configuration. The CCB should have representatives from the following areas:

    - security
    - systems support
    - applications development
    - users.

Procedures

9. All system changes require configuration management. These may include:

    - hardware changes
    - software changes; for example, changes to operating systems, applications, programmes, utilities, and packages such as e-mail or web applications
    - documentation for hardware, software and system operations.

Software Control

10. Take care when changing operational software—seemingly minor changes may have significant, unexpected effects. Be especially careful to isolate "one-off" research-type programmes, which can subvert the system if uncontrolled. Consider controlling:

    - software selection
    - software installation and tailoring
    - software development and test environments
    - vendor's distribution media
    - software documentation
    - version changes and upgrades
    - system and software patches and hotfixes

11. For more on configuration management, see GCSB publication *NZSIT 105, Configuration Management*.

Incident Management Procedures

System Monitoring

12. Organisations should set procedures to monitor system use, ensuring that users only perform authorised processes. Consider:

    - a separate risk assessment to decide the appropriate level of monitoring
    - audit trails, which record exceptions and other relevant events, kept for a defined period to assist in investigations and ongoing access-control monitoring
    - recording successful as well as rejected attempts at system access.

13. Accurate computer system clocks ensure the accuracy of audit logs, which may be needed for investigations or as evidence in legal or disciplinary cases. Where a computer or communications device uses a real-time clock, it should be set to an agreed standard such as Co-ordinated Universal Time (UTC) or local standard time. Clocks should be regularly checked and corrected against any variation from the standard.

Intrusion and Misuse Detection

14. Despite appropriate security measures, attacks on systems occur and succeed. Intrusion-detection products are recommended to detect and warn of attacks.

15. Intrusion-detection tools are like virus-detection products in that they must be regularly reviewed and kept up-to-date.

16. Network-based intrusion-detection products can detect a range of suspicious network activity, including:

- attempts to use services blocked by firewalls
- unexpected requests, especially from unfamiliar network addresses
- unexpected encryption, which may be used to conceal an attack
- excessive network traffic from an unfamiliar site
- notable changes from past network activity
- attempts to exploit known system bugs or vulnerabilities.

17. Host-based intrusion-detection tools may also use the audit features of the host operating system to detect suspicious activity, including:
    - users logging in at strange times or from unexpected addresses
    - failed login attempts with bad passwords
    - unauthorised or suspicious use of administrator-level functions
    - changes to critical system files
    - notable changes in a particular user's activity
    - attempts to exploit known system bugs or vulnerabilities.

18. Network and host-based intrusion-detection tools may overlap, detecting the same attacks.

19. While intrusion-detection tools will not detect all attacks, and there may be false alarms, they significantly reduce the risk of undetected intrusions.

Intrusion-Response Scenarios

20. When an intrusion-detection tool detects a suspected attack, to prevent further attempts:
    - the system administrator must be alerted, and may take specific actions
    - the intrusion-detection product may disable or constrain network services.

Protection against Malicious Software

21. There are many ways to exploit the vulnerability of computer software. The following can make unauthorised changes:
    - computer viruses
    - network worms
    - Trojan horses
    - logic bombs.

22. Organisations must know about and prevent the introduction of malicious software. Specific procedures might include:

    - a prohibition on software not authorised by a Configuration Control Board
    - the mandated use of approved anti-virus and software-change-detection software.

Network Management

23. Access to computers and networks should be closely managed to:

    - optimise service to the business
    - consistently apply security measures across the information-systems infrastructure.

24. Procedural controls to achieve and maintain network security may include:

    - allocation and/or separation of responsibilities
    - intrusion or misuse detection
    - guidelines for managing devices such as routers and firewalls
    - management of cryptographic keys and equipment.

25. Organisations may need to interconnect or share computers or networks beyond traditional boundaries. The risk of unauthorised access and security breaches is greater for information passed across such networks and their computer systems. Security policies for networks that span organisational boundaries should consider additional controls:

    - within networks, to segregate user groups
    - between networks, to protect information in transit.

Media Handling and Security

Protecting Storage Media

26. Organisations should develop and use procedures to protect all media, for example tapes, disks and system documentation.

27. Media should be protected against:

    - damage
    - theft
    - loss
    - unauthorised access
    - virus or other software, or network, attacks
    - inappropriate sanitisation and/or disposal

28. Classified information on media should be protected from unauthorised disclosure or modification during transport. (See Chapter 3 Annexes A to F).

29. Clearly defined procedures should be used to manage removable computer media, such as tapes and disks.All media should be marked and stored according to the most sensitive or highest-classified information it contains. Apply the handling procedures specified in Chapter 3 Annexes A to F.

30. Appropriately purge surplus media before disposing of or releasing from the department (see paragraph 40).

Labelling

31. Removable media, such as disks and back-up tapes, must be labelled clearly and distinctively, with the security classification on each item that contains material that is SENSITIVE, RESTRICTED or above.

Movement of Media

32. All movements of media in and out of an organisation should be recorded.

33. Media should be checked:

    - on arrival for classification, damage, and malicious software such as viruses
    - on departure for classified information and viruses.

34. Privately owned media should be strictly controlled. As a general rule, private media should not enter systems in government organisations.

35. Organisations that process classified information should have a checking procedure, independent of the originator, to ensure that exported media contains only the information intended.

Back-Up

36. Adequate back-up facilities should be used so that all essential business data and software can be accessed or recovered after an incident. This may include a system failure, virus attacks, or a natural disaster. Back-up for each system should meet the requirements of the organisation's business continuity plan (see Chapter 1 paragraph 16).

Emergency Destruction

37. Organisations should have procedures in place for the emergency destruction of classified or sensitive information held in high-risk environments.

Disposal of Media

Sanitisation and Declassification

38. Sanitisation is the process of erasing as far as possible the information from media or equipment. The process of sanitisation does not automatically change the classification of the media or equipment. Note that sanitisation does not involve destroying the media or equipment.

39. Declassification is the removal of or reduction in the classification of the media or equipment. The decision to declassify should be preceded by an assessment of the risk of improper disclosure of any information remaining on the media or equipment, should declassification take place. In considering risk associated with declassification, it is important to take into account the resale value of the asset(s)(where the value is low it may be preferable to opt for destruction), the destination of any released media (and therefore the likelihood of compromise), the serviceability of the media which may directly relate to the resale value, and any contractual obligations.

40. Considerable information can be retrieved from computing equipment and media that has failed or outlived its purpose. The only totally reliable method of removing all traces of information from memory devices and magnetic media is physical destruction. However, some sanitisation methods can be a reliable alternative, in making the information too expensive to be worth recovering. Approved sanitisation procedures can be used to cleanse a device or media for disposal or reuse.

41. Media or equipment retains the security classification of the highest-classified information it has ever held until appropriately sanitised or declassified.

42. For more on sanitisation, see NZSIT207, Declassification of Storage Media.

Document and Media Destruction

43. Waste material that could contain official information must be disposed of securely, as defined in Chapter 4.

44. Approved ways of disposing of information-systems media, such as magnetic media, include:

    - degaussing (or demagnetisation)—for floppy disks and magnetic tape, though hard disks may also have tracking information destroyed this way
    - overwriting with approved software—for hard disks, but not for floppy discs or magnetic tape
    - destruction— mandatory for magnetic media that has held information classified TOP SECRET.

