



Information Security Guideline for NSW Government – Part 3 Information Security Baseline Controls

Issue No: 3.0

First Published: Sept 1997

Current Version: June 2003

Table of Contents

1.	INTRODUCTION	4
1.1	Scope	4
1.2	Aim	4
1.3	Structure	4
1.4	Applicability.....	4
2.	CONCEPT	5
2.1	Control Classifications.....	5
2.2	Control Types	6
2.3	Developing an Agency-Wide Baseline	6
3.	ORGANISATIONAL AND MANAGEMENT CONTROLS.....	7
3.1	Information Security Policy.....	7
3.2	Information Security Infrastructure	7
3.3	Security of Third Party Access	9
3.4	Outsourcing.....	10
3.5	Mobile Computing.....	10
3.6	Teleworking	11
3.7	Asset Classification and Control.....	11
3.8	Personnel Practices	12
3.8.1	<i>JOB DESCRIPTIONS.....</i>	<i>12</i>
3.8.2	<i>SEGREGATION OF DUTIES.....</i>	<i>12</i>
3.8.3	<i>RECRUITMENT.....</i>	<i>12</i>
3.8.4	<i>TERMS AND CONDITIONS OF EMPLOYMENT</i>	<i>13</i>
3.8.5	<i>MONITORING OF PERSONNEL</i>	<i>13</i>
3.8.6	<i>TERMINATIONS AND JOB CHANGES.....</i>	<i>14</i>
3.9	Security Awareness and Training.....	14
3.10	Compliance with Legal and Regulatory Requirements	15
3.11	Compliance with Security Policies and Standards	16
3.12	Incident Handling.....	17
3.13	Disciplinary Process	18
3.14	Business Continuity Management.....	18
3.15	System Audits.....	21
3.15.1	<i>AUDITS OF OPERATIONAL SYSTEMS</i>	<i>21</i>
4.	PHYSICAL AND ENVIRONMENTAL CONTROLS.....	23
4.1	Secure Areas.....	23
4.2	Equipment Security	23
4.3	Clear desk and screen policy	24
4.4	Removal of property	24

5:	OPERATIONAL CONTROLS	25
5.1	Documentation	25
5.2	Configuration and change management	25
5.3	Incident Management.....	26
5.4	Software Development and Test Environment.....	27
5.5	Outsourced Facilities	27
5.6	Systems planning	28
5.7	Systems and Acceptance Testing	28
5.8	Protection against Malicious Code	29
5.9	Data Backup	30
5.10	Logging.....	31
5.11	Software and Information exchange.....	31
5.12	Security of media in transit	32
5.13	Electronic Commerce Security	32
	5.13.1 ELECTRONIC DATA INTERCHANGE (EDI)	32
	5.13.2 INTERNET COMMERCE	33
5.14	Electronic Mail Security	33
5.15	Electronic Office Systems	34
5.16	Electronic Publishing	34
5.17	Media 35	
6.	TECHNICAL CONTROLS	37
6.1	Identification and Authentication	37
	6.1.2 <i>PASSWORDS</i>	37
	6.1.2 <i>TOKENS</i>	38
	6.1.3 <i>BIOMETRIC DEVICES</i>	39
6.2	Logical Access.....	39
6.3	Review of Access rights	40
6.4	Unattended User Hardware.....	41
6.5	Network Management	41
	6.5.1 <i>OPERATIONAL PROCEDURES</i>	41
	6.5.2 <i>PREDEFINED USER ACCESS PATHS</i>	42
	6.5.3 <i>DIAL IN ACCESS CONTROLS</i>	42
	6.5.4 <i>NETWORK PLANNING</i>	43
	6.5.5 <i>NETWORK CONFIGURATION</i>	43
	6.5.6 <i>SEGREGATION OF NETWORKS</i>	43
	6.5.7. <i>FIREWALLS</i>	44
	6.5.8 <i>MONITORING OF NETWORK</i>	45
	6.5.9 <i>INTRUSION DETECTION</i>	45
	6.5.10 <i>INTERNET CONNECTION POLICIES</i>	45
6.6	Operating System Access Control	46
	6.6.1 <i>IDENTIFICATION OF TERMINALS AND WORKSTATIONS</i>	46
	6.6.2 <i>SECURE LOGON PROCEDURES</i>	47
	6.6.3 <i>SYSTEM UTILITIES</i>	47
	6.6.4 <i>DURESS ALARM</i>	47
	6.6.5 <i>TIME RESTRICTION</i>	47
6.7	Application Access Control.....	48
	6.7.1 <i>APPLICATION ACCESS RESTRICTION</i>	48
	6.7.2 <i>ISOLATION OF SENSITIVE APPLICATIONS</i>	48
6.8	Audit Trails and Logs.....	49
7.	SYSTEMS DEVELOPMENT AND MAINTENANCE CONTROLS	51

7.1 Application Security 51
7.2 Cryptography 54
7.3 Restrictions to Software Package Modifications 56
APPENDIX 1: CLASSIFICATION OF CONTROLS 57
APPENDIX 2: CONTROL TOPICS BY SECURITY CONCERN 61
APPENDIX 3: EXAMPLES OF THREATS AND MITIGATING CONTROLS 65
APPENDIX 4: REFERENCES 70

1. Introduction

The Information Security Guidelines provide a generic framework to all NSW government agency personnel who are responsible for establishing, managing, implementing or maintaining information security in their respective agencies.

The Guidelines consist of three parts, as follows:

- [Part 1](#)** Provides an overview of the information security risk management process;
- [Part 2](#)** Provides examples of threats and vulnerabilities that an agency may face;
- [Part 3](#)** Provides guidance for selecting controls and establishing a minimum set of controls to protect all or some of the agency's information.

1.1 Scope

This part of the Information Security Guidelines provides descriptions of the information security controls which are consistent with those in the Information Security Management Standard Part 2 (AS/NZS 7799.2:2003). ICT also provides a basis for the selection of those controls, according to business needs and security concerns.

1.2 Aim

The aim of this document is to provide guidance for establishing a minimum set of controls to protect all or some of an agency's information and a basis for an agency-wide baseline security manual.

It is not intended to describe all controls in detail.

1.3 Structure

[Section 2](#) provides an overview of the process for selecting controls and the concept of baseline security. [Section 3](#) describes the information security controls classified into organisational and management, physical, operation and technical controls, and referenced to the Information Security Management Standard Part 2 (AS/NZS 7799.2:2003).

