New Zealand Security of Information Technology Publication 101

INFORMATION TECHNOLOGY SECURITY POLICY HANDBOOK

CHAPTER 1

EXECUTIVE POLICY STATEMENT

Contents

101. The Executive Policy Statement is used for communicating the high-level departmental policy for information systems security to all people that use, are responsible for, or depend on, the department's information systems. It should be concise and unambiguous, but at the same time provide a solid foundation for the remaining chapters and the security plans, SOPs, etc that may need to be promulgated as detailed information systems security policy for the department. The Executive Policy Statement should not generally be longer than five pages.

102. An Executive Policy Statement generally consists of the following sections:

a. Introduction

b. Relevant Legislation and Policies

c. Information Security Philosophy

d. IT Security Overview

Introduction

103. The introductory section should set the scene by introducing the requirement for security and on whose authority it will be implemented. It may be advantageous to bind the need for security to organisational goals and objectives and to note that security is the responsibility of all personnel. The introductory section may also establish the authority of the associated detailed IT security instructions. It may be in the form of a introductory letter from the organisation's Chief Executive, for example:

Introduction

The Department has an ethical obligation and a legal and official mandate to protect the substantial amount of sensitive personal and official information we handle. Protection of this information from unauthorised viewing and copying is a critical aspect of the operation of the organisation, as are ensuring the integrity and availability of our information resources and services. While information technology has allowed us to handle information in ways never before envisaged, if we do not manage it properly it could also potentially

leave us open to sabotage, fraud, theft, vandalism, information capture and misuse in ways and magnitudes not previously possible.

This policy statement directs the philosophy and strategy for application of information security within the Department to minimise the likelihood and potential impact from such threats. The frameworks and management processes are addressed in the next two chapters, while the specific information security controls are provided in the remaining chapters.

Please note that security is the responsibility of all staff , not just those people filling roles with specific security duties written into their goals and objectives. The requirements described in this policy have been decided after careful consideration of our legal and ethical obligations to the NZ Government and citizens and to staff. I expect all staff to follow them. If, for any reason, they cannot be complied with a concession must be applied for through the Director of Corporate Security.

I also encourage you to submit any comments or suggestions you have regarding improvement of our information security policies or practices to the Director of Corporate Security.

These policies are in effect from the 1st of January 2000.

Chief Executive

1 December 1999

Relevant Legislation and Policies

104. The Relevant Legislation and Policies section of the Executive Statement should identify all legislation which directs security measures to be taken to protect information held or processed by the department. This section should also list any relevant internal directives or policies.

105. The publication *Security in Government Departments* provides national doctrine for the protection of official information. Legislation relevant to all departments has been enacted to direct the type and extent of protective measures required for official information. In addition, some departments will also be covered by specific legislation.

106. This section might also contain references to other national and international guidance documents, standards, and codes of practice relating to information systems security, particularly where they could be used as the basis for information system acquisition or outsourcing.

107. An example of a Relevant Legislation and Policies section is as follows:

Relevant Legislation and Policies

Government must protect its sensitive information from unauthorised disclosure. The primary legislative instruments with which it does this are as follows:

- ***The Official Information Act 1982*** *The Department has an obligation to protect official information to the extent consistent with the public interest.*
- ***The Privacy Act 1993*** *Personal information must be protected from unauthorised disclosure and use, and proper procedures must be followed for data matching between departments.*
- ***The Archives Act 1957*** *Appropriate measures must be taken to retain and preserve public records, including selected electronic records.*
- ***The Copyright Act 1994*** *Copyright provisions on commercial software must be recognised and enforced throughout the Department.*
- ***Doctrinal Publications*** *National doctrine relating to information systems security is provided in the publication Security in Government Departments: Part 2, promulgated by the Department of Prime Minister and Cabinet. Detailed guidance on the application of information systems security is provided by the GCSB in the form of the New Zealand Communications Security Standard (NZCSS) and New Zealand Security of Information Technology (NZSIT) series of publications.*

108. All policies and implementations must also comply with employment relations legislation and occupational health and safety regulations.

Information Security Philosophy

109. Information security is concerned with the confidentiality of sensitive information; the availability of information and information services; system and data integrity; and accountability of user actions in regards to the organisation's information resources. Therefore, the organisation's information security philosophy should encompass ongoing processes to assess the risks of the various events that could occur to affect those aspects of security, and processes to manage that risk accordingly.

110. The information security philosophy should take into account the culture of the organisation and the environment it operates in. While technological measures will mitigate many risks, a truly effective protection system will take a much more holistic view and will require all staff to consider information security issues as part of their day to day routine.

111. In 1990, the Information, Computer and Communications Policy (ICCP) Committee of the Organisation for Economic Co-operation and Development (OECD) established a Council to prepare guidelines for the security of information systems. The Council included government delegates, scholars in the fields of law, mathematics, and computer science, and representatives of the private sector including computer and communications providers and users. The Council met between January 1991 and September 1992 to prepare the *Recommendation of the Council Concerning Guidelines for the Security of*

Information Systems. In 1992 the 24 OECD member countries, including New Zealand, adopted the Guidelines.

112. The Guidelines detail nine principles of information systems security and recommend that member countries consult, coordinate, and cooperate in their implementation. The adoption of these Guidelines will provide departments with an internationally accepted security framework within which trustworthy information systems may be developed. A summary of the principles follows:

113. **Accountability Principle** The responsibilities and accountability of owners, providers, and users of information systems should be explicit. Accountability is an important personnel management issue and job descriptions should include security responsibilities as appropriate. The accountability of executive management, systems management and administration, designers, programmers, information systems security staff, auditors, and system users should all be documented and promulgated. From an information systems perspective, accountability also requires that all initiators of computer and network activity be identified. Computer operating and application systems should include audit trails to record system activity and identify those responsible for it, and an appropriate level of auditing should be established.

114. **Awareness Principle** All people with a responsibility for information systems security i.e., those identified in the application of the Accountability Principle, should have sufficient knowledge to carry out their responsibilities correctly. However, while awareness will assist those with a legitimate interest in the security of a system, it can also help those who would seek to attack the system. It is important, therefore, that the Awareness Principle is applied only to a level consistent with maintaining system security.

115. **Ethics Principle** Information systems should be operated in such a manner that the rights and legitimate interests of others are respected. "Others" in this regard means individuals and groups in some way associated with the information on the system. The implementation of this principle must take into account the environment, culture and social mores within which the system operates. For example, an Internet user is likely to consider security to be of lesser importance than usability, whereas hospital patients may consider the privacy of their medical records to be of paramount concern.

116. **Multidisciplinary Principle** Information systems should be designed with consideration for all relevant viewpoints, including legislation relevant to the system, relevant technical standards relating to security, and user perceptions of security. An example of this principle is the standard *AS/NZS4444: Information Systems Security Management*. This provides a multidisciplinary standard for security covering legal, physical, personnel, and technical security measures.

117. **Proportionality Principle** Not all information systems require absolute or maximum security. Security measures should be applied in proportion to the threats to and vulnerabilities of the system and the projected impact of security violations. This is best achieved by carrying out a formal risk analysis of the information system. The need for departmental risk analysis was

identified in the State Services Commission 1991 report: *A Review of IT in the Public Sector*. The GCSB's CATALYST software support tool, together with risk analysis training, is available to Government departments to assist staff to undertake risk analysis work.

118. **Integration Principle** The cost and complexity of information systems security should be minimised by co-ordinating and integrating departmental security practices and procedures, and merging these, in turn, with other business and corporate objectives. There is currently a strong business focus on quality assurance and in particular the ISO 9000 standards. Consequently, Standards New Zealand has produced *NZS6656: Code of Practice for the Implementation and Operation of a Trustworthy Computer System*, an information systems security standard which integrates information systems security practices with the ISO 9000 business quality assurance procedures.

119. **Timeliness Principle** Public and private parties, at both national and international levels, should act in a timely, co-ordinated manner to prevent and respond to breaches of information system security. With interconnected information systems that span the globe, the potential for simultaneous widespread damage to information systems requires rapid and effective co-operation on a global scale. This principle recognises the need for the public and private sectors to establish mechanisms and procedures to support an effective incident response.

120. **Reassessment Principle** Information systems change over time, as do the threats to the systems. The security of information systems should therefore be periodically reassessed.

121. **Democracy Principle** The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society. This principle highlights the fact that information systems, particularly those in use by Government, may need to be designed in such a way as to balance security issues with the greater good of society. The data matching clauses within the Privacy Act 1993 show how the Democracy Principle can be applied.

122. The following is an example of an Information Security Philosophy section:

Information Security Philosophy

The Department's information, whether stored in hard copy or electronic form, must be protected from unauthorised modification and access. All manual and computerised systems must provide protection to information to ensure that it is accurate, reliable, and available to users in a timely manner. The collective rules, procedures, and products used to achieve this are known as Information Security.