45. Reformatting a hard or floppy disk *does not* necessarily overwrite its data—*reformatting is not an approved means of sanitisation*.

46. For more on document and media destruction, see *NZSIT 207, Declassification of Storage Media.*

Security of System Documentation

Protection of System Documentation

47. System documentation may contain a range of sensitive information and should be protected from unauthorised access by:

    - physically securing it
    - minimising its distribution
    - disposing securely when it is superseded.

Security in Software Applications

48. Input data should be vetted in all key business systems.

49. Processing errors or deliberate acts can corrupt data that has been correctly entered into an application system. Systems should have validation checks to detect any such corruption. The specific controls needed depend on the application and the assessed impact of any corruption.

Operating Systems and Package Maintenance

50. All changes to operating systems software must be managed through strong configuration management processes.

51. Changes to original copies of systems software and standard commercial software should be discouraged. If necessary, changes should be made only to a clearly identified copy; the original software should be retained.

Protection of Development Suite and Test Data

52. Development and operational systems should be separated to reduce the risk of accidental changes or unauthorised access to operational software, processes and data. Developmental and operational software should be run in different operating environments.

53. Source code and configuration files should be protected from unauthorised viewing and changing. They should be managed under strict version control, with clear separation between operational and development versions. Source code should not be stored on operational systems, nor should it be freely available to information systems support staff who do not need access.

54. Testing data should be completed before implementation. Test data should be protected and controlled. System and acceptance testing usually requires much test data that mimics live data. The use of live databases containing personal information should be avoided.

Exchanges of Information and Software

Information and Software Exchange Agreements

55. Exchanges of information and software should be based on formal agreements, in line with any relevant legislation and licensing arrangements.

Security of Information in Transit

56. Procedures and standards should be set to protect information in transit, especially electronic data interchanges. One such mechanism is the Secure Electronic Environment (S.E.E.) for inter-governmental communications classified up to SENSITIVE. The State Service Commission's S.E.E. Mail network is an e-mail gateway to gateway encryption system.

Leased Lines and Public Networks

57. Organisations should consider the following security concerns in using leased lines or public networks to communicate between information systems that process classified information:

    - data interception
    - data modification
    - user impersonation
    - unauthorised access into networks.

Initial planning to use leased lines and public networks should incorporate security measures such as:

- configuration management
- security management
- cryptography
- border controls.

Internet Security

58. Government networks connected to public networks must be protected by appropriate security measures, even if processing only unclassified information. The main public network, the Internet, has become a widely used business tool; electronic mail (e-mail) and access to the World Wide Web are used more and more for business communications and transactions.

59. The Internet is vulnerable to:

- message interception
- unauthorised access to systems
- attacks which can modify, manipulate or destroy data and systems
- attacks which can hinder or disrupt services or systems.

60. Security policies should impose controls and processes to manage business or security risks from the Internet. These risks may include:

- vulnerability of traffic to unauthorised interception or modification
- vulnerability to error, for example, incorrect addressing or misdirection
- lack of control over the reliability and availability of service
- accessibility of official information in public directories.

61. Where the appropriate security measures are in place, connection to the Internet is permissible for networks handling official information classified up to RESTRICTED or SENSITIVE.

62. Systems that process information classified CONFIDENTIAL or above must not be connected to the Internet unless specific security measures are used such as encryption products and gateways approved by the GCSB.

63. The minimum standards for Internet security in the New Zealand Government are at Annex A to this Chapter.

Telephone Security

64. No telephone conversation is free from the risk of interception:

    - The telephone system is widely accessible by many people, such as maintenance technicians or switchboard operators, in the course of their normal duties.
    - Authorised and unauthorised monitoring of telephones is possible at junctions and distribution points throughout the system.

65. Conversations classified CONFIDENTIAL or above must not be held over a telephone circuit unless it has end-to-end cryptographic protection. Consult the GCSB for advice on appropriate protective measures.

66. All staff should be briefed on the danger of using a telephone for classified conversations.

67. Callers may try to get classified information by falsely representing themselves (social engineering). Staff should be reminded of the need to properly identify all callers before giving any information. Where a caller cannot be satisfactorily identified, they can be asked for a call-back number, which can be authenticated.

68. Security vulnerabilities of telephone systems include monitoring of room audio carried on telephone cables through built-in system features, or deliberate tampering with hardware or software, even when the telephone's handset is "on-hook".

69. For comprehensive advice on security issues related to telephone systems, see *GCSB Security Notice 2/97: Telephone Systems* (included in *NZSIT 109, Information Systems Security Notices).*

Cellular Phone Security

70. Cellular phones (cellphones), both digital and analogue, should never be permitted in sensitive areas because:

    - they can inadvertently transmit sensitive information.
    - some cellphones can be configured to ring silently and automatically answer an incoming call, and be used as an eavesdropping device to remotely monitor conversations.

71. Satellite phones have similar security issues to standard cellphones.

72. For more on the security of cellphones, see *GCSB Security Notice 1/99: Cellular Telephones* (in *NZSIT 109).*

Digital Cellphones

73. Digital cellphones (GSM and CDMA) have a lower probability of intercept than analogue cellphones (see paragraph 74). Within New Zealand only, digital cellphones may be used for transmission of information classified IN CONFIDENCE, SENSITIVE or RESTRICTED.

Analogue Cellphones and Cordless Telephones

74. Portable telephones (cellphones) and cordless telephones are generally vulnerable to intercept using inexpensive and readily available radio-scanning receivers.

Personal Electronic Devices

75. Personal Electronic Devices (PEDs) such as Personal Digital Assistants (PDAs) have further vulnerabilities so that potential risks increase from using them in or around areas where classified information may be discussed or processed. Some issues of concern are:

    Audio Recording Capabilities: Some PEDs are capable of recording up to six hours of audio. Additionally, microphones may be capable of picking up normal office conversations from a distance in excess of 50 feet.

    IR Ports: Data from the IR port of a PED can be intercepted at (or exercised from) significant distances.

76. The following minimum precautions should be observed:

    Microphones: Site policies should preclude the introduction of audio recording equipment including PEDs with microphones into controlled spaces.

    IR Ports: Any IR Port on a PED should be covered with an IR opaque metallic tape.

    Passwords: The use of strong device passwords should be mandated, as the password may be the only mechanism that prevents an attacker from loading malicious code onto a PED.

77. Wireless-enabled personal electronic devices (WPEDs) such as e-mail or web-enabled cellphones, and wireless enabled palm-top computers, have the same set of vulnerabilities as Wireless LANs (WLANs) and must be handled accordingly (see Chapter 9).

78. Further advice on precautions for the use of PEDs is available from the GCSB.

Pagers

79. Information transmitted to a pager can be easily intercepted. Pagers must not be used to transmit classified information.

Answering Services

- Care should be taken when using answerphones in offices handling classified information to ensure that classified messages are not left on them.

PABXs

80. PABXs generally have a dial-in facility for remote maintenance. This might allow a person distant from a secure site to gain system access.The remote maintenance facility of PABXs should be disabled.However, if used it should be physically or electronically isolated when not in use.