1.4 Applicability

This document applies to personnel who are responsible for selecting appropriate controls to information risks. ICT is assumed that these personnel and those responsible for implementing the controls are appropriately qualified and experienced people.

2. Concept

In the selection of controls to effectively protect against assessed risks, there are two main approaches, ie. using a baseline approach and conducting detailed risk analyses.

The baseline approach requires at least the minimum level of security to be defined by the agency. This level of baseline security is achieved by implementing a minimum set of controls to protect information against the most common threats. An early step in the baseline approach may be a gap analysis. The risk in the baseline approach is that there may be an unidentified 'non-standard' threat or vulnerability that is missed by gap analysis and/or baseline controls.

For information assets assessed as high risk, ICT may be necessary to conduct a detailed risk analysis. Although this type of analysis normally requires considerable time, effort and expertise, ICT has the advantage of providing a comprehensive view of the assessed risk. Controls, which are justified by the risks, are then selected. This avoids the provision of too much or too little protection.

The selection of controls should always include a balance of non-technical and technical safeguards. Non-technical controls are of a general nature and include those that provide physical, personnel, and administrative security. Technical controls relate specifically to the information system considered.

Considerations in selecting controls are addressed in Section 5 of [Part 1](#) of this Guideline.

2.1 Control Classifications

The ensuing sections describe the baseline information security controls classified into:

- Organisational and management controls;
- Physical and environmental controls;
- Operational controls;
- Technical controls.

The above classifications are used to assist in identifying non-technical (the first three classifications) and technical controls.

The controls are referenced to those set out in AS/NZS 7799.2:2003 and additional information can be found in the Information Security Management Standard Part 1 (AS/NZS 17799:2001) which identifies 10 classes of control:

- Security policy;
- Security organisation;
- Asset classification and control;
- Personnel security;

- Physical and environmental security;
- Communications and operations management;
- Access control;
- System development and maintenance;
- Business Continuity management;
- Compliance.

2.2 Control Types

Controls may perform one of the following functions:

Deter:	Avoid or prevent the occurrence of an undesirable event
Protect:	Safeguard the information assets from adverse events
Detect:	Identify the occurrence of an undesirable event
Respond:	React to or counter the adverse event
Recover:	Restore the integrity, availability and confidentiality of information assets to their expected state

The selection of controls should show a reasonable balance of the above types. For example, if a majority of controls were deterrence controls without adequate controls to detect when the deterrence controls are not effective, then the overall security will not be effective. Similarly protection controls are not guaranteed, therefore controls to detect intrusion are also required. Furthermore, there is usually scope for human error in any control and layered controls help manage this risk.

2.3 Developing an Agency-Wide Baseline

The following questions should be considered when applying baseline security:

- Which parts of the agency or systems can be protected by the same baseline?
- Should the same baseline be applied throughout the whole agency?
- What security level should the baseline agency(s) aim at?
- How will the controls forming the baseline(s) be determined?

The use of one baseline level will reduce the cost of implementing controls considerably, and everyone within the agency can rely on the same level of security being present. In doing so, ICT is usually advisable to aim at the highest security level of the information and information systems to be protected by the baseline controls since such implementation is normally not very expensive and provides adequate security for all information assets. A careful consideration of all information assets is necessary to make the final decision on which information assets should be protected by the same baseline.

3. Organisational and Management Controls

This section describes the controls dealing with the management of information security, planning, assignment of responsibilities for these processes, and all other relevant activities. The objective of these controls is to achieve an appropriate and consistent level of security throughout the agency.

Strong management practices provide a vital role in the implementation of effective information security measures. ICT is human nature for personnel to readily resort to shortcuts or circumventions when ICT suits them. Failure by management to respond to such situations will legitimise these actions and increases the risk of damage to the agency.

3.1 Information Security Policy

Information security is a responsibility shared by all members of the agency, which needs to be led by clear and visible management policy and procedures.

A policy issued and approved by executive management should clearly define the agency's direction on Information Security, including the use of assets, the performance standards expected and the conduct of all users within the agency.

The agency's policy must be clearly communicated to and acknowledged by all personnel.

Effective policy and procedures, backed by management commitment are an important front line defence against information security breaches. Reliance cannot be placed on technological measures alone.

Procedures, guidelines and standards for the performance of business and administrative functions, in support of the information security policy, should be developed. These procedures should be kept current and clearly communicated to all personnel.

AS/NZS 7799.2:2003	<i>A.3.1.1 A policy document shall be approved by management, published, and communicated, as appropriate, to all employees.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.3.1.2 The policy shall be reviewed regularly, in case of influencing changes, to ensure ICT remains appropriate.</i>
---------------------------	--

A discussion on Information Security Policy can be found in [Part 1](#), Section 3.

3.2 Information Security Infrastructure

Information security should be managed within the agency in a structure that is appropriate to its size.

The agency should identify resource requirements and assign the appropriate roles and responsibilities to allow the effective management of the Information

Security Policy from within the agency. This may involve the utilisation of specialist resources (either internal and / or external) if appropriate. [Part 1](#) Section 4 provides some discussion on the responsibility, authority and resourcing of the information security organisation.

Security responsibilities for the following roles include:

- Executive management – has ultimate responsibility for the management and implementation of information security;
- Information security officer – has responsibility for the development and implementation of security such as assisting owners in assessing risks and defining security guidelines with owners, advising on security issues, investigating suspected security incidents, and co-ordinating with other security organizations;
- Owner – has direct responsibility for the day-to-day implementation of security;
- ICT Management – has responsibility for development, implementation, management and maintenance of ICT facilities and systems in accordance with established policies;
- Users – must be aware of their responsibilities relating to information security, and be responsible for their actions;
- Auditor – must be an independent person (either within or outside the agency) who conducts reviews to provide assurance that information security policies and processes are complied with.

AS/NZS 7799.2:2003	<i>A.4.1.1 A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.4.1.2 Where appropriate to the size of the organisation, a cross-functional forum of management representatives from relevant parts of the organisation shall be used to co-ordinate the implementation of information security controls.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.4.1.3 Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined.</i>
---------------------------	---

Contact with external Information Security specialists should be developed to ensure that the agency keeps up with industry standards (best practice) and known security vulnerabilities.