All information security decisions should incorporate the following concepts developed from the OECD principles for information security:

- ***Accountability Principle*** *Executive staff, systems management and administration, designers, programmers, information systems security staff, auditors, and system users are all to be accountable for their responsibilities with respect to the security of information systems. System designers, in particular, are to ensure that the Department's obligations detailed in the relevant legislation and policies are properly addressed.*
- ***Awareness Principle*** *The Department will provide all staff with sufficient training in the threats to information and the application of information security to carry out their responsibilities correctly.*
- ***Ethics Principle*** *IT systems in the Department will be monitored to ensure they are used only for legitimate purposes. They will not be used to transmit or store non-official material, particularly any material incorporating derogatory or personal views of individual staff members, material of a socially unacceptable nature, or illegal copies of software.*
- ***Multidisciplinary Principle*** *Security procedures and plans will be designed taking into account the spectrum of relevant requirements. The views of technical, legal, administrative, and user staff will be considered in order to establish the optimal level of security for each system.*
- ***Proportionality Principle*** *Not all information systems require absolute or maximum security. Security measures will be applied as appropriate to the threats, vulnerabilities, and projected impact of security violations. The Department will apply this principle, where appropriate, through the use of risk management techniques.*
- ***Integration Principle*** *The cost and complexity of information systems security is to be minimised by co-ordinating and integrating departmental security practices and procedures with other corporate practices and procedures. For example, an IT system which operates wholly within a secure environment may require less stringent physical and technical protection than one which is within non-restricted office space.*
- ***Timeliness Principle*** *Department staff will act in a timely manner, using formal incident response procedures, to prevent and to respond to breaches of information systems security.*
- ***Reassessment Principle*** *Information systems, and the threats under which they operate, change over time. The security of the Department's information systems is to be reassessed periodically.*
- ***Democracy Principle*** *Security measures applied to the Department's information systems will be compatible with the legitimate use and flow of data and information in a democratic society, as detailed in the data matching clauses within the Privacy Act.*

IT Security Overview

123. There are six inter-dependant strategies for implementation of information security: policy development; risk management; system certification; education and training; trustworthy operation; and incident response.

a. **Policy Development** This manual provides an approach to policy development that follows international standards for information management.

b. **Risk Management** The security requirements of any particular system will need to be defined by reference to a predefined set of minimum standards for security, through the conduct of a risk analysis, or through a combination of both. Adopting a minimum set of security standards can be effective where a high level of security assurance is required for a specific architecture, but it can lead to the proliferation of unnecessary controls in lower sensitivity systems. The appropriate level of security can be defined using the formal risk management methodology promulgated by the GCSB as *NZSIT 104: Risk Analysis of Government Computer Systems*.

c. **System Certification** The process of defining the security requirements of a system, and confirming that the implemented system adequately meets the defined requirements, is known as system certification. This involves stating in a predefined way the security policy of a system, the security plan for the system, and the standard operating procedures to be used throughout the life of the system. Certification documents are normally passed to departmental executives for official acceptance of the system's implemented security posture.

d. **Education and Training** User and stakeholder knowledge and buy-in to the information security policies and safeguards are crucial aspects of information security. There should also be processes in place to ensure that staff are aware of the various threats and vulnerabilities inherent in the information systems they use or are responsible for.

e. **Trustworthy Operation** A system security plan and standard system operating procedures will provide an initial security posture, but may prove to be inadequate against new threats or may be affected over time by changes in the system's configuration. It is therefore important to supplement the certification process with an ongoing configuration management inspection programme to verify that the system's security posture remains intact, and to detect any signs of system intrusion.

f. **Incident Management** It is likely that, at some time in the life of a system, a security incident will occur. The seriousness of the incident will, in part, be dictated by the extent to which the department is prepared for the incident. Incident detection and response measures that need to be established in advance of an incident include software and data backup regimes, disaster recovery and business continuity plans, and system monitoring, communications procedures and offender pursuit and prosecution procedures.

124. An example of the IT Security Overview section of an Executive Policy Statement is as follows:

IT Security Overview

IT Security in the Department is implemented through six strategies: dissemination of policy and procedures, staff education and training, risk management, system certification, trustworthy operations, and incident response.

- ***Development of Policy and Procedures*** *This policy promulgates the Department's baseline IT security requirements. It will be updated and reissued periodically. Individual security plans must be also developed and maintained for each system. The appropriate security plans and procedures must be available and understood by everyone who uses or manages specific systems. However, they are only to be accessible to those people with a legitimate need-to-know.*
- ***Risk Management*** *Risk Management techniques will be used to achieve a cost-effective level of security for the Department's IT systems. A statement of risk will be formally established for each system and maintained throughout its life. Regardless of risk level, all IT systems processing classified information will conform to the security standards, instructions, and recommendations detailed in national doctrine. Systems are to be inspected from time to time to ensure their security posture is maintained and to detect any signs of attack.*
- ***System Certification*** *The security requirements of each of the Department's IT systems are to be formally articulated in a system security policy, and the means by which an appropriate security posture is achieved are to be formally stated in an associated system security plan and standard set of operating procedures. Executive overview of IT security is to be achieved through the adoption of formal system certification and accreditation procedures.*
- ***Staff Education and Training*** *Education and training in the vulnerabilities, risks, and safeguards relating to information systems is a prerequisite to developing an adequate security posture. All staff involved with the design, development, management, operation, or use of computer systems are to complete an IT security awareness course. Selected staff will also attend the advanced IT security training courses provided by the Government Communications Security Bureau.*
- ***Trustworthy Operation*** *The operation of IT systems within the Department is to conform, where appropriate, to the New Zealand Standards NZS6656: Implementation and Operation of a Trustworthy Computer System and NZS4444: Information Security Management. Regular inspections of the system are to be carried out to ensure the implemented security posture is maintained throughout the life of the system.*
- ***Incident Response*** *System administrators are to monitor activity on the IT systems under their purview and formally report any unauthorised access attempts. All staff are to report any security breaches that come to their attention. Disciplinary action will be taken against any staff member who violates IT security rules or procedures.*

CHAPTER 2

SECURITY ORGANISATION

Security Responsibilities

201. Departmental management will need to ensure that the requirements detailed in the Information Security Policy are appropriate and are properly implemented. This will involve developing and promulgating the departmental policies, standards and procedures, identifying and assigning staff to carry out in-house security monitoring and verification activities, and providing adequate

training and resources. These actions should be carried out within a well-defined management framework.

202. The Interdepartmental Committee on security, through the manual *Security in Government Departments,* assigns to Chief Executives the responsibility for all aspects of security within their departments. The Chief Executive should, in turn, delegate the authority and responsibility for ensuring that IT security requirements are implemented and maintained within the organisation. This could be a function of the Departmental Security Officer (DSO), or it may be more appropriate to appoint a separate IT Security Officer.

203. The Security Organisation section of each department's information security policy should clearly state the responsibilities and authorities of the various staff involved with aspects of information systems security. Detailed responsibilities should be included in the appropriate staff member's terms of reference or job description. A clear statement of security responsibilities is particularly important for those personnel who need the organisational freedom and authority to initiate action to prevent or respond to security incidents, and to verify the implementation of security solutions.

204. The following responsibilities will need to be delegated to ensure that all aspects of departmental IT security are properly addressed:

a. overall management of the security of information and information systems;
b. development, maintenance, and promulgation of IT security policy, standards, and procedures;
c. co-ordination and conduct of IT risk analysis;
d. planning and implementation of security measures for each IT system;
e. IT security awareness training for staff;
f. coordination and conduct of IT systems certification;
g. coordination and conduct of inspections of IT systems;
h. administration of computer user IDs and system access privileges;
i. reporting of IT systems security breaches; and
j. coordination of the response to IT security incidents.

205. An example of a Responsibilities section is as follows:

Responsibilities

The Chief Executive is responsible for all matters of security in the Department.

This responsibility is delegated to the following officers:

Director of Corporate Security. *The Director of Corporate Security is responsible for maintenance of the Department's security policy, and IT security incident response. He or she also holds the position of* ***Departmental Security Officer (DSO)****.*

Director of IT. *The Director of IT is responsible for:*

- *development, maintenance, and promulgation of the IT security circulars;*
- *design and development of security measures in the Department's IT systems;*
- *providing IT security awareness training to staff; and*
- *conduct of the IT systems certification, risk analysis, and inspection programmes.*

Group Managers. *Group Managers are responsible for the security of all IT systems within their purview. However, they may delegate routine IT security matters to other staff members.*

Staff. *All staff are responsible for the protection of their assigned passwords and access tokens, their proper use of IT systems, and reporting of IT systems security breaches.*

IT Security Forum

206. Information security is a responsibility shared by, and effects, all members of the management team. An IT Security Forum can be an important mechanism to ensure that there is clear direction, co-ordination, and management support for IT security initiatives and policies and input from all applicable stakeholder groups. This forum may be integrated into an existing IT or security forum.

207. A typical terms of reference for an IT security forum could be:

IT Security Forum : Terms of Reference

The IT Security Forum is responsible to the Chief Executive for evolving IT security requirements and implementation, and for monitoring the application of security in all departmental IT systems. The Forum comprises:

- *Director of IT (Chair)*
- *Director of Corporate Security*
- *Unit Managers*

Specific responsibilities of the IT Security Forum are:

- *review and approve information security policy and overall IT security responsibilities;*
- *co-ordinate major initiatives to enhance information security, e.g., security awareness campaigns;*
- *monitor the exposure of information assets to major threats by ensuring all systems are covered by a current risk profile;*
- *standardise specific security methodologies and processes for information security, e.g., risk assessment; and*
- *establish security incident response policy and procedures*
- *monitor adherence to the security policies and standards.*

Configuration Management Board

208. Configuration management provides a mechanism for identifying, controlling, and tracking the versions of each security-relevant component of a computer system. A configuration management system should be established for all departmental systems to:

a. uniquely identify each major information system component;
b. identify the versions of each component which together constitute a specific version of the information processing system;
c. control simultaneous updating of components by more than one person;
d. provide co-ordination for the updating of multiple components in one or more locations as required; and
e. identify and track all actions and changes resulting from a change request, from initiation through to release.

209. Configuration management procedures should include controls over all documents and data files that relate to configuration management. In particular, the procedures should ensure that appropriate documentation is available at all locations where operations essential to the effective functioning of the security system are performed, and ensure that obsolete documents are promptly removed from all points of issue or use. An appropriate methodology for implementing and operating a configuration management regime for Government computer systems is detailed in *NZSIT 105: Configuration Management.*

210. A document control procedure should be established to identify the current revision of software in order to preclude inadvertent reversion. Changes to departmental systems should be formally submitted for approval, and should be reviewed by a departmental Configuration Control Board (CCB).

211. An example of Terms of Reference for a CCB are as follows:

Configuration Control Board : Terms of Reference *The purpose of the Configuration Control Board (CCB) is to approve the baseline configuration management documentation, review the impact of all proposed changes, approve or decline proposed changes, and schedule approved changes into new system releases.*

The Configuration Control Board is to meet quarterly and at any other times as required by the System Sponsor.

The System Manager is responsible to the Configuration Control Board for maintenance of functional specifications, operating instructions, system change requests, and the Configuration Management (CM) List in accordance with NZSIT 105: Configuration Management.