81. Dial in Subscriber Access (DISA) lines should be carefully managed.

Facsimile Transmission Security

82. Commercial facsimile (fax) systems that transmit and receive information over open communications channels are not secure. They are as vulnerable as telephone systems.

83. Additional security risks come from facsimile units that scan and print. They should not be connected simultaneously to both unclassified and classified systems.

84. For occasional use within New Zealand, facsimile may be used without encryption to transmit information classified IN CONFIDENCE, RESTRICTED or SENSITIVE .

85. For more on facsimile security, see the GCSB's *INFOSEC Bulletin Number 21*.

Transmission of Video and Video-Conferencing

86. Video-conferencing systems should be protected by encryption systems appropriate to the classification of material transmitted and to the transmission medium (see paragraph 104). Note that:

    - the auto-answer features should be disabled
    - the Internet should not be used as a vehicle for sensitive video-conferencing at this time.

Security Requirements of Systems

87. Systems security must consider:

    - infrastructure
    - applications, including user-developed applications
    - availability of adequate capacity and resources.

88. Security can depend on how a business process that supports an application or service is designed and implemented.

89. Before developing information systems, organisations should identify and agree on security needs. At the requirements phase of an information systems project, as part of the overall business case, all security needs including fallback arrangements should be:

    - identified
    - justified
    - agreed
    - documented.

Security in Application Systems

Evaluated Products

90. Evaluation offers a measure of assurance on the functionality and security features of a product .

91. To properly evaluate a product, the recommended evaluation standard is ISO/IEC 15408, otherwise known as the “Common Criteria” (CC) method. The use of CC:

    - provides an international standard for the harmonisation of evaluation criteria
    - provides assurance that a product will provide the security services or functions stated
    - must be completed independently of the vendor, by an approved authority.

92. New Zealand jointly manages, with Australia, the Australasian Information Security Evaluation Programme (AISEP). A number of companies are licensed as Australasian Information Security Evaluation Facilities. For more on the AISEP see http://www.aisep.gov.au

93. A mutual-recognition arrangement has been established among a number of countries, including the United States, Canada, Germany, France, the United Kingdom, Australia and New Zealand. Generally, each of the signatories agrees to accept evaluations carried out by another signatory.

94. CC specifies eight levels of security, known as Evaluation Assurance Level (EAL) 0 (lowest level) to EAL7 (highest).

95. For all security applications evaluated products should be used wherever possible.

96. For more on the Common Criteria Organisation, see http://www.commoncriteria.org.

Protecting Classified Information

97. GCSB should be consulted for advice on the security aspects of design and architecture for systems to be used for processing classified information.

Cryptographic Controls

Appropriate Grades of Encryption

98. For systems with information that requires confidentiality, authentication, integrity and protection in transit or on magnetic media, consider cryptography.

99. Cryptography, or "encryption", is the process of transforming information into an unintelligible form to safeguard its security and integrity. It uses an encryption algorithm and a secret cryptographic key.

100. Cryptography also can ensure:

- authentication—the identity of the respective parties can be confirmed
- integrity—any change to the information while in transit can be detected
- non-repudiation—the sender cannot deny sending the information.

101. While encryption can be a powerful tool, used carelessly it can:

- hinder virus and system-misuse detection
- cause information to be lost
- provide users with a false sense of security.

102. The policy for cryptographic systems and techniques should account for business needs within and between departments.

103. For specialist advice on applying encryption and selecting cryptographic products, consult the GCSB.

104. The following table summarises national policy on encryption:

Security Classification	Grade of Cryptographic System Required	
	Within New Zealand	Outside New Zealand
TOP SECRET	High Grade[2]	
SECRET		
CONFIDENTIAL	High Grade or Enhanced Grade[3]	
RESTRICTED or SENSITIVE	Encryption Required Across Public Networks	Encryption Required[4]
IN CONFIDENCE	None Required But Assess Risk	
UNCLASSIFIED	None Required	

105. Before installing a system that varies from national policy, the government organisation must consult the GCSB.

Key Management

106. Strict rules protect the keys used with cryptographic systems for classified information. To protect Government information, keys must come directly from the GCSB or from a GCSB-approved system.

107. For more on key management, consult the GCSB.

2 High-grade encryption products are government-furnished and approved for all classifications of information. They can only be procured through the GCSB.

3 Enhanced-grade encryption products have been:

- evaluated
- modified from commercial products to incorporate a government-provided encryption algorithm
- approved for information classified up to CONFIDENTIAL.

- 4 Encryption products must be evaluated and approved by GCSB to transmit information classified up to SENSITIVE or RESTRICTED.

Emanation Security Controls (TEMPEST)

108. The term TEMPEST covers the issue of compromise by electromagnetic emanations from information-processing equipment. Specifically, the emanations might have components that allow classified information to be recovered.

109. Current practice is to counter TEMPEST vulnerabilities following risk management techniques, applying countermeasures as needed.

110. Equipment designed or modified to reduce TEMPEST vulnerabilities is more expensive to purchase, install, and maintain than the original product, and generally not available until much later.

TEMPEST Countermeasures

111. TEMPEST countermeasures are not normally required for installations within New Zealand. However, consult the GCSB about TEMPEST countermeasures for facilities:

- that process volumes of classified or especially sensitive information
- where foreign organisations occupy adjacent premises.

112. TEMPEST countermeasures are normally required at overseas New Zealand installations that process information classified CONFIDENTIAL or above.

113. For more on selecting appropriate TEMPEST countermeasures consult the GCSB.

Technical Security (TECSEC)

114. Technical security (TECSEC) is the protection against unauthorised access to official information by accidental or intentional oversight, overhearing or technical attack.

Technical Attack

115. A key defence against technical attack is strict access control. For example, in a room often used for classified conversations:

- always restrict access to only authorised persons
- supervise cleaning, redecoration and maintenance work
- fit access doors with secure locks, and properly secure the keys
- keep records of all maintenance work and all furniture in the room.

Inspection Services and Advice

116. The GCSB offers departments a technical security inspection service and specialist advice on TECSEC countermeasures.

Annex A—Minimum Standards for Internet Security in the New Zealand Government

Introduction

Why do we need Internet Security Standards?

1. The Internet is changing the way that citizens, government and business interact and collaborate with each other. Governments around the world, as part of electronic government initiatives, are taking advantage of the opportunities that the Internet provides for improving service delivery to citizens as well as improving the way governments work within their structures and functions.

2. The development of standards for use of the Internet across government will provide citizens with confidence that government systems provide adequate security and privacy safeguards.

About this Document

3. This document defines a set of policies and guidelines for Internet security, limited to the following five broad subjects:

   - *Information Security Management*
   - *Internet Gateways*
   - *Internet Server Configuration*
   - *Malicious Software (malware) Protection*
   - *Incident Detection and Handling*.

4. The measures outlined in this document define the minimum standards required to provide an acceptable level of security in those subject areas for government systems connecting to the Internet.

5. It is not anticipated that Government sector organisations will tailor their own versions of these documents or produce detailed Statement of Compliance or Specified Departures documents for auditing purposes. However, they should ensure they can justify any departure from these best practices during an audit or following an incident.