To ensure appropriate action can be quickly taken in response to a security incident, ICT is beneficial to develop and maintain appropriate contacts with the Police, Independent Commission Against Corruption, other regulatory bodies, information service providers and telecommunications operations.

Information security officers should also be encouraged to join security and industry forums.

AS/NZS 7799.2:2003	<i>A.4.1.5 Advice on information security provided by in-house or specialist</i>
---------------------------	---

advisers shall be sought and communicated throughout the organisation.

AS/NZS 7799.2:2003 *A.4.1.6 Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.*

The approval process for new information processing facilities should ensure that all relevant security requirements are met and should take into account the compatibility with other system components such as networks and underlying communications.

AS/NZS 7799.2:2003 *A.4.2.1.4 A management authorisation process for new information processing facilities shall be established.*

An independent review should be conducted to provide assurance that the information security procedures reflect the policy and that they are practical and effective. The review must be performed by skilled personnel either in the internal audit function or third party organisation.

AS/NZS 7799.2:2003 *A.4.1.7 The implementation of the information security policy shall be reviewed independently.*

3.3 Security of Third Party Access

The agency should control access to information processing facilities by third party organisations and access should be assigned based on the assessment of the risk of granting such access.

Third parties include:

- Hardware and software staff of service providers located off-site;
- Trading partners or joint ventures;
- On-site contractors for hardware and software maintenance and support;
- Cleaning, catering, security guards and other outsourced support services;
- Student placement;
- Casual short-term appointments;
- Consultants.

Permission of access and use of any information should be governed through clauses built into third party agreements and contracts. Clauses 4.2.2 in AS/NZS 17799:2001 provides a list of conditions to be considered.

AS/NZS 7799.2:2003 *A.4.2.1 The risks associated with access to organisation information processing facilities by third parties shall be assessed and appropriate security controls implemented.*

AS/NZS 7799.2:2003 *A.4.2.2 Arrangements involving third party access to organisational information processing facilities shall be based on a formal contract containing all necessary security requirements.*

If confidentiality of information is an issue, third parties should be required to sign a non-disclosure agreement.

3.4 Outsourcing

An agency with any outsourcing arrangement must ensure that ICT has control over the service provider and its staff and contractors.

The agency should address the risk, security controls and procedures required for all aspects of information security through contractual arrangements in the outsourcing agreement. Some of the issues that need to be considered are:

- Responsibilities for the management and security of information;
- Ownership of data, software, policies and procedures;
- The protection of the agency's information from other clients using shared resources;
- Access to agency data by staff of the service provider;
- Service provider's change control procedures;
- Business continuity plans consistent with agency's availability requirements;
- Service provider's compliance with relevant NSW government regulations;
- Independent security compliance audits.

AS/NZS 7799.2:2003	<i>A.4.3.1 The security requirements of an organisation outsourcing the management and control of all or some of its information systems networks and/or desktop environments shall be addressed in a contract agreed between the parties.</i>
---------------------------	---

3.5 Mobile Computing

Policies and procedures should be established for the use of mobile computing facilities such as laptops, notebooks, palmtops and mobile phones. These should cover:

- Physical security;
- Transit security;
- Security labeling;
- Access controls including remote access;
- Virus protection;
- Encryption of data;
- Backups;
- Sanitisation, declassification and destruction of equipment.

As a minimum, security features should include user identification and authentication before access is given to data and applications, and a screen lock facility.

Controls should be commensurate with the risks associated with working with mobile computing facilities.

AS/NZS 7799.2:2003	<i>A.9.8.1 A formal policy shall be in place and appropriate controls shall be adopted to protect against the risks of working with mobile computing facilities, in particular unprotected environments.</i>
---------------------------	---

3.6 Teleworking

Policies and procedures should be established to control teleworking activities. Teleworking activities must be authorised by management.

Appropriate controls should be implemented to achieve the same level of security as that in an office environment. Controls for mobile computing also apply to teleworking activities.

Clause 9.8.2 in AS/NZS 7799.2:2003 provides additional guidance in the control of teleworking activities.

AS/NZS 7799.2:2003	<i>A.9.8.2 Policies and procedures shall be developed to authorise and control teleworking activities</i>
---------------------------	--

3.7 Asset Classification and Control

In order to assess information security risks effectively, the agency needs to identify all major assets that require protection and assign an Owner who has primary responsibility for the protection of this asset. The Owner should be able to establish the relative importance and value of the asset to the agency.

Section 5 Step 2 of [Part 1](#) of this Guideline provides a list of asset types that could be included.

AS/NZS 7799.2:2003	<i>A.5.1.1 An inventory of all important assets shall be drawn up and maintained.</i>
---------------------------	--

Assets should be classified in accordance with business needs and the impacts associated with these needs. The responsibility for classifying assets is with the originator or nominated owner of the asset. A classification scheme outlined in Section 5 [Part 1](#) of this Guideline may be used. Based on this information, the agency can then provide the appropriate level of protection.

AS/NZS 7799.2:2003	<i>A.5.2.1 Classifications and associated protective controls for information shall be suited to business needs for sharing or restricting information and the business impacts associated with such needs.</i>
---------------------------	--

Appropriate information labelling and handling procedures in accordance with the classification scheme should be established.

AS/NZS 7799.2:2003	<i>A.5.2.2 A set of procedures shall be defined for information labelling and handling in accordance with the classification scheme adopted by the</i>
---------------------------	---

Physical labels are normally used to label information assets. Electronic labelling may have to be used for documents in electronic form.

Additional guidance on asset classification and labelling may be found in Section 6 Volume C of the Protective Security Manual.

3.8 Personnel Practices

Personnel covers not only permanent and casual employees of the agency, but extends to contractors, consultants and other individuals working on the agency's premises or using the agency's information and information processing assets. ICT includes individuals working for vendors and other service providers.

3.8.1 JOB DESCRIPTIONS

To reduce the risks resulting from errors or intentional or unintentional breach of security, all personnel should be made aware of their responsibilities for implementing and maintaining effective information security controls. Clear roles and responsibilities for the security of information and information systems, should be developed and documented in their job descriptions.

AS/NZS 7799.2:2003 A.6.1.1 Security roles and responsibilities as laid down in the organisation's information security policy shall be documented in job definitions where appropriate.