The Configuration Control Board under the chairmanship of the System Sponsor is to:

- *oversee programmed and unprogrammed maintenance of the system;*
- *ensure the creation and maintenance of the CM List;*
- *maintain control of the configuration of each CM Item on the CM List;*
- *make recommendations on resource allocation relevant to the system;*
- *approve configuration changes and connections to the system;*
- *ensure that any proposed changes include the necessary changes to the supporting documentation;*
- *ensure that the accreditation status of the system is recorded and verify that documents pertaining to these processes are controlled by configuration management;*
- *verify that software, hardware and design documentation CM Items are traceable;*
- *ensure that the system change procedures are documented and understood by users and processing staff;*
- *assess when any proposed changes indicate the need for re-certification and advise accordingly;*
- *oversee certification and accreditation activities; and*
- *report quarterly on the configuration status of departmental IT systems.*

Security Advice and Assistance

212. Most organisations can benefit from specialist security advice. While such a service is ideally provided by an experienced in-house information security adviser, not all departments will be able to justify a specialist appointment. In such circumstances, a departmental technical representative should be identified to ensure continuity when dealing with outside consultants.

213. Departments requiring advice or assistance on any aspects of information systems security are encouraged, in the first instance, to contact the GCSB. Departmental IT security advisors should also be encouraged to liaise with their counterparts in other departments and agencies and with commercial security specialists where appropriate. Such exchanges will provide opportunities to share experience and assessments regarding security threats, and promote the adoption of consistent, proven security practices, helping to remove obstacles to inter-organisational dealings. However, exchanges of security information with commercial organisations should be restricted to ensure that unauthorised persons do not obtain details of departmental security measures. The quality of the information security advisers' assessment of security threats and advice on vulnerabilities and countermeasures will be an important factor in determining the effectiveness of the department's information security programme.

214. It is important that departmental information security advisors maintain appropriate contacts with law enforcement authorities & service providers to ensure that appropriate and timely assistance can be gained in the event of a security incident.

215. Information security advisers should be consulted at the earliest possible stage following a suspected security incident or breach, to provide a source of expert guidance or investigative resources. Although most security investigations will normally be carried out under internal management control, the information security adviser may be called on to advise, lead or conduct the investigation.

216. An example of a management directive regarding advice and assistance is as follows:

Security Advice and Assistance

The Departmental IT Security Officer is to be contacted immediately upon identification of a possible security incident. All liaison with the GCSB, other departments, and commercial security specialists on matters of departmental systems security is the responsibility of the IT Security Officer.

Outsourcing and Contractors

217. Access to departmental IT facilities, and particularly security subsystems, by contractors should be controlled. The controls should be agreed and defined in their contracts. Where applicable, the contract should explicitly name individuals and the conditions of their access. The contract should be in place before access to the IT facilities is provided.

218. The security of departmental IT systems might be put at risk by remote access from locations with an inadequate security regime. Where there is a business need to connect to a location under independent security control, a risk analysis should be carried out to identify any requirements for additional security measures. The risk analysis should take into account the type of access required, the value of the information at risk, the security measures employed by the contractor and the implications for the security of the departmental IT infrastructure.

219. The following example list of contract items may be appropriate:

Contractor Access to Departmental Systems

The following items are to be included in any contract with external suppliers involving access to departmental systems:

- *relevant departmental information security policies, including constraints on copying or disclosing departmental information;*

- *permitted access methods, and the control and use of unique user identifiers and passwords;*
- *descriptions of the services available to contractors;*
- *the procedures for specific access authorisation for contractor staff;*
- *the times and dates when the service is available;*
- *any relevant contingency arrangements;*
- *the respective liabilities of the parties to the agreement;*
- *the right to monitor, audit, and revoke contractor activity;*
- *the return or destruction of information and assets at the end of the contract;*
- *any required physical protection measures in contractor sites;*
- *required security mechanisms in contractor systems, e.g. anti-virus procedures;*
- *training obligations relating to security methods and procedures; and*
- *arrangements for reporting and investigating security incidents.*

220. The need to formalise control over IT security matters related to outsourcing or subcontractor relationships suggests that departments should allocate this responsibility to a management representative. This representative should be given the authority to deal with contractual matters which include, but are not limited to, defining the department's requirements to the supplier, answering questions from the supplier, approving the supplier's proposals, concluding agreements with the supplier, ensuring that the department observes the agreements made with the supplier; and defining acceptance criteria and procedures.

221. Where an outsourcing or contracting arrangement is in place, regular joint reviews involving the department and the supplier should be held, and minutes kept, to ensure conformance of the system or service to the agreed departmental specifications and to provide visibility for the results of acceptance tests, audits, and inspections.

CHAPTER 3

ASSET CLASSIFICATION AND CONTROL

Asset Inventories

301. All major information systems assets, including information, should be accounted for and have a nominated owner and/or custodian. The owner is responsible for ensuring that appropriate security measures are implemented and maintained throughout the life of the asset.

302. Inventories of assets help to ensure that effective security protection is maintained, and may be required for other business purposes, such as health and safety, insurance or financial reasons. An inventory should be drawn up of the major assets associated with each information system. Each asset, or group of assets, should be clearly identified and its ownership and security

classification agreed and documented. Examples of assets associated with information systems include:

a. **Information assets** Databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements;
b. **Software assets** Application software, system software, development tools and utilities;
c. **Physical assets** Computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation; and
d. **Services** Computing and communications services, other technical services (heating, lighting, power, air-conditioning).

The owner of each information asset is responsible for approving who may have access to it and the type of access they are permitted.

303. While the asset inventory should not be included in the security policy document, this section should define the process and requirements relating to the inventory, and may define, in broad terms, the value placed on each category of asset.

Information Classification and Marking Scheme

304. Information varies in sensitivity and criticality. A security classification system should be used to define an appropriate set of security protection levels, and to communicate the need for special handling measures to users. The use of a common marking system throughout Government ensures that all official information exchanged between departments will receive a common level of protection.

305. It is a requirement of Government that official information relevant to national security be marked, for confidentiality purposes, as RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET and protected accordingly. The marking scheme for integrity and availability of classified information, and for all aspects of other sensitive official information, is less well defined. Where there is a need to establish standards for integrity and availability, this section should include definitions for the levels of availability and integrity.

306. Security markings for official information should take account of business needs for sharing or restricting information, and the business impact of unauthorised access or damage to the information. A set of standard confidentiality markings for Government is detailed in the publication *Security in Government Departments*. Other markings, for information availability and integrity, may also need to be formally defined.

307. An example of a departmental marking scheme is as follows:

Information Sensitivity Marking Scheme

***Confidentiality**. These markings are to be used to clearly identify the sensitivity of the information to unauthorised disclosure, and to limit access to information. The confidentiality markings to be used are:*

- *CONFIDENTIAL - to be used, for example, on the department's strategies and tactics papers;*
- *RESTRICTED - e.g. operational plans, pre-release budgets, etc;*
- *SENSITIVE - all other highly-sensitive material that could not affect national security; and*
- *IN-CONFIDENCE - personal or commercial information, etc.*

***Integrity**. These markings are to be used to identify the required accuracy of the information and the restrictions on how the information may be modified. The following terms are to be used:*

- *STANDARD for normal purposes;*
- *MEDIUM where independent verification is required; and*
- *HIGH where unequivocally assured integrity is required.*

***Availability**. These markings are to be used to identify the timeframe in which information must be available to an authorised user. The following terms are to be used:*

- *ROUTINE for information required to be available within 24 hours;*
- *PRIORITY for information required to be available within 6 hours;*
- *IMMEDIATE for information required to be immediately available at all times.*

308. The responsibility for defining the classification of an item of information e.g., a document, data record, data file or diskette, and for periodically reviewing the classification, should rest with the originator or nominated owner of the data.

309. Output from IT systems containing classified or unclassified but sensitive information should carry an appropriate classification label that reflects the classification of the most sensitive data in the output. Output forms include printed reports, screen displays, magnetic media (tapes, disks, cassettes), electronic mail messages and file transfers.

Document and media destruction

310. Any waste material that could contain sensitive information must be disposed of in a secure manner. For paper copy this may include shredding or burning. For magnetic media it may be by degaussing or by overwriting the media (refer to NZSIT207.)

Media Destruction

Hardcopy waste containing sensitive information is to be placed in the 'burn' bags located beside the photocopier machines in each office. Computer media (e.g. floppy and hard disks and CDs) containing sensitive material must be passed through helpdesk before being removed from the Department or disposed of in any way. This includes computers that are to be sold or sent out for repair and media to be released to business partners.

CHAPTER 4

PERSONNEL SECURITY

Introduction

401. The remaining chapters of this handbook address a range of core security practices and procedures which have been compiled from the collective experiences of a variety of Government and private sector organisations. Not all will be relevant to all departments, as individual circumstances will dictate the suitability of each measure. However, a departmental security policy which has been developed through consideration of the following measures is likely to provide departments with an effective and acceptable policy.

402. The first group of security standards are the personnel security measures used to ensure staff are trustworthy and are managed appropriately.

Staff Trustworthiness

403. Departments should ensure that all personnel with access to sensitive information are trustworthy and understand their responsibilities. This can be achieved by the application of normal departmental personnel security standards relating to security vetting, information disclosure, and security incident procedures.

404. Security roles and responsibilities should be included in job descriptions where appropriate. These should include any general responsibilities for implementing or maintaining security policy, as well as any specific responsibilities for the protection of particular assets or the execution of particular security processes or activities.

Code of Conduct Agreement

405. Departmental staff should sign an appropriate confidentiality undertaking as part of their initial conditions of employment. This may be included in a Code of Conduct Agreement that establishes the principles of conduct that all employees are expected to observe. Contract personnel and

staff not already covered by an existing confidentiality agreement should also be required to sign the Code of Conduct prior to being granted access to departmental IT facilities. The agreement should be reviewed when there are changes to terms of employment or contracts.