6. The technical guidelines referenced here are evolving rapidly due to the progression of the underlying technology and products and the discovery of new vulnerabilities and attack methods on almost a daily basis. For this reason, only references to the recommended guides are provided here. The current version of the specific guidelines should be obtained when and as required.

7. The key words “must” and “should” are used as within Internet RFCs:

- **Must** means that the definition is an absolute requirement.
- **Should** means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- Where a document is defined as “**should be considered**” the applicable document must be reviewed, but the decision whether or not to follow the individual recommendations is a departmental risk management issue.

High Level Policies

8. The implementation of effective Internet security strategies involves:

- protection of government online systems and information assets
- detection of incidents and vulnerabilities
- reaction to address and resolve issues or incidents as they emerge.

9. In regard to Internet-connected systems, agencies must:

- adopt a structured approach to the management of Internet security, employing a sound risk management model
- ensure that appropriate risk assessments are conducted
- avoid default installations of operating system and server software
- test and install security patches in a timely manner
- regularly review security logs
- ensure that applications are reviewed for secure coding practices
- ensure that relevant documentation is kept up to date
- ensure that security training is relevant and up to date
- plan and regularly test ways in which to detect and react to system failure, misuse and unauthorised access.

Information Security (IS) Management Standards

10. An IS management framework following *AS/NZS ISO/IEC 17799 Code of Practice for Information Security Management* (available from www.standards.co.nz) must be employed for all systems processing classified (including IN CONFIDENCE) information or hosting Government services. The individual security countermeasures defined in the standard should be considered but are not mandated.

11. IT security risks must be managed following the processes in either:

    - *NZ Security of IT (NZSIT) Publication 104: Risk Analysis* (http://www.gcsb.govt.nz/nzsit/index.html) or
    - *Standards New Zealand AS/NZS4360: Risk Management and HB231: IT Risk Management*.

Internet Gateway Standards

12. All government networks that are attached to the Internet should be connected through a firewall.

13. Those systems that process information classified SENSITIVE or above must use firewalls that have been evaluated through the AISEP or a compatible scheme. They should be evaluated to a level of EAL4 (or ITSEC E3) or higher.

14. A network access policy should be defined and documented, and the firewall should be verified to comply with the policy.

15. CERT Co-ordination Center's *Security Improvement Module 8: Deploying Firewalls* (www.cert.org/security-improvement/) contains a set of best practices that should be considered when designing a firewall architecture and network access policy.

16. PCs, laptops, etc that are connected directly to the Internet should have personal firewall systems installed or—if possible—the operating system configured to provide equivalent functionality.

17. The addition of a firewall should also be considered when departments connect any two networks together that do not share a common security policy.

18. All security-relevant firewall software patches must be kept up to date.

19. Internet routers must be configured in accordance with *RFC2827: Network Ingress Filtering* (www.rfc.net/rfc2827.html) to reduce the risk of them being used in denial of service attacks against other sites.

20. Mail servers must be configured to prevent Open Relaying (ie. reject attempts to forward e-mail from non-departmental senders to non-departmental addresses). Guidance is available in *RFC2505: Anti-spam Recommendations for SMTP MTAs* (www.rfc.net/rfc2505.html).

Internet Server Configuration Standards

21. Internet servers (web, e-mail, news, DNS, etc) must never be located inside government networks without Internet firewall protection between them and computers on the internal network segments. They should preferably be located on De-militarised Zones (DMZ, eg. connected to a third interface on the firewall), so that the server is shielded from the Internet, but where compromise of the server would not result in access to the internal network.

22. Internet servers must be configured in accordance with the following guidelines:

    - All unnecessary services and networking protocols must be removed or disabled from the operating system.
    - All unnecessary programs, scripts, code, programme development systems and administrative utilities must be removed from the platform.
    - Security-relevant patches must be kept up to date.
    - One of the following guideline documents should be consulted for appropriate configuration of the server operating system:
        - *SANS Step By Step* operating system configuration guidelines (www.sansstore.org); or
        - *NSA Securing Windows 2000* (nsa2.www.conxion.com); or
        - *Centre for Internet Security* provides best practice benchmarks for configuring Solaris, Linux, or Windows 2000 systems (www.cisecurity.org).

23. System administrators should keep up with the *SANS/FBI Top 20 Internet Security Vulnerabilities* (www.sans.org/top20.htm) and manage the risks accordingly.

24. Administration of the system should be restricted to local access only or require strong authentication, refer to *NZSIT 204, Authentication Services and Mechanisms* (www.gcsb.govt.nz/nzsit/index.htm).

Malware Protection Standards

25. All computers used for Government business with any communications to external systems (Internet, dial-in, CD access, etc) must operate appropriate anti-virus software.

    - The virus signature databases must be kept current.
    - Networks should have anti-virus and/or appropriately configured content scanners around entry points (eg. on e-mail servers).

26. Networks that process information classified SENSITIVE or higher, or that contain critical systems, must take particular care when permitting active code (eg. Java, ActiveX) to be run from untrusted sites on the Internet (e.g. other than *.govt.nz and trusted partners) or other uncontrolled networks. Agencies must put in place mechanisms to mitigate the risks and should consider completely disabling such functions from their computers.

27. Agencies should consider rejecting Internet cookies and script and macro languages if they are not required for business processes.

28. Most Internet browsers have the capability to add application extensions to the basic functionality (eg. when a .doc file is encountered *Microsoft Word* is activated to view the document). Many such extensions or plug-ins can be exploited to run malicious code on the browser computer, so qualified security staff must approve any application extensions before they are included in user Web browsers.

29. Users must be made aware of the potential risks inherent with opening or running attachments and executable content that has arrived unsolicited or originates from an untrusted source.

30. For more information on malicious software refer to NZSIT 208 : Dealing with Malicious Software.

Incident Detection and Handling

31. IT system security is never infallible, so measures must be in place to detect and react to system failure, misuse and unauthorised access. The exact nature of the detection systems and response processes will depend on the type of system and an assessment of the potential threats and impacts.

32. For systems processing Government information or hosting Government services, security-relevant events such as failed access attempts, security configuration changes, and changes to the user account database should be logged to another system.

33. File integrity checking systems should be considered to monitor critical files on such systems, and any connections with other networks should be monitored for intrusion attempts.

34. Procedures must be employed to monitor and react to the outputs and alerts generated by intrusion or misuse systems in a timely and appropriate manner.

35. The security configuration of each Internet connected system should be audited periodically to ensure it has not been inadvertently misconfigured or tampered with.

36. The *SANS Incident Handling Step By Step Survival Guide* (from www.sansstore.org) provides an excellent basis for development of incident handling procedures.

37. Guidance on intrusion detection is available from the CERT Co-ordination Center in the form of *Security Improvement Module 9: Detecting Signs of Intrusion*, and *Module 6: Responding to Intrusions* (www.cert.org/security-improvement/).