3.8.2 SEGREGATION OF DUTIES

In the development of job descriptions, ICT is important to ensure that no individual has the ability to both perpetrate and conceal an accidental or intentional breach of information security. This is best achieved by the segregation of incompatible duties or knowledge so that collusion between two or more personnel is required to conceal a security breach. Where segregation of duties is not practical, there should be adequate supervision and review of activities.

Extending the segregation of duties to the 'two person' rule, is good practice; this means that certain tasks must be performed by two people, of similar knowledge and expertise, working together. This helps protect against mistakes as well as deliberate weaknesses and is particularly important when setting up security controls.

AS/NZS 7799.2:2003 A.8.1.4 Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorised modification or misuse of information or services.

3.8.3 RECRUITMENT

Personnel employed in the administration, operation and support of information assets or in the handling of sensitive data are often in positions of trust. They have specialist technical knowledge and business insight that

places them in a unique position to abuse their job roles. More stringent screening processes should be utilised during recruitment of these personnel. In addition to technical skills, personal integrity is an important factor in the recruitment process.

Recruitment policies should emphasise the importance of adequate formal qualifications or other training, augmented by an appropriate level of relevant experience. References and previous employment details of applicants should be validated and police or other security checks should be performed on applicants for sensitive positions.

AS/NZS 7799.2:2003 <i>A.6.1.2 Verification checks on permanent staff shall be carried out at the time of job applications.</i>
--

3.8.4 TERMS AND CONDITIONS OF EMPLOYMENT

The terms and conditions of employment should include the employee's responsibilities for information security either within or outside the agency, as well as the consequences of non-compliance to information security policies and procedures.

As part of the terms and conditions of employment, all personnel should be required to sign confidentiality agreements.

AS/NZS 7799.2:2003 <i>A.6.1.3 Employees shall sign a confidentiality agreement as part of their initial terms and conditions of employment.</i>

AS/NZS 7799.2:2003 <i>A.6.1.4 The terms and conditions of employment shall state the employee's responsibility for information security.</i>
--

3.8.5 MONITORING OF PERSONNEL

Work of all staff should be subject to periodic review and approval procedures by a more senior member of staff.

Activities of personnel should be supervised and peer reviews of their work may be established. Close supervision is especially important for junior personnel with privileged system access. Periodic formal performance reviews for all personnel should be conducted.

Periodic rotation of tasks between personnel should be implemented to limit the opportunity for fraud and to increase the chance of exposure. Where shift work is involved, rotate personnel through all shifts and mix the composition of shift rosters.

Management should be aware of changes to a person's morale, attitude to work and external pressures and take appropriate action to ensure that information security is not threatened. Suspicions should be aroused when staff do not take holidays, work unduly long hours or live beyond their means.

When personnel are disciplined or otherwise feel disaffected, a program of closer supervision and audit of their activities should be implemented.

3.8.6 TERMINATIONS AND JOB CHANGES

Formal communication between the human resources function and the information security function should be in place for notification of any terminations or changes in employment.

A formal exit procedure for personnel leaving the agency should be established to ensure that:

- All assets of the agency are returned, including policy and procedure manuals and technical documentation;
- Keys, passes and other access devices are returned;
- Deactivation or deletion of the person's access identifiers and the removal of the access authorities granted to them revokes access to information systems.

Management should ensure that personnel leaving the agency under duress or with ill-feeling do not have access to information assets during any period of notice. Escalating the provisions of the exit procedures, especially immediately revoking system access, is a recommended first step. For additional protection the person, particularly if he/she is in a position of trust, should not be required to serve the period of notice and should be escorted from the premises.

Similar procedures should be applied to personnel who have temporarily or permanently changed jobs within the agency, particularly for those moving from a sensitive position to a less sensitive one.

3.9 Security Awareness and Training

Adequate training of all personnel is critical to the effective implementation of information security. Security awareness and training activities should be ongoing to further demonstrate management's commitment to information security.

Information security policies and procedures are of little use unless they are understood and observed by the personnel who are affected by them. The agency must be proactive in communicating its expectations and requirements to its personnel, as well as in prescribing disciplinary action for non-compliance. ICT is not sufficient to publish policies and assume that personnel are aware of them, will read them and will adhere to them.

The agency must foster the development of a pervasive information security culture and personalise the issue so that all personnel are aware of their own responsibilities.

Personnel should be made aware of the importance of the information processes, the associated threats, vulnerabilities and risks and understand why controls are needed.

Personnel should be appropriately trained to perform their tasks, prior to access to systems and information being granted. Different levels of training may be required to match the requirements of their jobs. Security officers may require specialised security training or education.

Disciplinary measures that may be invoked for deliberate breaches of security should be publicised.

Periodic information security awareness seminars for all personnel should be conducted to advise of industry developments in information security and of new security initiatives within the agency, to present case studies, and to reinforce the need for security and for complying with the policies and procedures.

This topic is also discussed in [Part 1](#), Section 6 of this Guideline.

AS/NZS 7799.2:2003	<i>A.6.2.1 All employees of the organisation and, where relevant, third party users, shall receive appropriate training and regular updates in organisational policies and procedures.</i>
---------------------------	---

3.10 Compliance with Legal and Regulatory Requirements

Legal and regulatory requirements include various State Acts as listed in Section 8 of [Part 1](#) of the Guidelines. Agencies need to also consider the acts and regulations governing their specific industry.

When assessing information security risks and designing or implementing information systems, ICT is important to consider all relevant statutory, regulatory and contractual requirements to ensure compliance. Advice on specific legal requirements should be obtained from the agency's legal counsel.

AS/NZS 7799.2:2003	<i>A.12.1.1 All relevant statutory, regulatory and contractual requirements shall be explicitly defined and documented for each information system.</i>
---------------------------	--

In particular, policies and procedures should be established to:

- Ensure that restrictions relating to intellectual property rights such as copyright, design rights or trademarks are complied with;
- Prevent unauthorised copying and piracy of software for in-house use. This also applies to unauthorised copying and distribution of internally developed software to external organizations or individuals.

AS/NZS 7799.2:2003	<i>A.12.1.2 Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.</i>
---------------------------	---

- Provide guidance on the retention, storage, handling and disposal of records and information.

AS/NZS 7799.2:2003 ***A.12.1.3 Important records of an organisation shall be protected from loss, destruction and falsification.***

- Ensure that the processing, transmission and storage of personnel data are protected.