Training and Review

406. Security training is important in ensuring that users are aware of information security threats and concerns, and are equipped to support the departmental security policy in the course of their normal work. Users should be trained in security procedures and the correct use of IT facilities. They should also be formally advised of the scope of their permitted access to IT systems and all specific restrictions such as import of personal floppy disks and unauthorised penetration testing.

407. There should be a formal disciplinary process for employees who violate departmental security policies and procedures. Such a process will also act as a deterrent to those who might be inclined to place the department's information in jeopardy through disregarding security procedures. The disciplinary process should be drawn up in accordance with the department's human resources philosophy and approved by management.

Personnel Security

All staff are to read and agree to comply with the Department's Information Security and Privacy agreement before they are to be given access to any official information or information systems. Staff must also attend the Training Unit's half-day IT Workshop within the first three months of employment, and attend the 2-hour IT Refresher Briefing at no more than two year intervals.

All staff who will use or be responsible for any of the systems described in ***IT Schedule A: Critical Systems*** *must have gained a Positive Vetting (PV) clearance through the Director of Corporate Security BEFORE he or she is to be permitted login or physical access to the system.*

Staff should be aware that system use and content may be monitored. All files, e-mails etc may be subjected to review by a representative of the Director of Corporate Security. Disciplinary measures may be taken against any person found breaking the Department's Acceptable Use policy.

Comments regarding improvements to information security in the Department are welcomed by e-mail to IT Security or by contacting the Director of Corporate Security directly. Submissions will be treated in confidence. If, for any reason, a contributing staff member wishes to remain anonymous, those suggestions, comments or alerts can be submitted via the intranet Webpage www.anydept.govt.nz/security/staffsay.html. No identifying information will be passed with the submissions unless the employee explicitly provides it.

CHAPTER 5

PHYSICAL AND ENVIRONMENTAL SECURITY

Secure Areas

501. The term *IT facility* is used to describe the building or premises in which significant IT equipment is operated. It is important that departmental IT facilities supporting critical or sensitive business activities be physically protected from unauthorised access, damage, and interference. IT facilities should be sited away from areas of public access or direct approach by public vehicles, and consideration should be given during siting to any security threats presented by neighbouring accommodation.

502. In addition to the general physical protection afforded by an IT facility, an additional boundary or boundaries should be placed around areas supporting particularly sensitive, critical or vulnerable operations or information. A physically isolated area for delivery and loading of supplies and equipment may also be required to reduce the opportunity for unauthorised access to the premises or to items in transit. Measures may also be required to reduce the risk of damage to equipment or loss of service due to problems in the physical environment. The specific security requirements for IT facilities can best be determined by a risk assessment.

503. The following is an example of baseline physical security measures for IT Facilities:

IT Facilities

Appropriate safety equipment is to be installed, such as heat and smoke detectors, fire alarms, fire extinguishing equipment and fire escapes. Safety equipment is to be checked regularly in accordance with manufacturers' instructions. Employees are to be properly trained in the use of safety equipment.

Specific controls to guard against unauthorised access to computer rooms located within IT facilities must be implemented. The minimum standard of control is as follows:

- *All personnel must wear visible identification within the facility and should be encouraged to challenge .*
- *Dedicated computer rooms should be physically contained within a larger restricted area for output processing and distribution.*
- *Visitors to a computer room must be supervised and their date and time of entry and departure recorded. Visitors are to be granted access only for a specific period and for an authorised purpose.*
- *Access to delivery and output pickup areas from outside of the building is to be restricted to identified, authorised personnel.*

- *The restricted delivery and pickup area is to be designed so that supplies can be unloaded, and output picked up, without gaining access to the restricted area of the facility.*
- *Incoming material is to be inspected for potential hazards before it is moved from the holding area to the point of use.*
- *Access rights to controlled areas are to be revoked immediately for staff where employment is terminated, or who are subject to disciplinary action likely to result in termination of employment.*

Doors and windows are to be locked when the facility is unattended. Additional, external protection may need to be considered for windows.

Fallback equipment and back-up media are to be sited at a safe distance to avoid damage from a disaster at the main site.

Hazardous and combustible materials are to be securely stored at a safe distance from the site. Combustible computer supplies such as stationery, other than immediate operational needs, are not to be stored within dedicated computer operations rooms.

Emergency procedures are to be fully documented and regularly tested.

504. Departments should adopt a 'clear desk' policy for papers and storage media in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours. The following guidelines might be applied:

Workspace Security Measures

Papers and disks are to be stored in cabinets when not in use, especially outside working hours.

Sensitive and Classified information is to be locked away in an approved fire-resistant cabinet when not being used.

Workstations must be protected by key locks, passwords or equivalent controls when not in use.

Incoming and outgoing mail points and unattended facsimile machines must be provided with adequate protection.

Equipment security

505. IT equipment should be sited or protected to reduce the risks from environmental hazards and to minimise the opportunity for unauthorised access.

506. IT equipment should be correctly maintained to ensure its continued availability and integrity. Critical equipment should be protected from power failures or other electrical anomalies. Consideration should also be given to the possible need for a stand-by power supply and/or an uninterruptable power supply (UPS). Such equipment should be regularly tested in accordance with the manufacturer's recommendations.

507. The following example shows how equipment control guidelines may be included in the baseline physical security standards:

IT Equipment

Where possible, equipment should be sited to minimise the risk from unauthorised casual access.

Countermeasures or contingency procedures are to be defined for environmental hazards such as fire, smoke, water, dust, vibration, chemical effects, electrical supply interference, and electromagnetic radiation.

Smoking, eating, and drinking is prohibited in computer equipment areas.

The use of special protection, such as keyboard membranes, should be considered where equipment is being operated in harsh environments.

Consideration should be given to isolating equipment requiring special protection to reduce the need for a higher level of general protection.

Consideration should be given to potential hazards originating from neighbouring floors and adjacent premises. Some form of security agreement with building owners and/or other tenants may be required to provide the necessary security assurance.

Manufacturers' instructions regarding the protection of equipment, such as its protection against exposure to strong electromagnetic fields, is to be observed at all times.

Equipment is to be maintained in accordance with the supplier's recommended service intervals and specifications.

Equipment is to be serviced or repaired only by authorised maintenance personnel.

A record of all faults or suspected faults is to be kept.

508. All departmental IT equipment used outside the department's premises should be subject to the same degree of security as that afforded to equipment used for the same activities on-site. The risk of damage, theft, and electronic eavesdropping will vary considerably between locations and should be taken into account in determining the most appropriate security measures. The following additional IT equipment guidelines may need to be considered:

Personal computers used at home for business activities are subject to strict virus avoidance controls. Explicit management approval is required for all off-site computer use in connection with departmental business.

Portable computers are particularly vulnerable to theft, loss or unauthorised access during travel. They must always be carried as hand luggage when travelling and must never be left unattended in a public area unless they can be locked to, or in, an immovable object. A GCSB-approved disk encryption product will also be used to prevent unauthorised access to the contents of the hard disk.

509. Official information can be compromised through the improper disposal of equipment. Procedures should be established to ensure that all items of equipment containing storage media, e.g. hard disk drives, are checked to ensure that any sensitive data and licensed software are removed or overwritten prior to disposal. Damaged storage devices containing very sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded. An appropriate guideline along the following lines should be included in the baseline security standards, for example:

All IT equipment must be carefully inspected prior to its disposal or release outside of departmental premises to ensure that it contains no official information, including any data remnants that might have been retained on the equipment after processing. Magnetic media is to be sanitised by overwriting.

Protection of cabling

510. Power and telecommunication cabling should be protected from interception or damage. The following is an example of the security standards relating to cabling:

Cabling

Power and telecommunications lines into IT facilities should be underground, where possible, or subject to adequate alternative protection.

Network cabling is to be protected from unauthorised interception and communications loss or damage by:

- *the use of conduits;*
- *avoiding routes through public areas;*
- *the use of data encryption;*
- *installation of locked rooms or boxes at inspection and termination points; and*
- *implementation of secondary transmission media and/or routings.*

General controls

511. The use of screen savers or screen shields should be considered for computer monitors in open areas or where public may have oversight of the screen.

512. Equipment, information or software should not be taken off-site without authorisation. Where appropriate, equipment should be logged out and logged back in when returned.

513. Laptop and palmtop computers are particularly at risk when taken outside of the controlled environment. In many cases it may be appropriate to encrypt the information on the device to prevent unauthorised access to the information. Cable locks may also be appropriate to secure the hardware from theft.

514. Visitors to the organisation should be clearly identified as such and should not be permitted uncontrolled freedom of movement around the premises.

General Controls

All workstations in located public areas must be fitted with anti-oversight shields and have password-locked screen savers enabled to activate on either 30 minutes of inactivity or activation of a 'hot-key' (however, hotkeys may not be used in place of a password for re-activation of the workstation).

Any computer equipment or media that is taken outside or the Department's premises must be sighted and logged with Helpdesk both on removal and return.

CHAPTER 6

COMMUNICATIONS AND OPERATIONAL SECURITY

General

601. Management of the security of computer systems and networks requires special attention, particularly of those networks that span organisational boundaries. Appropriate controls should be established to ensure the system is operated consistently and as planned over its entire lifecycle. Networked services should be managed in such a way as to ensure that connected users or services do not compromise the security of the other IT applications or services.

Operational Procedures

602. The procedures identified within the Security policy should be documented and provided to the applicable groups. Such Standard Operating Procedures (SOPs) should define the instructions for executing each job including: processing and handling of information; scheduling requirements; instructions for handling errors or exceptions; support contacts; output handling instructions; and system back-up, restart and recovery procedures. The SOPs may also consider segregation of duties in areas where there is a risk of accidental or deliberate misuse of the system or loss of integrity of the data. The security policy may give reference to this document or series of documents.

603. Major changes to the system or facility, not covered within SOPs, should be reviewed with reference to the security policy, and should be approved by the Configuration Control Board before implementation. Any resulting actions should be documented in a system or facility log.

Incident Management

604. Procedures should be established, documented and maintained for detecting any security breach or attempted breach, and establishing the cause. They should also define the corrective action to be taken and any recommendations on preventing a recurrence. Controls will be needed to monitor the implementation and effectiveness of any corrective action, including any required changes to existing procedures.