Summarised List of Internet Security Standards

Function	Standard or System	Purpose	Status
Management	AS/NZS 17799	Information Security Management	Mandated
or	NZSIT 104 AS/NZS4360 plus HB231	Risk Analysis Risk Management	Mandated
Internet Gateways	CERT/CC: Security Improvement Module 8	Best Practices for designing firewall architecture	Guidance
	RFC2827	Router configuration	Mandated
	RFC2505	Mail server configuration	Guidance
Internet Server Configuration	SANS: Step by Step	Operating System Configuration Guidelines	Guidance
or	NSA: Windows 2000 Security Recommendation Guides	Windows 2000 Configuration Guidelines	Guidance
or	Centre for Internet Security Solaris Benchmark	Security configuration guidance for hardening Linux, Solaris and Win NT operating systems	Guidance
	NZSIT 204	System administration restrictions	Guidance
Malware Protection	NZSIT 208	Dealing with Malicious Software	Guidance
Incident Detection and Handling	SANS: Incident Handling Step-by-Step Survival Guide	Development of Incident Handling Procedures	Guidance
or	CERT/CC: Security Improvement Module 9 CERT/CC: Security Improvement Module 6	Guidance on Intrusion Detection Responding to Intrusions	Guidance

Table of Contents

Chapter 9: Control of Access to Information Systems

Business Requirement for Access Control

1. Appropriate access controls assist to protect information processed and stored in computer systems. The “defence in depth” principle should be followed based on risk management, and where appropriate using several “layers” to protect critical information. (See Chapter 7 paragraphs 1 to 5).

2. The organisation's system security policy must clearly define the needs of each user or group to access systems, applications and data.

3. User and group file-access rights should be configured according to business requirements and the “need to know” principle.

4. Formal procedures should control how access is granted to information-system services or how such access is changed, so as to prevent unauthorised access to data or system resources.

5. A usage profile, detailing privileges and access rights, should be assigned to each user. Give special attention to privileged access rights that can override system controls. Administration accounts must be strictly controlled and subject to special authorisation by the DSO.

6. A user registration policy should:

   - formally authorise who gives out user IDs
   - control the levels of access that can be granted
   - maintain formal records on registered users
   - make sure that all redundant user accounts are deleted
   - regularly review registered users priveleges.

Access Control Rules

7. Access control can start by allowing access to everything, and then revoking access to whatever systems, applications or data repositories a user does not need. However, it is better to start by *denying* access to everything, and then explicitly granting access to just the specific resources a user needs.

8. Secure logon procedures can control access to host-based information systems. Logon procedures should reveal minimal information about the system, to deter unauthorised use.

Least Privilege Authorisation ("Need to Know")

9. Consider the principle of least privilege: grant no user greater access to the system than their duty demands.

10. This principle can be applied to users' modes of access, such as whether they receive "read or write" privileges.

Logon Banners and Warning Notices

11. There may be a defence against prosecution for computer-related offences if warnings about how an information system may be used are missing or inadequate. To pre-empt such a defence, an organisation should provide warnings on the system's logon banners that say:

    - the system is for authorised users only
    - usage is monitored
    - evidence of misuse may be presented in legal proceedings
    - by continuing to access the system after seeing the warning, people represent themselves as authorised users.

File-System Controls

12. Server file systems must have access control mechanisms to prevent unauthorised access or changes to data. This is critical when server file systems are connected to the Internet, even behind a firewall.

13. Server file-system access controls should restrict:

    - direct-write access to system areas
    - adding software or services
    - accessing other users' files.

User Access Management

14. Access control to information systems and services should cover all stages in the life-cycle of user access: from registration of new users to de-registration of users who no longer need access. Where possible, user policies should be enforced by the operating system or other software.

User Authentication

15. When users log on, organisations must authenticate their identities. How to authenticate depends mainly on risk assessment and cost. There are three types (factors) of authenticating information:

    - something the user knows, usually a password or pass-phrase
    - something the user has, such as a magnetically coded card, or a "smart" card

- something the user is, such as a fingerprint, verified by biometric measurement.

- where possible and practical, use two authentication factors.

User Registration

Account and Access Management

16. Users should be assigned only the access privileges needed for their job.

17. System administration accounts should be assigned and used only as needed. Do not log on to administration accounts, for example, when using the system as a regular user, not performing administration duties.

18. Personnel management should include documented procedures describing the entire lifecycle of user accounts.

Single Sign-On and Trusted Domains

19. Where single sign-on or trusted domains are used to simplify user authentication, internal mechanisms must protect against critical failure.

20. Use evaluated products wherever possible.

21. Servers containing user credentials should be:
    - physically protected
    - tightly configured
    - monitored for inappropriate use.

Inactivity Timeout and Restricted Connection Times

22. An additional security measure to prevent unauthorised access to an information system is to automatically disable logged-on workstations after a period of inactivity.

23. Restricting connection times can provide additional security for high-risk applications, reducing the window of opportunity for unauthorised access.

Further Guidance

24. For more on access control and authentication, see *NZSIT 101, Information Technology Security Policy Handbook, Chapter 7,* and *NZSIT 204, Authentication Services and Mechanisms*.

User Password Management

Passwords

25. The first line of defence for a host computer system is usually the user-identification code (user ID) and some form of authentication, such as a password.

26. Passwords must be secure but memorable. They should be granted through a formal management process, where users agree to keep them confidential.

One-Time Passwords and Tokens

27. Tokens are devices used to generate a one-time password or Personal Identification Number (PIN). Because they are expensive, they are normally found only on higher-security systems. Where they generate passwords tThey should be used with PINs to protect against unauthorised use if lost or stolen. PINs should be safeguarded to the same degree as passwords.

Digital Signatures

28. Digital signatures can be used to verify the content and originator of messages, documents, and software. The advent of public key cryptography (PKC) has made digital signatures available for access control, authentication, and user identification.

29. Digital signature information must be protected against loss or misuse.

30. A digital signature may be given in the form of a token.

Biometrics

31. Biometric devices can provide better security than either passwords or tokens, but they can present additional engineering issues. Organisations intending to use biometric devices should seek advice from the GCSB.

System Access Control

32. Systems have five main access vulnerabilities to attack:

    - users' workstations
    - dial-in lines
    - interference with communications paths
    - connections to public networks such as the Internet
    - interfaces with other systems.

33. System vulnerabilities can be reduced by using:

    - a carefully designed security architecture incorporating the principles of defence in depth
    - physical security for unattended workstations
    - encryption and other techniques for communications paths
    - approved firewalls, where connections are permitted to public networks
    - intrusion-detection systems, used in conjunction with a firewall
    - applying strong controls to any operating system access.

34. For specific advice on reducing network vulnerabilities, consult the GCSB.

Firewalls and Border Controls

35. A firewall can control and record access to services from both inside and outside an organisation's private network. The firewall can permit, deny, or redirect the flow of data.

36. For a firewall to function effectively:

    - all traffic between the internal and external networks must flow through the firewall
    - it must be properly configured, managed, and audited.

37. Firewalls are only approved for systems handling information classified up to RESTRICTED or SENSITIVE. Higher-classified systems must use an air-gap[1] for passing information to systems connected to public networks.

38. Firewalls should be evaluated products (see Chapter 8 paragraphs 86-93).

Approved Circuits

39. An "approved circuit" is a fibre-optic or wire landline, and associated terminal equipment, with electro-magnetic and physical safeguards against unauthorised interception.

40. Approved circuits are usually under close control, reducing risk sufficiently so that higher-classified information may be sent without encryption.

41. GCSB advice should be sought where an approved circuit is being considered.

1 Where there is no direct connection between systems, information is passed across an "air-gap" by media such as floppy disks. Formal procedures are required to ensure that only permitted data pass from system to another.