AS/NZS 7799.2:2003 ***A.12.1.4 Controls shall be applied to protect personal information in accordance with relevant legislation.***

- Ensure specific written authorisations for the use of information processing facilities are obtained prior to use and to monitor usage.

AS/NZS 7799.2:2003 ***A.12.1.5 Management shall authorise the use of information processing facilities and controls shall be applied to prevent the misuse of such facilities.***

- Ensure that legal advice is obtained regarding cryptographic controls, and particularly when encrypted data or cryptographic controls are moved to another country.

AS/NZS 7799.2:2003 ***A.12.1.6 Controls shall be in place to ensure compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls.***

- Ensure that adequate evidence is collected, in terms of admissibility, quality and completeness.

AS/NZS 7799.2:2003 ***A.12.1.7 Where action against a person or organisation involves the law, either civil or criminal, the evidence presented shall conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard. This shall include compliance with any published Standard or code of practice for the production of admissible evidence.***

3.11 Compliance with Security Policies and Standards

Managers should ensure that the information security policy and accompanying procedures are adhered to within their areas of responsibility through regular review. A formal regular review process should be implemented to periodically assess compliance with all policy and procedural requirements.

AS/NZS 7799.2:2003 ***A.12.2.1 Managers shall ensure that all security procedures within their area of responsibility are carried out correctly and all areas within the organisation shall be subject to regular review to ensure compliance with security policies and standards.***

Technical compliance checking of the correct implementation of hardware and software controls should be carried out regularly. This should only be conducted by, or under the supervision of, competent authorised persons.

The use of tiger teams or penetration testing are examples of such compliance checks.

AS/NZS 7799.2:2003	<i>A.12.2.2 Information systems shall be regularly checked for compliance with security implementation standards.</i>
---------------------------	--

3.12 Incident Handling

Incident handling is an important aspect of managing information security risk. A security incident may occur from failures of hardware, infrastructure or software; inadequate operational procedures; malicious code; hacking; and/or human errors.

Whatever factors contribute to an incident, ICT is important that the cause be analysed and corrected, to prevent a recurrence.

Procedures should be established to:

- Require all employees and contractors to quickly report incidents, whether observed or suspected, that may have an impact on the security of the Agency's assets to a designated point of contact.
- Use a standard taxonomy for classifying incidents. See Attachment C in [Part 1](#) of these Guidelines.
- Provide suitable feedback to relevant personnel regarding the status of the reported incidents.

AS/NZS 7799.2:2003	<i>A.6.3.1 Security incidents shall be reported through appropriate management channels as soon after the incident is discovered as possible.</i>
---------------------------	--

AS/NZS 7799.2:2003	<i>A.6.3.2 Users of information services shall be required to note and report any observed or suspected security weaknesses in or threats to systems or services.</i>
---------------------------	--

- Ensure that adequate details relating to software malfunctions are recorded and the actions to be followed are implemented.

AS/NZS 7799.2:2003	<i>A.6.3.3 Procedures shall be established and followed for reporting software malfunctions.</i>
---------------------------	---

- Quantify and monitor incidents and malfunctions for analysis to assist in implementing measures to avoid incidents.

AS/NZS 7799.2:2003	A.6.3.4 Mechanisms shall be in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.
---------------------------	--

- Implement incident response procedures, which should be consistent with the business continuity plan.

AS/NZS 7799.2:2003	A.8.1.3 Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents.
---------------------------	--

Incident handling management helps in containing and repairing damage from incidents, preventing future occurrences and damages, providing input to threat and vulnerability assessments, improving internal communications, training and awareness programs.

3.13 Disciplinary Process

A formal disciplinary process should be established for employees who have violated the Agency information security policy and / or procedures. Any process established should ensure correct and fair treatment for employees suspected of committing any breaches of security.

All employees should be aware of and acknowledge the consequences of any violation of the information and security policy and procedures.

AS/NZS 7799.2:2003	A.6.3.5 The violation of organisation security policies and procedures by employees shall be dealt with through a formal disciplinary process.
---------------------------	---

3.14 Business Continuity Management

A management process must be in place to protect the agency, especially its critical business processes, from the effects of a major failure or disaster, and minimise any damage or loss caused by such events. This management process should address the following:

- Identifying the events and environmental surroundings that can adversely affect the agency and its facilities with disruptions or disasters, the likelihood and impact of such occurrences;
- Assessing the impacts of these events with the view to identifying critical business processes, recovery periods and priorities, and inter-dependencies;
- Determining business continuity strategies which are consistent with agreed business objectives and priorities;

- Developing and implementing procedures for responding to and stabilizing the disruption or disaster situation;
- Developing and implementing business continuity plans consistent with agreed strategies;
- Providing awareness and training programs in the execution of the plans, including emergency and crisis management procedures;
- Maintaining and testing business continuity plans to ensure that they are current, practical and effective;
- Assigning responsibilities for the co-ordination, development, implementation, review and update of the business continuity plans;
- Considering the purchase of suitable insurance as part of the process.

AS/NZS 7799.2:2003	<i>A.11.1.1 There shall be a managed process in place for developing and maintaining business continuity throughout the organisation.</i>
---------------------------	--

AS/NZS 7799.2:2003	<i>A.11.1.2 A strategy plan based on appropriate risk assessment shall be developed for the overall approach to business continuity.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.11.1.3 Plans shall be developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes.</i>
---------------------------	--

AS/NZS 7799.2:2003	<i>A.11.1.5 Business continuity plans shall be tested regularly and maintained by regular reviews to ensure that they are up to date and effective.</i>
---------------------------	--

A number of business continuity plans may be developed, eg for different information processing platforms. A single framework must be maintained to ensure consistency and to identify priorities for testing and maintenance. Each plan must have an owner and should clearly specify the conditions for its activation, emergency procedures, fall back procedures, resumption procedures, maintenance procedures, awareness and education activities, and individuals responsible for the execution of the plan.

AS/NZS 7799.2:2003	<i>A.1.1.4 A single framework of business continuity plans shall be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.</i>
---------------------------	--

The planning should also address the availability of backup processing facilities and the vital records that the business will need to service each of its critical functions. Vital records include, but are not limited to, the following types of information:

- Backups of critical computer files, in a form suitable for speedy and reliable restoration on the backup processing facilities;
- A catalogue of the contents of each backup;

- Reports to assist the business units to operate with manual procedures or an incomplete ICT service;
- Independent or external transaction logs;
- Operating instructions, procedures and business rules, adjusted for the emergency situation;
- The names and contact details for all relevant personnel;
- The business continuity plans.