605. The following guidelines might be provided in the Management Directive:

Incident Handling

Incident handling procedures are to be developed for each system to cover system failures, loss of service, and errors resulting from breaches of security. These procedures are to be compatible with the Business Continuity Plan procedures and must include:

- *analysis and identification of the cause of the incident;*
- *planning and implementation of remedies to prevent recurrence;*
- *collection of audit trails and similar evidence for internal problem analysis and as evidence in relation to a potential breach of contract or regulatory requirements, and to support claims for compensation; and*
- *communication with business users and others affected by, or involved with, recovery from the incident.*

Action to correct and recover from security breaches and system failures must be defined so that:

- *only clearly identified and authorised staff are allowed access to live systems and data;*
- *all emergency actions taken are documented in detail;*
- *emergency action is reported to management and reviewed in an orderly manner; and*
- *the integrity of business systems and security controls is confirmed with minimal delay.*

606. All employees and contractors should be made aware of the procedures for reporting the incident and should be required to report any observed or suspected incidents as quickly as possible to the correct authority. A formal reporting procedure should be established, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. All employees and contractors should be familiar with the procedure.

Separation of Development and Operational Facilities

607. When development and testing activities are performed on the operational computing environment there is a high likelihood of the development work causing unintended changes to operational software and data or affecting the integrity of the system. Segregation of development and operational facilities is therefore desirable to reduce the risk of accidental changes or unauthorised access to the operational software, processes and data. The following is an example statement of separation controls:

Separation of Development and Production

Development and operational software are to be run on different processors or, at a minimum, in different operating domains.

System acceptance testing is to be carried out by staff independent of the system development team.

Updating of the operational program libraries is to be performed only upon authorisation from the system manager.

Executable code is not to be implemented on an operational system until evidence of successful testing and user acceptance is obtained, and the corresponding program source libraries have been updated.

An audit log of all updates to operational program libraries is to be maintained.

Previous versions of software are to be retained for contingency purposes.

Compilers, editors and other system utilities are not to be openly accessible on operational systems.

Different logon procedures are to be used for operational and test systems, to reduce the risk of confusion. Users are to use different passwords for these systems, and menus are to display appropriate identification messages.

Outsourcing of IT Services

608. The use of external facilities or contractors to manage one or more of an organisation's IT systems is common in Government. However, it does bring with it a number of new or increased threats. These can be brought about by the increased connectivity, staff loyalty issues, variations in policies and practices, staff turnover, or just by cultural differences between the two organisations. Therefore any exclusions or additions to the policies to make up for these variations should be documented either in the IT Security policy or in the applicable system security plan. All parties should be made aware of where the responsibilities lie for the various aspects of security management.

System Planning and Acceptance

609. Advance planning and preparation are required to ensure new or modified systems have adequate security, capacity and resources to meet the present and future requirements. The operational requirements should be established, documented and tested prior to acceptance of the system.

610. Projections of future computer capacity requirements should be made to ensure that adequate processing power and storage remain available. These projections should take account of new system requirements as well as current and projected trends in computer and network use. Mainframe and special purpose computing systems require particular attention because of the much greater cost and lead time for procurement of new capacity. For major new developments, operations staff should also be consulted at all stages in the development process to ensure the operational efficiency and maintainability of the proposed system design.

611. The following is an example of a system planning directive:

System Planning

All proposals for new systems must include a security plan that describes how the system satisfies the security requirements provided in this document and any other applicable security policy definitions. The System Design document must also include the minimum and optimal performance and capacity requirements expected from the system.

All new application proposals are to include evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times such as month end. Alternatively, they should include provision for additional equipment to maintain adequate resource levels.

All IT systems are to be subject to an ongoing performance monitoring regime. The measurement metrics will be agreed before the system is commissioned and will cover such aspects as system processing speed, capacity and security performance. Acceptable levels of service will be negotiated at least annually.

Malicious Software

612. Precautions are required to prevent and detect the introduction of malicious software. A range of malicious techniques exist to exploit the vulnerability of computer software to unauthorised modification. These techniques include computer viruses, network worms, Trojan horses, and logic bombs. Managers of IT facilities should be alert to the dangers of malicious software and should apply countermeasures to prevent or detect its introduction.

613. It is essential that virus prevention procedures and, as a second line of defence, virus detection measures be implemented on all PC systems. Users should be reminded that prevention of a virus attack will be far less costly than recovering their systems after an attack. The management of virus protection should be founded on sound security awareness, appropriate system access controls, and specific procedures such as those shown in the following example:

Malicious Software

The use of software not authorised by the Configuration Control Board is prohibited on departmental systems.

Approved anti-virus software and software change detection software is to be used wherever possible. Whenever a virus is detected the system's administrator is to be notified immediately. Virus software signature updates are automatically uploaded to workstations by the IT Division as required.

All disks and electronic files of uncertain or unauthorised origin are to be checked for viruses before use.

No executable files from the Internet are to be run on the Department's network. Network controls will be configured not to allow executable e-mail attachments and active Web content to pass into the network from the Internet. Where a file with such content does need to be used on a Department system, the file may be routed to the Helpdesk where it will be checked through a 'quarantine' procedure.

Back-up and Recovery Procedures

614. Back-up copies of essential business data and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all

essential business data and software can be recovered following a computer disaster or media failure. Back-up arrangements for individual systems should meet the requirements of business continuity plans. An example of back-up arrangements follows:

Backup Controls

At least three generations of back-up data must be retained for important business applications. System administrators should establish and formally document an appropriate schedule of full and incremental backups.

A minimum level of back-up information, together with accurate and complete records of the back-up copies, must be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.

Back-up data must be given an level of physical and environmental protection, consistent with the standards applied at the main site. The controls applied to media at the main site must be extended to cover the back-up site.

Backup data should be regularly checked, to ensure that they can be relied upon in an emergency.

615. Data should be retained for the period necessary to satisfy both business and legislative requirements. Data owners should identify the retention period for essential business data, and should establish any requirement for archive copies to be retained.

Network Management

616. A range of procedural controls are required to achieve and maintain network security. These may include:

a. *separation of responsibilities e.g., between computer systems and networks or between administration and usage audit;*
b. *allocation of responsibilities for equipment, including equipment in remote locations;*
c. *procedures for intrusion- and misuse detection and management;*
d. *guidelines for management of routers, firewalls, VPNs, remote access servers, etc; and*
e. *cryptographic key and equipment management.*

Data Storage Media Handling and Security

617. Computer media should be controlled and physically protected. Appropriate operating procedures should be established to protect tapes, disks, data cassettes, input/output data and system documentation from damage, theft, unauthorised access and virus attacks as appropriate.

618. Authorised couriers using approved modes of transport should be employed for media distribution between sites. A list of authorised couriers should be maintained and a procedure implemented to check the identification of couriers. Packaging should be sufficient to protect media from any physical damage likely to arise during transit. Special measures should be adopted, where necessary, to protect sensitive information from unauthorised disclosure or modification during transportation, including the use of locked containers, safe hand delivery, and tamper-proof packaging.

619. There should be clearly documented procedures for the management of removable computer media, such as tapes, disks, cassettes and printed reports. The following provides an example of the controls that may be established for media security:

Storage Media Security

All media is to be marked in order to identify the maximum sensitivity or classification of information held on it.

Media containing unclassified but sensitive material may be distributed through normal mail channels. Media containing classified material that has been encrypted using an approved encryption scheme may also be distributed through normal mail services. Media containing unencrypted, classified information is to be delivered through approved safe hand channels only.

A formal record of the authorised recipients of media containing classified information is to be kept and receipt notification requested.

Media may not be removed from the department without written authorisation. An audit record of all such removals is to be maintained.

All media is to be stored in a safe, secure environment, and in accordance with the manufacturers' specifications.

Media no longer required and planned for release or disposal from the department is to be purged in an approved manner before release. Media holding up to and including CONFIDENTIAL information may be overwritten with an approved utility; media having held higher grade information must be destroyed.

Protection of System Documentation

620. System documentation may contain a range of sensitive information relating to descriptions of applications processes, procedures, data structures, and authorisation processes. The following is an example of the controls that might be applied to protect system documentation from unauthorised access:

System Documentation

System documentation can in many cases be of significant benefit to a would-be attacker. It is therefore required that:

- *system documentation is to be physically secured after hours in lockable cabinets;*
- *distribution of system documentation must be kept to a minimum and authorised by the application owner;*
- *computer generated documentation must be stored separately from other application files, and assigned an appropriate level of access protection; and*
- *sensitive documentation must be disposed of through approved means when no longer required.*

Data and Software Exchange

621. Exchanges of data and software between departments and external organisations should be controlled. Such exchanges should be carried out on the basis of formal agreements. Procedures and standards to protect media in transit should be established and consideration should be given to the security implications of electronic data exchanges.

622. Formal agreements should be established for exchange of data and software (whether electronic or manual) between departments and other organisations. The security content of such an agreement should reflect the sensitivity of the business information involved. An example of a baseline standard covering data exchange agreements is as follows:

Data Exchange

Data exchange agreements must detail the responsibilities and procedures for controlling and notifying transmission, dispatch and receipt.

A set of standards for packaging, or protocols for transmission, is to be defined and agreed between both parties.

Procedures are to be established for the identification of couriers.

The Department's responsibility and liability in the event of loss of exchanged material is to be defined in the data exchange agreement.

The agreement is to cover data and software ownership and responsibilities for data protection, software copyright compliance and similar considerations. This must include the requirement for any special measures required to protect very sensitive items, such as encryption.