Wireless Local Area Networks

42. Wireless local area networks (WLANs) have significant vulnerabilities that must be addressed by organisations considering the use of such devices for processing classified official information.

43. Wireless LANs (WLANs) use radio frequency (RF) transmissions instead of cables to connect together computer equipment such as printers and terminals through an Access Point (AP).

44. WLANs are generally compliant with published international standards, but these standards do not in themselves guarantee security. WLANs are vulnerable to a range of attacks and threats, some of which are summarised below:

    Confidentiality - Communications between a legitimate mobile device and an AP may be overheard or intercepted by other users.

    Authentication - An unauthorised party might gain access to the network using a compliant device and, by emulating an authorised user, access information on the system or provide incorrect or misleading information.

    Denial of Services Attacks - Unauthorised users may tie up network resources so normal users do not receive a service.

    Interference - WLANs commonly operate in frequency bands set-aside for use by other systems, including industrial, scientific or medical equipment. Other devices operating legitimately in these bands may inadvertently disrupt a WLANs communications.

    Cryptography - Cryptographic implementations may in reality provide little security.

45. WLANs processing government-classified information must be appropriately encrypted. Consult GCSB for further advice.

46. Departments should consider privacy and policy issues before permitting WLANs to be used for passing or processing unclassified official information, or before connecting to internal networks.

47. Further advice on the security implications of WLAN services is available from the GCSB.

Application Access Control

48. Controls should be used to restrict access within application systems. Logical access to software and information should be limited to authorised users. Application system controls should:

    - control user access to information and application system functions, according to a defined access-control policy
    - prevent unauthorised access to any utility or operating-system software that can override system or application controls
    - prevent compromise to the security of other systems with which information resources are shared
    - allow access only to the owner of information and other authorised users or groups
    - carefully manage any interfaces.

Sensitive System Isolation

49. Particularly sensitive systems may need to run on a dedicated computer, or share resources only with other trusted application systems. The sensitivity of an application system should be clearly identified and documented in the system security policy and security plan.

Monitoring-System Access and Use

50. Systems should be monitored to detect deviation from the access-control policy.

51. Deviations should be recorded, both as evidence and for process enhancement in case of all security incidents.

52. System monitoring should make sure controls are working and that they are appropriate and in accordance with the access-control policy.

Mobile Computing, Teleworking and Homeworking

53. With mobile computing, teleworking and homeworking, consider the risks of:

    - compromise at the remote site
    - vulnerability to data interception.

54. Since many personal and laptop computers are lost or stolen every year, additional physical protection such as alarms or cable locks may be needed in open or shared environments.

55. Consider media encryption to protect information on computers used outside of a department's physically controlled areas.

56. Remote access to an organisation's network should be configured and managed so that it:

    - allows only the specific services needed
    - is only available when needed
    - can only be used by specific, authenticated users.

57. When transmitting classified information, apply the security measures specified in Chapter 3 Annexes A to F of this manual .

58. Where classified information must be processed on a portable computer in an area where not all personnel are cleared or have a "need to know", position the computer carefully to avoid casual overview.

59. Products for secure access control and hard-disk encryption are recommended for laptops that contain classified information and may be taken outside the organisation. Consult the GCSB for advice on laptop-security products.

60. For more advice on homeworking, see the NZSIS *Protective Security Manual*.

Cross-Reference to AS/NZ ISO/IEC 17799:2001

The information in “Security in the Government Sector” is based on the Joint Australian New Zealand Standard AS/NZ ISO/IEC 17799:2001, Information Technology—Code of Practice for Information Security Management.

"Security in the Government Sector" provides information in a layout that suits security responsibilities and arrangements in the New Zealand public sector. For these reasons, its layout does not exactly match the layout in the Standard. This table provides a cross-reference to the Standard, for audit purposes.

1. Scope

2. Terms and Definitions

3. Security Policy

3.1 Information security policy Objective: To give management direction and support for information security. Management should set a clear policy direction and demonstrate support for, and commitment to, information security, by issuing and maintaining an information-security policy across the organisation.		
AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
3.1.1 Information-security policy document	2	1 - 5
3.1.2 Review and evaluation	2	6 - 8

4. Organisation Security

4.1 Information-security infrastructure

Objective: To manage information security within the organisation.

A management framework should be set up to initiate and control how information security is applied within the organisation.

Management forums, with management leadership, should be set up to approve the information-security policy, assign security roles and co-ordinate setting up security across the organisation. If needed, a source of specialist information security advice should be made available within the organisation. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security should be encouraged, so that managers, users, administrators, application designers, auditors, specialists in areas such as insurance and risk management and security staff collaborate and co-operate.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
4.1.1 Management information-security forum	2	9 -10
4.1.2 Information-security co-ordination	2	11 - 12
4.1.3 Allocation of information-security responsibilities	2	13 - 17
4.1.4 Authorisation process for information-processing facilities	8	1 - 11
4.1.5 Specialist information-security advice	2	30 - 34
4.1.6 Co-operation between organisations	1	7 - 8
4.1.7 Independent review of information security	2	6 - 8

4.2 Security of third-party access

Objective: To maintain the security of organisational information-processing facilities and information assets accessed by third parties.

Access to the organisation's information-processing facilities by third parties should be controlled.

Where there is a business need for such third-party access, a risk assessment should be done to decide how security is affected and what controls are needed. Controls should be agreed and defined in a contract with the third party.

Third-party access may involve other participants. Contracts conferring third-party access should cover designation of other eligible participants and conditions for their access. This standard could be used as a basis for such contracts and when considering the outsourcing of information processing.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
4.2.1 Identification of risks from third-party access	6	1 - 4
4.2.2 Security requirements in third-party contracts	6	25 - 27

4.3 Outsourcing

Objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

Outsourcing arrangements should address the risks, security controls and procedures for information systems, networks and/or desktop environments in the contract between the parties

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
4.3.1 Security requirements in outsourcing contracts	6	22 - 24

5. Asset classification and control

5.1 Accountability for assets

Objective: To maintain appropriate protection of organisational assets.

All major information assets should be accounted for and have a named owner.

Accountability for assets helps to ensure that appropriate protection is maintained. All major assets should have assigned owners and people responsible for maintaining appropriate controls. Responsibility for setting up controls may be delegated. Accountability should remain with the owner of the asset.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
5.1.1 Inventory of assets	3	2

5.2 Information classification

Objective: To ensure that information assets receive the right protection.

Information should be classified to indicate the need, priorities and degree of protection.

Information has varying degrees of sensitivity and criticality. Some items may need extra protection or special handling. An information-classification system should be used to define the right protection levels, and communicate the need for special handling measures.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
5.2.1 Classification guidelines	3	4-33
5.2.2 Information labelling and handling	3	Annexes A-F
	4	14 - 15, 20 - 27, 39 - 41, 47, 51 - 72
	8	31

6. Personnel security

6.1 Security in job definition and resourcing

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

Security responsibilities should be addressed at the recruitment stage, included in contracts and monitored during employment.