AS/NZS 7799.2:2003 A.8.4.1 Back up copies of essential business information and software shall be taken regularly.

The decision for the type of backup processing facilities will depend on the agreed business priorities and strategies.

The common types of backup facility are categorised below, in increasing order of protection and likely cost.

- *Reciprocal arrangements* may be made with another organisation using similar ICT hardware and software for each party to make a portion of its facilities available should the other party suffer a disaster. The major concern with this approach is in the commitment of the partner organisation and its ability to deliver the promised ICT resources when they are needed. The partner organisation will still have to satisfy the processing needs of its own business functions. In addition, its spare resources may not be easily realisable and may be insufficient to provide the backup service required. This type of facility is best suited to an organisation that has a low level of dependence on ICT for its critical business functions, and only limited or no requirement for on-line services. Even then ICT is advisable to make reciprocal arrangements with more than one partner.
- *Cold sites* are premises fitted out with the necessary utility supplies and ready to receive replacement equipment. The premises may belong to the organisation or to a service provider who contracts to make them available when required. ICT may take some days, perhaps a week or two, to make the site fully operational.
- *Warm sites* are premises already housing IT equipment suitable for sustaining the critical business functions. The data backups must firstly be loaded and other vital records used to resume business processing. Communications lines may also have to be rerouted to the site. ICT should typically take several hours, perhaps up to a day or two, to make the site operational. Again the site may be owned by the organisation or the service may be contracted from an external supplier.
- *Hot sites* are premises housing IT equipment and duplicate communications facilities that are continuously available and that process critical business functions in parallel with the primary site. ICT is possible to activate the site instantaneously, or with a delay of several minutes at

most. One effective implementation is referred to as site mirroring, in which two identical sites share the workload and continuously update each other. They can each provide instantaneous backup of the other. Hot sites may be owned by the organisation.

Once the type of facility has been selected, there are a number of important issues to consider in selecting a suitable partner or service provider, in particular, the likelihood of the other party also being affected by the same disaster.

Separate power grids and communications exchanges might be prudent, for example. Accommodation and telephone access for personnel is also important. When contracting with service providers additional considerations might include the compatibility of the hardware and software available, the location and numbers of other subscribers, and the capability to support joint emergency use. Formal contracts or written agreements with external parties to guarantee access to the backup facilities when required, including for testing, and periodically reconfirm their ability to supply the service.

3.15 System Audits

The importance of independent audit as a control cannot be underestimated. ICT can take many forms, from reviewing other controls and identifying their strengths and weaknesses, to monitoring user behaviour and system activity. Audits are a key element in managing vulnerabilities. Monitoring of system activities is covered in [Section 5.9](#)

3.15.1 AUDITS OF OPERATIONAL SYSTEMS

The audits of operational systems involve the review of existing controls within the operational systems (ie, the operating system and/or application system) with the objective to provide management assurance that the controls implemented are effective and to report to management any deficiencies together with the appropriate recommended actions. Internal and/or external auditors, or specialist organisations, with the appropriate skills and experience may perform audits.

To minimise disruptions to business activities, the scope, approach, audit requirements and timing of the audits should be planned carefully and agreed with the appropriate management. Access to ICT resources should be made available but access to software and data should be restricted to “read” access only. Where access required is other than “read-only”, separate copies of files should be made to be accessed solely for audit purposes, and should be erased once the audit is completed.

AS/NZS 7799.2:2003	<i>A.12.3.1 Audits of operational systems shall be planned and agreed such as to minimise the risk of disruptions to business.</i>
-------------------------------	---

When system audit tools are used, these should be separated from the development and operational systems environments to prevent any misuse

or compromise. Both software and data files should be restricted from access by ICT personnel (eg, in tape libraries) or users (eg, in user areas).

AS/NZS 7799.2:2003	<i>A.12.3.2 Access to systems audit tools shall be protected to prevent possible misuse or compromise.</i>
-------------------------------	---

4. Physical and Environmental Controls

This section describes the controls associated with physical protection of data, systems, buildings and related supporting infrastructure to prevent:

- Unauthorised access, damage and interference to business premises and information;
- Loss, damage or compromise of assets;
- Compromise or theft of information and information processing facilities.

4.1 Secure Areas

Information processing facilities should be maintained within secure areas to protect them from unauthorised access destruction or manipulation. Such protective measures may include physical security, fire protection, water / liquid protection, power and air-conditioning protection, infrastructure planning (building design or cabling), and visitor control systems.

AS/NZS 7799.2:2003	A.7.1.1 Organisation shall use security perimeters to protect areas which contain information processing facilities.
---------------------------	---

AS/NZS 7799.2:2003	A.7.1.2 Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.
---------------------------	---

AS/NZS 7799.2:2003	A.7.1.3 Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.
---------------------------	--

AS/NZS 7799.2:2003	A.7.1.4 Additional controls and guidelines for working in secure areas shall be used to enhance the security provided by the physical controls protecting the secure areas.
---------------------------	--

AS/NZS 7799.2:2003	A.7.1.5 Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.
---------------------------	---

4.2 Equipment Security

All information processing equipment should be safeguarded from the environment and only accessible to authorised personnel. Equipment should be protected from the elements, power surges, power failures, electromagnetic interference and unauthorised access.

AS/NZS 7799.2:2003	A.7.2.1 Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.
---------------------------	---

AS/NZS 7799.2:2003	A.7.2.2 Equipment shall be protected from power failures and other electrical anomalies.
---------------------------	---

AS/NZS 7799.2:2003	A.7.2.3 Power and telecommunications cabling carrying data or
---------------------------	--

supporting information services shall be protected from interception or damage.

AS/NZS 7799.2:2003 *A.7.2.4 Equipment shall be maintained in accordance with manufacturer's instructions and/or documented procedures to ensure its continued availability and integrity.*

AS/NZS 7799.2:2003 *A.7.2.5 Security procedures and controls shall be used to secure equipment used outside an organisation's premises.*

AS/NZS 7799.2:2003 *A.7.2.6 Information shall be erased from equipment prior to disposal or re-use.*

4.3 Clear desk and screen policy

The accumulation of papers and files on desks is subject to theft or loss. Sensitive data and files should be maintained in lockable cabinets and passworded screen savers should be employed when staff have data on their PCs or terminals.