The Internet

623. Electronic mail (e-mail) and the World Wide Web are increasingly being used for business communications and transactions, replacing traditional forms of communication such as hardcopy correspondence and facsimile. This medium differs from traditional forms of business communications in its speed, message structure, degree of formality, and vulnerability to interception. Consideration should be given to the need for controls to reduce business or security risks that may be generated by the use of the Internet. For example:

a. *the vulnerability of traffic to unauthorised interception or modification;*
b. *the vulnerability to error (e.g. incorrect addressing or misdirection) and the lack of control over the reliability and availability of the service;*
c. *the impact of a change of communication media on business processes e.g., effect of increased speed of dispatch or a change from company-to-company to person-to-person addressing;*
d. *legal considerations such as the potential need for proof of origin, dispatch, delivery and acceptance and archiving;*
e. *the security implications of publishing staff lists etc in publicly accessible directories; and*
f. *the need for security measures to control remote user access to Internet services such as e-mail accounts and restricted Webpages.*

624. Computers that host Internet services should be managed and monitored particularly carefully. Not only could their compromise cause embarrassment or damage to the organisation, but such computers, once compromised, are often used as a staging point to attempt to access computers on the internal network or those of another organisation. While it can be significantly simpler to publish material on the Internet than by the more traditional hardcopy methods, the same care and management processes should be in place to ensure that the data is correct and appropriate for publishing before it is made available on the Internet. For instance:

Publishing Information on the Internet

No agency information is to be published or otherwise made available on the Internet before going through the following procedure:

- *a draft of the information or the scope and an example set of the information must be provided to the Chief Information Officer (CIO) for approval in concept*
- *the draft or template will then be processed through the communications office to ensure that is satisfies business, security and organisational standards*
- *the mechanism for delivery, if new, is to be approved by the Director of Corporate Security before operation (see Chapter 10).*

SOPs for publishing updates to the information will be developed where applicable

625. Government workstation computers that are used to access the Internet should also be managed carefully whether they are located offsite or

on the internal network. The risk of hackers or malicious software (e.g., viruses, Trojan horses and network worms) is increasing as the attack methods become more sophisticated and as more sensitive information is stored on workstations. The widespread use of the set of Internet TCP/IP protocols on internal networks also means that a single compromised workstation might allow an intruder to access the whole internal network. Therefore, policies regarding the protection of these computers should be stated. For example:

Workstation Management

All agency workstations are maintained by the IT Division to a common profile. The profile includes:

- *approved hardware configuration*
- *approved operating system and software*
- *access control configuration*
- *automated management processes including virus protection, software updates, system performance monitoring*

Users are not to install any additional hardware or software or alter any operating system or application security settings unless authorised to by Director IT or the system administrator. On no account are users permitted to install modems or other communications devices on computers connected to an agency LAN.

626. Internet users should also be aware of what is and is not acceptable behaviour on the network. The types of controls that should be considered are:

a. *the amount of work time what can be used for non-official use of the Internet (e.g., sending and reading personal e-mail, Web surfing);*
b. *policy on use of computer games;*
c. *content deemed acceptable and not acceptable in the work environment (e.g. pictures, jokes, gossip);*
d. *restrictions on running downloaded or e-mailed executable files;*
e. *use of disclaimers on e-mails and Webpages; and*
f. *use of the Internet for formal communications.*

CHAPTER 7

ACCESS CONTROL

Introduction

701. Appropriate controls must be established to ensure that information processed and stored in computer systems is adequately protected. Access to computer services and data should be controlled on the basis of business requirements, but should also take account Government and departmental policies for information dissemination and entitlement e.g. the "need to know" principle. To manage this effectively, each business application owner should

maintain a clearly defined access policy statement that defines the access requirements of each user or group of users to that application or system. Service providers should then be provided with the requirement definition so they can implement and maintain an effective level of control. A policy of "Defence in Depth" should be employed, where several 'layers' of protection are used to protect critical resources rather than a relying on a single security mechanism.

702. Discretionary access to application systems and data should be applied though configuration of user and group file-access rights. Strict controls should be placed on application system source code, compilers, computer operating software and scripting facilities to ensure that the system's access control mechanisms cannot be bypassed through code subversion. Users should also be briefed on application and operating system access control functions on a need-to-know basis. Menu systems may also be used to control access to application and system functions rather than allowing users access to a command prompt interface.

Account Management

703. Once a user has entered a computer system, a usage profile will normally be assigned which associates privileges and access rights to the user. There should be formal procedures to control allocation of access rights to IT services to prevent unauthorised access to data or system resources. The procedures should cover all stages in the lifecycle of user access, from the initial registration of new users to the final deactivation of accounts that are no longer required. Special attention should be given to privileged access rights that allow users to override system controls.

704. A standard relating to the formal user registration process should be included in the Access Control section. The following excerpt is an example of a user registration policy.

User Registration

Unauthorised access to computer systems is prevented through the controlled registration of users and allocation of accounts. User registration procedures must be designed to:

- *allocate user IDs only upon proper authorisation from the system owner;*
- *provide a level of access appropriate for the business purpose;*
- *provide users with a written statement of their access rights;*
- *require users to sign undertakings to indicate that they understand the conditions of access;*
- *maintain a formal record of all persons registered to use the service; and*
- *periodically check for, and remove, redundant user IDs and accounts that are no longer required.*

Access rights of users who have changed jobs or left the department should be immediately revoked. Redundant user identifiers should not be reissued.

Passwords

705. The first line of defence for a host computer system is usually the user identification code (user ID) and some form of authentication. Passwords are currently the principal means of authenticating a user and validating their authority to access the computer service. The allocation of passwords should be controlled by a formal management process, in which users sign an undertaking to keep their passwords confidential. Other technologies for authentication should be considered if a higher level of security is justified. The publication *NZSIT 204: Authentication Mechanisms* provides details of password and other authentication mechanisms.

706. Users should be provided initially with a secure temporary password that they are forced to change on the first system access, and this should be passed directly to the user after positive identification. Conveyance of passwords by unprotected (clear text) Email messages should be avoided. Users should acknowledge receipt of passwords.

707. As passwords are the principal means of validating a user's authority to access a computer service, password management systems should provide an effective, interactive facility that ensures quality passwords. Very strong authentication requirements will involve user passwords being assigned by an independent authority. An example of a password standard is as follows:

Passwords

Normally, individual passwords are to be used for access to computer facilities. Anonymous access is to be authorised on a case by case basis.

Password management schemes for departmental computer systems are to allow users to select and change their own password and include a confirmation procedure to allow for typing errors. Computer security features are to be configured to enforce a minimum password length of six characters and require the password to be changed at least quarterly. Passwords for privileged system administration and support accounts must be changed at least monthly.

Systems are to be configured to ensure that the initial, temporary passwords for newly allocated accounts are changed at the first logon, and a record of the last five passwords for the account should be maintained to prevent password reuse. Default vendor passwords are to be removed immediately following installation of software.

Passwords are not to be displayed on the screen when being entered, and the password verification file is to be stored separately from the main application

system data. Passwords in this file should be stored in encrypted form, if possible, using a one-way encryption algorithm.

708. In most cases passwords are selected and maintained by users, so users should be encouraged to adopt good security practices in their selection and use. The following is an example of user password guidelines:

Users are responsible for ensuring their passwords are:

- *kept confidential. They should NOT be shared with other users;*
- *not written down, except for lodging with departmental security staff or secure safekeeping, where appropriate;*
- *changed whenever there is any indication of possible system or password compromise;*
- *not based on:*
  - *dates, such as birthdates, anniversaries, etc;*
  - *company names, identifiers or references;*
  - *user ID, user name, group ID or other system identifier;*
  - *more than two consecutive identical characters; or*
  - *all-numeric or all-alphabetic groups.*
  - *telephone numbers or similar all-numeric groups; and*
- *not stored in any automated logon process, macro, or keyboard function key;*
- *not reused between different systems.*

Users are also responsible for logging off workstations and networks when they leave the office for longer than 30 minutes.

709. A single user identifier and password for multiple systems may be appropriate where an adequate level of protection for password storage and transmission exists. In a network environment, this technique is known as Single Sign On (SSO).

710. More rigorous authorisation systems based on encryption or challenge-response techniques are becoming available. These systems are usually more expensive than standard password schemes but do provide a higher assurance of access control. They should be used whenever they can be justified on the basis of business risk.

Logon Procedures

711. Access to host-based IT services should be via a secure logon process. The procedure for logging on to a computer system should be designed to minimise the opportunity for unauthorised access. The procedure should therefore disclose the minimum information about the system in order to avoid providing an unauthorised user with unnecessary assistance. The following is an example of a logon procedure:

System Logon

No system or application identifiers are to be displayed until the logon process has been successfully completed.

A notice warning that the computer is only to be accessed by authorised users must be displayed.

No help messages are to be provided during the logon procedure that would aid an unauthorised user.

Logon information is to be validated only on completion of all input data.

If an error condition arises, the system must not indicate which part of the data is correct or incorrect.

No more than three unsuccessful logon attempts are to be allowed before action is taken to:

- *record the unsuccessful attempt;*
- *force a time delay before further logon attempts are allowed; and*
- *disconnect data link connection.*

The workstation should be disconnected and give no assistance after a rejected logon attempt. The maximum time allowed for the logon procedure is 30 seconds. If exceeded, the system must terminate the logon process.

On completion of a successful logon, the date and time of the previous successful logon and details of any subsequent unsuccessful logon attempts must be displayed.

User Access Control

712. Systems often require controls to restrict users' connectivity and functionality in order to support the access policy requirements of business applications. User access control can be based on allowing access to everything and then only controlling access to the systems, applications and data repositories that the user is not permitted to access. However, it is usually better practice to start with a premise of denying access to all resources, and then explicitly providing access to the user for those resources he or she needs access to based on their individual, group and/or location attributes. Such controls can be implemented in the network components, the operating systems or within the applications themselves.

713. Network components can provide access control based on the source and or destination address (IP, MAC, etc) of the communications, the network protocol, the service, and in some firewalls, the content of the communications. The user could also be required to log in to the network component before being permitted access to components on the other side.

The network components could also be used to protect information by encrypting traffic and/or by routing it through a specific communications path.

714. Authentication of the user, workstation or application may be required to make the access control decision. This can be achieved using a password scheme, a challenge/response system, Kerberos style single sign on, or cryptography (e.g., digital signature). Dedicated private lines or a network user address (NUA) checking facility can also be used to provide assurance of the source of communications. Whether authentication is done by the network, the operating system or the application will depend largely on the access control granularity requirements of the business applications. For instance, where the access-control decision relies only on whether a communication comes from a particular LAN could be achieved through the use of VPN authentication completely transparently to the user and applications; while a database application that restricts access to individual rows based on the user ID may require application-level access control. Network and operating system authentication is generally preferable because of the duplication and additional management required with application-level authentication.