Potential recruits should be adequately screened (see 6.1.2), especially for sensitive jobs. All employees and third-party users of information-processing facilities should sign a confidentiality (non-disclosure) agreement.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
6.1.1 Including security in job responsibilities	5	2
6.1.2 Personnel screening and policy	5	8 - 10
6.1.3 Confidentiality agreements	5	6 - 7
6.1.4 Terms and conditions of employment	5	4

6.2 User training

Objective: To ensure that users know about information security threats and concerns, and that they can support organisational security policy as part of their work.

Users should be trained in security procedures and correctly using information-processing facilities to minimise security risks.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
6.2.1 Information security education and training	2	24-29

6.3 Responding to security incidents and malfunctions

Objective: To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

Incidents affecting security should be reported through appropriate management channels as quickly as possible.

All employees and contractors should know the procedures for reporting the different types of incident (security breach, threat, weakness or malfunction) that might affect the security of organisational assets. They should be required to report any observed or suspected incidents as quickly as possible to the designated contact. The organisation should establish a formal disciplinary process for dealing with employees who commit serious breaches. To address incidents properly, evidence may need to be collected as soon as possible after the event (see 12.1.7).

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
6.3.1 Reporting security incidents	2	45 - 49
6.3.2 Reporting security weaknesses	2	50 - 51
6.3.3 Reporting software malfunctions		
6.3.4 Learning from incidents	2	52
6.3.5 Disciplinary process	2	53

7. Physical and environmental security

7.1 Secure areas

Objective: To prevent unauthorised access, damage or interference to business premises and information.

Critical or sensitive business information-processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage and interference.

The protection should match the identified risks. A clear-desk and clear-screen policy is recommended to reduce the risk of unauthorised access or damage to papers, media or information-processing facilities.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
7.1.1 Physical security perimeter	7	10 - 15
7.1.2 Physical entry controls	7	32 - 33
7.1.3 Securing offices, rooms and facilities	7	51 - 52
7.1.4 Working in secure areas	4	16 - 19
7.1.5 Isolated delivery and loading areas	7	7 - 19, 32 - 33

7.2 Equipment security

Objective: To prevent loss, damage or compromise of assets, or interruption to business activities.

Equipment should be physically protected from security threats and environmental hazards.

Protection of equipment, including that used off-site, is needed to reduce the risk of unauthorised access to data and to protect against loss or damage. This should also apply to where equipment is and how it is disposed. Special controls may be needed to protect against hazards or unauthorised access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
7.2.1 Equipment siting and protection	7	2 - 5
7.2.2 Power supplies		
7.2.3 Cabling security		
7.2.4 Equipment maintenance	6	5
7.2.5 Security of equipment off-premises	6	12 - 17
7.2.6 Secure disposal or re-use of equipment	8	37 - 46

7.3 General controls

Objective: To prevent compromise or theft of information or information-processing facilities.

Information and information-processing facilities should be protected from disclosure to, change to or theft by unauthorised persons; and controls should be set to minimise loss or damage.

Handling and storage procedures are considered in 8.6.3.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
7.3.1 Clear-desk and clear-screen policy	4	39 - 41
7.3.2 Removal of property	4	47

8. Communications and operations management

8.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information-processing facilities.

Responsibilities and procedures for managing and operating all information-processing facilities should be set. This includes developing appropriate operating instructions and incident-response procedures.

Duties should be segregated (see 8.1.4), where appropriate, to reduce the risk of negligent or deliberate system misuse.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
8.1.1 Documented operating procedures	8	12
8.1.2 Operational-change control	8	8
8.1.3 Incident-management procedures	8	12-20
8.1.4 Segregation of duties	8	24
8.1.5 Separation of development and operational facilities	8	52
8.1.6 External facilities management	6	22 - 24

8.2 System planning and acceptance

Objective: To minimise the risk of systems failures.

Advanced planning and preparation are needed to ensure adequate capacity and resources.

Projections of future capacity should be done, to reduce the risk of system overload.

The operational requirements of new systems should be set up, documented and tested prior to being accepted or used.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
8.2.1 Capacity planning		
8.2.2 System acceptance	8	5

8.3 Protection against malicious software

Objective: To protect the integrity of software and information.

Precautions are needed to prevent and detect the introduction of malicious software.

Software and information-processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses (see also 10.5.4) and logic bombs. Users should know about the dangers of unauthorised or malicious software; and managers should, where appropriate, use special controls to detect or prevent its introduction. In particular, precautions must be taken to detect and prevent computer viruses on personal computers.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
8.3.1 Controls against malicious software	8	21-22

8.4 Housekeeping

Objective: To maintain the integrity and availability of information-processing and communication services.

Routine procedures should be set up to carry out the agreed back-up strategy (see 11.1), taking back-up copies of data, rehearsing their timely restoration, logging events and faults and monitoring the equipment environment where appropriate.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
8.4.1 Information back-up	8	36
8.4.2 Operator logs		
8.4.3 Fault logging		

8.5 Network management

Objective: To safeguard information in networks and protect the supporting infrastructure.

Attention must be given to managing the security of networks that may span organisational boundaries.

Additional controls may also be needed to protect sensitive data passing over public networks.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
8.5.1 Network controls	8	23-25

8.6 Media handling and security

Objective: To prevent damage to assets and interruptions to business activities.

Media should be controlled and physically protected.

Appropriate operating procedures should be set up to protect documents, computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft or unauthorised access.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
8.6.1 Management of removable computer media	8	26-30
8.6.2 Disposal of media	8	38-42
8.6.3 Information-handling procedures	4 8	36-103 51 - 103
8.6.4 Security of system documentation	8	47

8.7 Exchanges of information and software

Objective: To prevent loss, modification or misuse of information exchanged between organisations.

Exchanges of information and software between organisations should be controlled and compliant with any relevant legislation (see Clause 12).

Exchanges should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit should be set up. The business and security implications of electronic-data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
8.7.1 Information and software exchange agreements	8	55
8.7.2 Security of media in transit	8	32-35
8.7.3 Electronic commerce security		
8.7.4 Security of electronic mail	3	Annexes A-F
	8	55-63
8.7.5 Security of electronic office systems	4	73 - 77
	8	87 - 89
8.7.6 Publicly available systems	8	58-63
8.7.7 Other forms of information exchange	4 8	32, 53 - 62, 75-77, 87, 55-56

9. Access control

9.1 Business requirement for access control

Objective: To control access to information.

Controls on access to information and business processes should be based on business and security needs.

These controls should meet information-dissemination and authorisation policies.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
9.1.1 Access-control policy	7	32-50
	9	1-13

9.2 User access management

Objective: To prevent unauthorised access to information systems.

Formal procedures should control the allocation of access rights to information systems and services.

These procedures should cover all stages in the lifecycle of user access, from registering new users to de-registering users who no longer need access. Special attention should be given, where appropriate, to privileged access rights which allow users to override system controls.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
9.2.1 User registration	9	16 - 18
9.2.2 Privilege management	9	1 - 10
9.2.3 User password management	9	25-31
9.2.4 Review of user-access rights	9	14

9.3 User responsibilities

Objective: To prevent unauthorised user access.

The co-operation of authorised users is essential for effective security.

Users should know their responsibilities for maintaining effective access controls, particularly regarding passwords and the security of user equipment.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
9.3.1 Password use	9	15, 25-27
9.3.2 Unattended user equipment	9	33

9.4 Network access control

Objective: Protecting network access.