AS/NZS 7799.2:2003 *A.7.3.1 Organisations shall have and implement a clear desk and a clear screen policy in order to reduce the risks of unauthorised access, loss of, and damage to information.*

4.4 Removal of property

The removal of property including data, hardware or software should not be allowed without authorisation. Consideration could be given to anchoring all desktop computers to prevent their theft and passwords being implemented before access to laptops is allowed.

AS/NZS 7799.2:2003 *A.7.3.2 Equipment, information or software belonging to the organisation shall not be removed without authorisation.*

5: Operational controls

This section describes the controls relating to the secure, correct and reliable functioning of the ICT Facilities. Operational controls can be implemented by instituting organisational procedures.

5.1 Documentation

Documented operating procedures shall be maintained for all normal operating situations and kept under configuration control. The ICT Security Policy, where all the security procedures are documented and the Business Continuity Plan, where the BCP strategies are documented, should be maintained and kept current.

AS/NZS 7799.2:2003 A.7.1.1 <i>The operating procedures identified in the security policy shall be documented and maintained.</i>
--

5.2 Configuration and change management

Software, hardware and documentation changes to ICT facilities must be controlled. Configuration Management is the process of controlling and tracking changes to all ICT items, software, hardware or documentation to ensure that they are authorised and can be reversed if required. Configuration management requires the establishment of baselines against which all changes are tracked. Traceability of changes requires the use of versions so that changes can be traced to a specific version of the software, hardware or document.

Configuration Management is an essential element in managing the vulnerability of systems. Areas of potential vulnerability include security control applications and devices, security features in other applications and databases, and the configuration of operating and other system software. Particular issues to be addressed include:

- Procedures to react promptly to vendor announcements of defects and software patches;
- Procedures to document and audit configurations and settings.

Software changes should only be “checked out” from and “checked into” the production libraries after they been authorised. Hardware changes must also be carefully planned before being implemented.

Configuration and change management ensures that changes to ICT systems do not introduce additional security threats by reducing the effectiveness of existing controls.

AS/NZS 7799.2:20030 A.7.1.2 <i>Changes to information processing facilities and systems shall be controlled.</i>
--

Configuration management must also be applied when changes to the operating system are implemented. When operating system patches are released, they should be tested on a separate test system to ensure that the application software will not be affected.

AS/NZS 7799.2:2003	A.7.5.2 Application systems shall be reviewed and tested when changes occur.
---------------------------	---

5.3 Incident Management

Procedures should be developed, documented and updated to record any security breach, whether accidental or deliberate, the action taken to correct the breach and any recommendation to prevent such a breach.

Whenever a Security breach occurs the incident should be:

- Logged;
- Assigned for follow-up;
- Analysed;
- Recommendation made in respect of prevention;
- Closed out.

Incident response procedures should be established for each system to include system failures, denial of service and breaches of confidentiality. These procedures need to cover:

- Analysis and identification of the cause of an incident;
- Development and implementation of countermeasures to prevent the breach;
- Review of Audit trails;
- Discussions with business users and others affected by, or involved with, recovery from the incident.

Corrective action to recover from a security breach and system failure should be developed so that:

- Authorised staff are allowed access to systems and data;
- Emergency actions are documented;
- Emergency action is reported to management;
- The integrity of business systems and security controls is confirmed quickly.

Management of security incidents should lead to improvements in Information Security Management.

AS/NZS 7799.2:2003	A.8.1.3 Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents.
---------------------------	--

5.4 Software Development and Test Environment

Software development, testing and operational environments should exist separately. Software developers should only be able to access software development libraries. Configuration management should ensure that the movement of code from development to testing and production (operations) is done in a controlled and authorised manner.

Separating development, testing and operational environments is necessary to enforce an adequate segregation of duties between developers, testers and operations staff in an ICT environment. This segregation of duties is desirable so as to reduce the risk of accidental or deliberate change or unauthorised access to operational software and data.

The updating of operational libraries should only be performed by authorised operational staff.

Audit logs should be maintained for all access to Operational program source and object libraries.

AS/NZS 7799.2:2003	<i>A.8.1.4 Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorised modification or misuse of information or services.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.8.1.5 Development and testing facilities shall be separated from operational facilities.</i>
---------------------------	--

AS/NZS 7799.2:2003	<i>A.10.4.1 Control shall be applied to the implementation of software on operational systems..</i>
---------------------------	--

AS/NZS 7799.2:2003	<i>A.10.4.3 Strict control shall be maintained over access to program source libraries.</i>
---------------------------	--

AS/NZS 7799.2:2003	<i>A.10.5.1 The implementation of changes shall be strictly controlled by the use of formal change control procedures to minimize the corruption of information systems.</i>
---------------------------	---

5.5 Outsourced Facilities

Outsourced ICT facilities can introduce potential security exposures, such as the unauthorised access, damage or loss of data at the outsourced facility. Risk identification should be undertaken and these risks addressed in the outsourcing agreement.

Specific security issues which need to be addressed are:

- Determining whether sensitive data and/or applications can be outsourced;

- Defining the security standards to be applied and how compliance is to be measured;
- Obtaining authorisation of systems owners;
- Definition of security roles and responsibilities in monitoring, reporting and handling breaches;
- Business continuity requirements and responsibilities

AS/NZS 7799.2:2003	<i>A.8.1.6 Prior to using external facilities management services, the risks shall be identified and appropriate controls agreed with the contractor and incorporated into the contract.</i>
---------------------------	---

Outsourced software development requires consideration of the following issues:

- Quality assurance procedures to be applied, including the rights and obligations of the Agency and Outsourcer;
- Licensing arrangements and ownership of code;
- Rights to software in the event of financial failure of the outsourcer.

AS/NZS 7799.2:2003	<i>A.10.5.5 Controls shall be applied to secure outsourced software development.</i>
---------------------------	---

5.6 Systems planning

Capacity planning must be performed to ensure that existing ICT facilities can cater for any new systems. Capacity planning should be used to avoid failures due to inadequate capacity. Storage and memory requirements need to be monitored and new capacity planned for, so that new systems can be implemented when required.