System Access Control

Operating system access controls must be employed for all systems connected to agency networks. Where possible, access restrictions are to be based on user groups/domains with individual user IDs assigned to the groups as required. User authentication is based on passwords and IP address. Remote users are to be authenticated via digital signature technology.

715. The unnecessary allocation and use of system privileges is often found to be a major contributing factor in the vulnerability of systems that have been breached. Accordingly, the management and use of special privileges should be restricted and controlled. For multi-user systems the allocation of privileges should be controlled through a formal authorisation process, as in the following example:

Privileged Access

The requirement and level of privileged access associated with each system, and the categories of staff to which privileged access is to be allocated, must be predefined and approved.

Privileged access must be allocated to individuals on a "need-to-use" basis and on an "event by event" basis.

Where possible, special system routines should be developed and used to avoid the need for manual privileged user access.

A regular review of users' system access privileges should be carried out to detect any inappropriate access rights.

716. Access to system resources such as source code, application development environments and configuration files should also be controlled. The following is an example of additional controls that may be required in sensitive systems:

Access to System Resources

Where possible, program source libraries and programs under development or maintenance should not be held in operational systems. IT support staff should not have unrestricted access to such software.

A program librarian should be nominated for each application and the updating of program source libraries and the issuing of program sources to programmers should only be performed by the nominated librarian upon authorisation from the IT support manager for the application.

Program listings should be held in a secure environment.

An audit log should be maintained of all access to program source libraries.

Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures.

Maintenance and copying of program source libraries should be subject to strict change control procedures.

Workstation Security

717. Automatic terminal identification is a technique that can be used in some network configurations for applications in which sessions should only be initiated from a particular location. An identifier in, or attached to, the workstation is checked by the system to indicate whether the session request should be allowed. The use of such a scheme may also necessitate physical security measures to protect the terminal in order to maintain the anonymity of its identifier.

718. Workstations in locations that are outside the department's security management, or those systems handling sensitive information, should be set to timeout after a period of inactivity, to prevent access by unauthorised persons. The timeout delay should reflect the level of risk associated with the location and the users of the terminal. Upon timeout, the terminal screen should clear and both the application and network connections should be closed. A limited form of timeout facility can be provided for some PCs in the form of a secure screen saver or keyboard lockout. If implemented properly, such a facility can prevent unauthorised access without closing down the application or network sessions.

719. Restrictions on connection times will provide additional security for high risk applications. Limiting the period during which connections are allowed to computer services reduces the window of opportunity for unauthorised access.

720. The following is an example of a workstation security standard:

Workstation Security

Remote access should be controlled, where possible, on the basis of workstation identity as well as user identity and may be further controlled by limiting access to specific times of day appropriate to the particular computer and/or user.

Login sessions must be terminated with the correct logoff procedure, or timed out after 15 minutes inactivity.

All sensitive files are to be stored on the file servers; no copies should be stored on workstation hard drives.

Sensitive System Isolation

721. Some particularly sensitive systems may need to be run on a dedicated computer, or share resources only with other trusted applications systems. The sensitivity of an application system should be explicitly identified and documented by the application owner in the system security policy.

Inter-Network Access Control

722. Computer and network access management should be closely co-ordinated; both to optimise the service to the business and to ensure that security measures are consistently applied across the IT infrastructure.

723. Networks are increasingly being extended beyond traditional departmental boundaries as business arrangements are formed which require the interconnection or sharing of computer or network facilities. Such connections increase the risk of unauthorised access to the data passed across the network or to the existing computer systems on the network, and could potentially breach privacy protection requirements. In such circumstances the introduction of controls within the network to segregate groups of users and computers should be considered as well as controls to protect the information in transit.

724. Shared networks, especially those extending across departmental boundaries, may require the incorporation of routing controls to ensure that computer connections and information flows do not breach the access policy covering business applications. These controls should be based on positive source and destination address checking mechanisms. They can be

implemented in software or hardware. However, implementers should be aware of the strength of any mechanisms deployed and the level of trust that should be placed in address information.

725. One method of controlling the security of large networks is to divide them into separate logical domains, each protected by a defined security perimeter controlled by a firewall or other form of network gateway. Access between domains can then be controlled based on routing, protocol and connection controls. The criteria for segregation of networks into domains should be based on business access control policies and requirements and should take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.

726. The policies for communication between the domains should be negotiated based on the business needs versus the security exposure and the administrative overhead. The results should be documented in detail in a Network Access Policy, and all changes to the network or its components should comply with the policy or re-negotiate it if necessary.

727. Access to diagnostic and maintenance ports should be securely controlled. Many computers have a dial-up remote administration facility for use by maintenance engineers. If unprotected, these ports could provide a means of unauthorised access and should be protected by an appropriate security mechanism, such as a key lock or some form of electronic authentication.

728. An example of a baseline network security standard is as follows:

Network Security

Network security measures are required to protect data in transit from being intercepted, modified, removed, or replayed. The following controls are to be applied to all communications services and systems used by the Department.

- *All information transmitted on public data network services is to be protected by an appropriate, GCSB-approved, encryption system (see Cryptographic Controls in the next chapter).*
- *Remote equipment is to be adequately protected from physical abuse or subversion.*
- *Remote users and equipment are to be appropriately authenticated.*
- *All network connections, including dial-in modems, must be authorised.*
- *Diagnostic ports must be protected from unauthorised remote access.*
- *Where possible, terminals should be uniquely identified.*

System Monitoring

729. Procedures for monitoring system use should be established. Such procedures are necessary to ensure that users are performing only processes that have been explicitly authorised. The level of monitoring required for individual systems should be determined by separate risk assessment.

730. Audit trails recording exceptions and other security-relevant events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. A record of successful system access, in addition to rejected attempts, is also worthwhile.

731. Where system logs are used for monitoring there must also be procedures and responsibilities in place to audit the logs. However, because of the significant amount of work involved in this type of monitoring, and the increasing speed and sophistication of attacks, it may be more appropriate to use specialised intrusion detection systems and/or outsourced intrusion and misuse detection services.

732. The Rules of Evidence might also require consideration when choosing the type of logs to be collected and the data items to be in them. An example of a monitoring standard is as follows:

System Monitoring

Network intrusion and misuse detection is to be performed centrally by the IT division. All traffic on the major network bearers must be scanned for attack signatures and anomalous behaviour. As part of this task, the IT Division is responsible to query staff in cases where unusual traffic was passed to or from computers under the staff member's control; this will be necessary to develop a comprehensive picture of legitimate traffic to help the system differentiate between legitimate and unauthorised communications.

Host computers must also be configured to record:

- *all successful and unsuccessful login attempts;*
- *all allocation and use of accounts with a privileged access capability; and*
- *the use of selected transactions.*

Monitoring records (audit trails) should include user identifiers, dates and times for logon and logoff, terminal identity or location, the programs executed, the files accessed; and the program and/or session completion status.

Duress Alarm

733. Provision of a duress alarm should be considered for users who might be a target for coercion. Such an alarm is often implemented through the use of special user identifiers or passwords. The decision whether to supply a duress alarm should be based on an assessment of risk and there should be defined responsibilities and procedures for responding to an activated alarm.

Clock Synchronisation

734. The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, such as Greenwich Mean Time (GMT) or local standard time. Clocks tend to drift from the correct time over time, so routine procedures that check for and correct any significant variation should be included in the system administration procedures.

Mobile Computing and Teleworking

735. When mobile computing and teleworking are employed the risks of compromise of the remote site must be considered, as must be the vulnerability of data interception and of unauthorised access into the organisation's internal network through the remote access path.

736. There are a huge number of laptop computers lost and stolen every year. Therefore, additional physical protection such as cable locks should be considered for equipment in open or shared environments where it cannot be monitored at all times. In situations where unauthorised users might gain access to the computing equipment removable media should be used and secured when the equipment is vulnerable, or media encryption should be considered. Protection for sensitive or classified hard copy output should also be considered at the remote sites.

737. File or communications encryption should be employed when transferring sensitive information across a public network (e.g. the PSTN or the Internet). Most communications encryption products also include strong authentication services, which will reduce the risk of unauthorised access to the organisation's network via the remote access service compared with password authentication. Passwords should never be passed 'in the clear'.

738. The remote access entry point into the organisation's network should be configured and managed very carefully. Only those services required by the remote workers should be available through this communications path. The remote access capability should only be activated when it is needed and only for those users that need it. Modem call-back should be considered where dial-in access is used. Connection statistics should be monitored to detect unauthorised access attempts. Remote workstations should also have a virus checking capability, which should be updated whenever the organisation's other systems are updated, and should check all file transfers into and out of the workstation.

CHAPTER 8

SYSTEM DEVELOPMENT AND MAINTENANCE

Security Requirements

801. Controls introduced at the design stage are generally significantly cheaper to implement and maintain than those included during or after implementation. Therefore, the Departmental Security Officer (or the IT Security Officer if the department has one) should be included in all IT developments during the design stage, and also preferably during the requirements specification. The security controls should also be agreed to by the Configuration Control Board and/or the IT Security Forum prior to implementation.

Security in Software Applications

802. Vetting of input data should be included in all departmental application software systems where the integrity of the data (e.g. accuracy, completeness, correctness, etc) is important. Data correctly entered into an application system can be corrupted by processing errors or through deliberate acts. Validation checks should be incorporated into systems to detect such corruption. The specific controls required will depend on the nature of the application and the assessed business impact of any corruption of data. The following controls and checks might be considered:

Data Verification Controls

The accuracy of captured information is important to the operation of departmental business systems. All applications should include controls such as out-of-range checking, checking for invalid characters in data fields, missing or incomplete data, exceeding upper and lower data volume limits, and inconsistent control data.