Access to both internal and external networked services should be controlled.

Controls are needed so that users who have access to networks and network services do not compromise the security of these network services; this includes:

- appropriate interfaces between the organisation's network and public networks or those owned by other organisations
- appropriate authentication mechanisms for users and equipment
- control of user access to information services.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
9.4.1 Policy on use of network services	8	23-25
9.4.2 Enforced path		
9.4.3 User authentication for external connections	9	56
9.4.4 Node authentication	9	56
9.4.5 Remote diagnostic port protection	8	80
9.4.6 Segregation in networks	9	49

9.4.7 Network connection control		
9.4.8 Network routing control		
9.4.9 Security of network services		

9.5 Operating-system access control

Objective: To prevent unauthorised computer access.

Security facilities at the operating-system level should restrict access to computer resources. These facilities should:

- identify each authorised user, and if necessary their terminal or location
- record both successful and failed system accesses
- authenticate users, with quality passwords if using a password-management system (see 9.3.1 d)
- where appropriate, restrict connection times.

Other access-control methods, such as challenge-response, may be justified by business risk.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
9.5.1 Automatic terminal identification		
9.5.2 Terminal log-on procedures	9	7 - 11
9.5.3 User identification and authentication	9	15
9.5.4 Password-management system	9	25-31
9.5.5 Use of system utilities	8	17
9.5.6 Duress alarm to safeguard users		
9.5.7 Terminal time out	9	22
9.5.8 Limitation of connection time	9	23

9.6 Application access control

Objective: To prevent unauthorised access to information in information systems.

Security facilities should restrict access to application systems.

Logical access to software and information should be limited to authorised users.

Application systems should:

- control user access to information and application system functions, per a defined, business, access-control policy
- prevent unauthorised access to any utility or operating-system software that can override system or application controls
- not compromise the security of other systems with which information resources are shared
- allow access to only the owner of information, or to other authorised users or groups.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
9.6.1 Information-access restriction	9	48
9.6.2 Sensitive system isolation	9	49

9.7 Monitoring system access and use

Objective: To detect unauthorised access.

Systems should be monitored to detect deviation from access-control policy, and to record monitorable events, for use as evidence in case of security incidents.

System monitoring verifies whether controls work and conform to an access-policy model (see 9.1).

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
9.7.1 Event logging	8	17
9.7.2 Monitoring system use	8	12
9.7.3 Clock synchronisation	8	13

9.8 Mobile computing and teleworking

Objective: To ensure information security when using mobile-computing and teleworking facilities.

Protection should match the risks from these specific ways of working. With mobile computing, the risks of working in an unprotected environment should be considered and appropriate protection applied. With teleworking, the organisation should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
9.8.1 Mobile computing	9	53-60
9.8.2 Teleworking	4	49
	9	53-60

10. System development and maintenance

10.1 Security requirements of systems

Objective: To ensure that security is built into information systems.

Requirements apply to infrastructure, business applications and user-developed applications. The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed before developing information systems.

All security requirements, including the need for fallback arrangements, should be identified at the requirements phase of the project and justified, agreed and documented as part of the overall business case for an information system.

AS/NZ ISO/IEC 1779:2001 Reference	**Security in the Government Sector Reference**	
	Chapter	**Paragraph**
10.1.1 Security requirements analysis and specification	9	1-4

10.2 Security in application systems

Objective: To prevent loss, modification or misuse of user data in application systems.

Appropriate controls and audit trails or activity logs should be designed into application systems, including user-written applications. These should include the validation of input data, internal processing and output data.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
10.2.1 Input-data validation	8	48 - 49
10.2.2 Control of internal processing	8	49
10.2.3 Message authentication		
10.2.4 Output-data validation		

10.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information.

Cryptographic systems and techniques should protect information that is considered at risk and not adequately protected by other controls.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
10.3.1 Policy on the use of cryptographic controls	8	98-107
10.3.2 Encryption	8	98-107
10.3.3 Digital signatures	9	28-30
10.3.4 Non-repudiation services	8	100
10.3.5 Key management	8	106

10.4 Security of system files

Objective: To ensure that IT projects and support services are conducted in a secure manner. Access to system files should be controlled.

Maintaining system integrity should be the responsibility of the user, function or development group that owns the application system or software.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
10.4.1 Control of operational software	8	10
10.4.2 Protection of system test data	8	52 - 54
10.4.3 Access control to programme source library	8	53

10.5 Security in development and support process

Objective: To maintain the security of application system software and information.

Project and support environments should be strictly controlled.

Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed against compromise of the security of either the system or the operating environment.

AS/NZ ISO/IEC 1779:2001 Reference	Security in the Government Sector Reference	
	Chapter	**Paragraph**
10.5.1 Change-control procedures	8	8 - 11
10.5.2 Technical review of operating-system changes	8	10
10.5.3 Restrictions on changes to software packages	8	50-51
10.5.4 Covert channels and Trojan code	8	21
10.5.5 Outsourced software development	6	22-24

Glossary of Abbreviations

Abbreviation	Meaning
ADAS	Automated Document Accounting System
AISEP	Australasian Information Security Evaluation Programme
AusCERT	Australian Computer Emergency Response Team
BCP	Business Continuity Plan
CC	Common Criteria
CCB	Configuration Control Board
CCIP	Centre for Critical Infrastructure Protection
CCTV	Closed Circuit Television
CDMA	Code Division Multiple Access
CD ROM	Compact Disk - Read Only Memory
CERT	Computer Emergency Response Team
COMPUSEC	Computer Security
COMSEC	Communications Security
DCCS	Departmental Committee on Computer Security
DMZ	De-militarised Zones
DSO	Departmental Security Officer
EAL	Evaluation Assurance Level
Fax	Facsimile
GCSB	Government Communications Security Bureau
GCSC	Government Communications Security Committee
GMT	Greenwich Mean Time
GSM	Global System for Mobile Communication
iaw	in accordance with
ICS	Interdepartmental Committee on Security
ID	Identification
IDS	Intruder Detection Systems
INFOSEC	Information Systems Security
IPR	Intellectual Property Rights
IS	Information Security
ISSP	Information System Security Policy
ISSM	Information Systems Security Manager

IT	Information Technology
ITSEC	Information Technology Security
LAN	Local Area Network
MDT	Mechanical Document Transfer System
MFAT	Ministry of Foreign Affairs and Trade
MOD	Ministry of Defence
NSCSS	National Supervisory Council for Security Systems
NZDF	New Zealand Defence Force
NZSA	New Zealand Security Association Inc
NZSIS	New Zealand Security Intelligence Service
NZSIT	New Zealand Security in Information Technology Publications
ODESC	Officials Committee for Domestic and External Security
OS	Operating System
PABX	Private Automatic Branch Exchange
PC	Personal Computer
PIDS	Perimeter Intrusion-Detection System
PIN	Personal Identification Number
PISG	Private Investigators and Security Guards
PKC	Public Key Cryptography
PSM	Protective Security Manual
SOP	Standard Operating Procedure
SSC	State Services Commission
SSP	System Security Plan
TECSEC	Technical Security
TRA	Threat and Risk Assessment

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W