Application systems should include the following controls for data verification and cross-checking:

- *session or batch controls, to reconcile data file balances after transaction updates;*
- *balancing controls, to check opening balances against previous closing balances, namely:*
  - *run-to-run controls;*
  - *file update totals; and*
  - *program-to-program controls;*
- *validation of system-generated data; and*
- *checks on the integrity of data or software down-loaded, or up-loaded, between central and remote computers.*

Cryptographic Controls

803. Cryptographic systems and techniques should be considered for incorporation into systems that require additional confidentiality, authentication or integrity protection of information in transit or in storage. However, while encryption can be a powerful tool, used carelessly it can hinder virus and system misuse detection, cause information to be irrecoverably lost, and provide users with a false sense of security. Therefore, policy for the use of cryptography within the department should be defined based on business needs and interoperability requirements.

804. Encryption is the process of transforming information into an unintelligible form to safeguard its confidentiality and integrity, and involves an encryption algorithm and a secret cryptographic key. Encryption is mandatory for the transmission of information classified CONFIDENTIAL and above and for RESTRICTED/SENSITIVE information transmitted outside of New Zealand or over public networks (e.g. the Internet). Encryption should also be considered for IN-CONFIDENCE information in transit and for all classified data stored on magnetic media. The level of protection provided depends upon a number of factors including the quality of the algorithm and its implementation, the key length, and the secrecy of the key. Specialist advice on the application of encryption and suitable cryptographic products should be sought from the GCSB.

805. Message authentication is a technique used to detect unauthorised changes to, or corruption of, the contents of a transmitted electronic message and should be considered for applications where it is vital to protect the integrity of the message content, such as electronic funds transfers. Message authentication is usually achieved through the use of modification detection codes. A digital signature is a special form of message authentication, usually based on public-key cipher techniques, which provides authentication of the sender, as well as assurance of the integrity of the message content.

806. Non-repudiation is a technique used to ensure that a message originator cannot subsequently deny having sent the message, and a recipient cannot subsequently deny having received it. Non-repudiation is usually achieved through the use of digital signatures.

Operating Systems and Package Maintenance

807. The requirement to establish a configuration management regime for all systems and application software has already been outlined in Chapter 2. However, changes to operating systems software merit special consideration and may require additional standards that cover:

a. *the review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;*
b. *assurance that a reversion process is available in case a software change causes problems; and*

c. assurance that notifications of operating system changes are provided in time to allow appropriate reviews to take place before implementation.

808. Modifications to systems software and standard commercial software packages should be discouraged. If changes are deemed essential, then the original software should be retained and the changes applied to a clearly identified copy. These changes should be fully documented, so that they can be reapplied if necessary to future software upgrades. If a software package is to be modified, there will be a risk of damage to the built-in controls and integrity processes.

Protection of the Development Suite and Test Data

809. Source code and configuration files should be protected from unauthorised viewing and alteration. They should be under strict version control, with clear separation between operational and development versions. Where possible, the source code should not be stored on operational systems, nor should it be freely available to all IT support staff.

810. Test data should also be protected and controlled. System and acceptance testing usually requires substantial amounts of test data that are as close as possible to live data. The use of live databases containing personal data should be avoided, but if necessary then all data records should be 'depersonalised' before use.

CHAPTER 9

BUSINESS CONTINUITY MANAGEMENT

901. Having a set of backup data is an important prerequisite for successful recovery after a major disaster. However, the success or failure of the recovery will depend upon the extent to which recovery has been planned. A Business Continuity Plan (BCP) should be developed for each site or system to ensure timely recovery of processing facilities and databases in the event of a major disaster or failure. Such interruptions may be caused by, for example, natural disasters, accidents, equipment failures, deliberate action, loss of supplied services, or loss of utilities.

902. Each plan should include measures to identify and reduce risks, limit the consequences should a threat be realised, and ensure speedy resumption of essential operations. The recovery plan should focus on keeping critical business processes and services running, including staffing and other non-computing requirements, not merely on the fallback arrangements for computer systems. Departmental systems should also be prioritised in terms of criticality for staged recovery in the event of a major breakdown or disaster.

903. Each system should have a specific custodian defined in the BCP. Emergency procedures, manual fallback plans, and resumption plans should be the responsibility of the appropriate business process owner. Fallback arrangements for alternative technical services, such as computers and communications, should usually be the responsibility of the service providers.

904. Many BCPs fail when activated, often because of incorrect assumptions, oversights or changes in equipment or personnel. They should therefore be tested regularly to ensure that they are effective. Such tests should also ensure that the plan is fresh in the minds of all members of the recovery team and other relevant staff. A test schedule for the plan should be drawn up. The schedule should indicate how and when each element of the plan will be tested. A phased approach to testing is recommended, based on frequent tests of individual components of the plan, to ensure that the documented procedures continue to be relevant and accurate. It should also reduce the need for, and frequency of, full tests of the plan.

905. BCPs can quickly become out of date because of business or departmental changes. They should be updated regularly to protect the initial investment in developing the plan and to ensure its continuing effectiveness. Examples of changes that might necessitate updating plans include:

a. *acquisition of new equipment, or upgrading of existing operational systems;*
b. *new problem detection and control technology, eg. fire detection;*
c. *new environmental control technology;*
d. *staff or departmental changes;*
e. *changes of contractors or suppliers;*
f. *changes of addresses or telephone numbers;*
g. *termination, modification, or introduction of new business processes;*
h. *changes to the system applications portfolio;*
i. *changes in system operating practices; or*
j. *changes in legislation.*

906. There are many established BCP methodologies that can be adopted. An example of a management directive for BCP is as follows:

Business Continuity

Procedures for the prioritised recovery of each operational system after a system failure or disaster must be included in the Business Continuity Plan (BCP). The plan will include:

- *identification and prioritisation of critical business processes;*
- *determination of the potential impact of various types of disaster on business activities;*
- *identification of and agreement on all responsibilities and emergency arrangements;*
- *emergency procedures, which describe the immediate action to be taken following a major incident which jeopardises business operations and/or human life;*

- *documentation of agreed fallback and/or recovery actions, procedures, and processes, particularly covering computer services, telecommunications, and accommodation;*
- *appropriate education of staff in the execution of the agreed emergency procedures and processes; and*
- *a test schedule, which specifies how and when the plan will be tested.*

CHAPTER 10

COMPLIANCE

Management Approval Process

1001. The Security Policy should document the management approval process that is used to ensure that new IT systems and facilities are for a valid business purpose, will provide an adequate level of protection to the information they hold, and will not adversely affect the security of the existing corporate infrastructure.

1002. Each new installation should have appropriate management approval, authorising its purpose and use. Approval should also be obtained from the manager responsible for maintaining the local IT security environment, to ensure that the installation conforms to all relevant security policies and requirements.

1003. Where necessary, the system should be checked to ensure that all devices connected to communication networks or maintained by a particular service provider are of an approved type. Alternatively, independent tests of the devices may be necessary to ensure they adequately implement their defined security functionality.

1004. A documented security management system should be established and maintained to provide the vehicle for management approval. An appropriate system for Government is fully documented in *NZSIT 102: Certification of Government Computer Systems* and the GCSB provides training in the practical application of this system. Certification documentation consists of:

a. ***Top Level Specification (TLS)*** *The TLS provides an overview of the functionality, design, users, and data flows of the information processing system;*
b. ***System Security Policy (SSP)*** *The SSP defines the environment in which the system operates, the security functionality required, and the level of assurance to which security will be provided;*
c. ***Security Plan (SP)****. The SP defines the mechanisms used to implement the requirements stated in the SSP; and*

d. ***Standard Operating Procedures (SOPs)*** *SOPs are used to specify the manual procedures used to support systems operation, including those which contribute to the security of the system.*

1005. The implementation and operation of information security measures in critical or high-risk systems should be reviewed independently to provide assurance that they properly reflect departmental policies. Such a review could be carried out by an internal auditor or an independent senior manager. The GCSB will, on request, assist in the review of such measures.

1006. An example of a management approval directive is as follows:

Management Approval

The security measures for the protection of all Department IT systems processing sensitive or classified information are subject to management approval prior to system implementation. This involves the development of a Top Level Specification, System Security Policy, Security Plan, and Standard Operating Procedures for the system (see NZSIT 102: Certification of Government Computer Systems) and submitting these documents to the IT Security Forum for endorsement. The managers concerned will then be asked to certify that the system meets the criteria stated in the documentation. An independent assessment may also be carried out before the system is given final approval to operate. All Department systems are subject to regular inspection and audit once operational to ensure that they continue to meet departmental policies.

All security products used in the Department's systems are to be either formally approved for Government use or subject to specific evaluation to provide adequate assurance of their functionality.

Inspection and Testing

1007. The management approval procedures should require that no business-critical information systems are brought into service until they have been inspected, or otherwise verified, as conforming to the specifications laid down in the system security policy and security plan. Verification should be in accordance with pre-established acceptance procedures and site inspection. A temporary waiver of acceptance requirements should be sought from management in situations where the information system is required before the formal audit and approval process can be completed.

1008. A comprehensive programme of planned and documented internal security audits should be carried out to verify that security activities comply with planned arrangements and to determine the effectiveness of the security management system. Documented procedures should be established for the audits and follow up actions to ensure that a consistent level of audit is maintained. Audit requirements and activities involving checks on operational

systems should be carefully planned to minimise the risk of disruptions to business processes.

1009. Audits should be scheduled on the basis of the criticality of the activity, the sensitivity of the information being processed, and the assessed risk to the system. Audits should be carried out by personnel independent of the system administration, and results should be documented and formally brought to the attention of system management so that timely corrective action can be taken on any deficiencies identified.

1010. Access to system inspection and audit tools should be strictly controlled to ensure their continued integrity. They should be separated from development and operational systems and not held in tape libraries or user areas, unless given an additional level of protection.

1011. The following is an example of audit and inspection management controls:

Compliance Audit and Inspection

All departmental IT systems are to be subject to regular audit and inspection.

Audit scope and requirements must be approved by the IT Security Forum

Checks will be limited to read-only access to software and data.

IT resources for performing audit checks should be explicitly identified and made available, and requirements for special or additional processing should be identified and agreed with service providers.