In planning future capacity requirements for a system, current trends should be taken into account. Potential bottlenecks should be avoided that could cause a threat to system security or user access.

AS/NZS 7799.2:2003	<i>A.8.2.1 Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.</i>
---------------------------	--

5.7 Systems and Acceptance Testing

System Testing, which tests that the system meets its System Design specifications, must be completed, before the system is handed over to the business users for Acceptance Testing. System Testing must be planned and comprehensive in scope. Live data should not be used for System Testing. During System Testing, controls over test data need to be implemented. These controls may include:

- All actual data should be changed prior to use;
- Authorisation should be obtained every time copies of actual data are made;

- Where live data is used ICT should be deleted after use;
- Logs should be updated when copying of operational data is made.

Acceptance criteria for all new systems should be agreed in advance. Acceptance Testing ensures that the system delivered complies with the functionality specified in the User Requirements and works in an acceptable way to the user. User Acceptance Testing must be documented and may include:

- Functional testing – testing of functionality delivered against specification.
- Performance testing – testing the application against performance benchmarks.
- Useability testing – verifying that the system is logical and can be used by end users. Note that a system may have correct functionality but be difficult to use.
- Interface testing – verifying that the user interface (eg, Windows) is consistent and integrates with other applications.
- Security testing – ensuring that the overall security requirements of the system at the application level are acceptable.
- Sociability testing – to ensure the application works as expected in the specified environment where other applications run concurrently.
- Recovery testing – testing that the system can recover if the hardware or network fails.

AS/NZS 7799.2:2003	<i>A.8.2.2 Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.10.4.2 Test data shall be protected and controlled.</i>
---------------------------	---

5.8 Protection against Malicious Code

Viruses, trojan horses, worms and logic bombs are all examples of malicious code. Controls need to be in place to prevent, detect and correct the effects of malicious code.

Controls over Malicious Code include:

- All systems should be protected by the latest version of Anti Virus software. Many vendors such as McAfee, Symantec (Norton's), Cheyenne, Dr Solomon have Anti virus products that are updated regularly. Agencies must keep their anti virus software up to date so that new viruses can be detected and prevented from infecting the organisations hardware. Anti virus software should be continually monitoring the users machine or server (web, mail, file) to detect virus as soon as one attempts to infect the agency's hardware.

Users must be educated:

- Not to install unauthorised software onto the agency's computers.;
- Not to download software from the Internet onto the agency's computers;
- To only install software purchased from reputable sources;
- Not to open e-mails from sources they are not familiar with.

All e-mail attachments must be scanned by suitable software to detect the presence of known macro viruses. Some of these viruses are spread very quickly so security administrators must act immediately when such a virus is identified to limit its effect.

The Agency should be a member of a Virus Security Alert group or mailing list that will advise when a new potentially dangerous virus has been detected. Many of the virus detection software companies maintain Virus update pages that provide information on new viruses and as mentioned above updates to their products which can be downloaded.

Agencies should maintain a Formal policy requiring compliance with software licencing and prohibiting the use of unauthorised (pirated) software.

AS/NZS 7799.2:2003	<i>A.8.3.1 Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.10.5.4 The purchase, use and modification of software shall be controlled and checked to protect against possible covert channels and Trojan Code.</i>
---------------------------	--

5.9 Data Backup

Backup data is vital when trying to recover files that have been corrupted or destroyed. Backups should be scheduled to ensure the timely restoration of files as and when required. Many organisations backup data at least daily with weekly and monthly cycles maintained for archive purposes. System backups of the operating system or application software can be performed less frequently as this data is less volatile. Weekly System backups are recommended to minimise the disruption of a corrupt file or hardware problem requiring restoration of any system files. Backup copies (preferably the most recent) must be retained offsite for Business Continuity Plan purposes.

Backup and restore procedures should be documented and tested on a regular basis. Backup procedures will be tested every time a backup is made, but only by performing a successful restore can the validity of the backup/restore procedure and the reliability of the media be verified.

Data and System Backups should be kept in suitable media containers, preferably in fire rated premises or safes.

Backup media should be recycled and replaced after a period of use. The cost of not having a reliable copy of a file is much higher than the value of the storage media.

AS/NZS 7799.2:2003	<i>A.8.4.1 Backup copies of essential business information and software shall be taken regularly.</i>
---------------------------	--

5.10 Logging

Operator logs should be maintained which report all the activities performed by the computer operator. These logs should detail:

- What applications were running;
- What actions were initiated by the operator;
- What system messages were displayed on the operator console;
- System errors and corrective action taken.

Operator logs should be reviewed on a regular basis to ensure that correct operating procedures have been complied with.

Faults should be reported on fault logs. Fault logs should be completed whenever a user reports a problem with the System. Fault logs must be reviewed to ensure there are no outstanding issues and that corrective action is appropriate and does not compromise security.

AS/NZS 7799.2:2003	<i>A.8.4.2 Operational staff shall maintain a log of their operational activities.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.8.4.3 Faults shall be reported and corrective action taken.</i>
---------------------------	---

5.11 Software and Information exchange

Exchanges of data between organisations should be controlled and comply with relevant legislation. Such exchanges of data should be subject to a written agreement. The business and the security implications associated with electronic data interchange, electronic commerce and electronic mail need to be considered.

When reviewing such agreements, security conditions should be considered such as:

- Management responsibilities in respect of notifying and controlling transmission, dispatch and receipt;
- Notification of the sender re transmission, dispatch and receipt;
- Identification of couriers;
- Responsibility and liability for data loss;
- Technical standards for packaging, transmission, recording and reading information and software;

- Controls to be used such as cryptography.

AS/NZS 7799.2:2003 **A.8.7.1 Agreements, some of which will be formal, shall be established for the electronic or manual exchange of information and software between organisations.**

5.12 Security of media in transit

Media are vulnerable to unauthorised physical access while being transported. Mail services and couriers have access to this media.

Security of media in transit should be protected by ensuring that:

- Only reputable couriers or postal services are used;
- Protective packaging should be utilised to protect the contents from physical damage;
- Sensitive information should be protected by special controls such as locked containers, hand delivery, tamper evident packaging.

AS/NZS 7799.2:2003 **A.8.7.2 Media being transported shall be protected from unauthorised access, misuse or corruption.**

5.13 Electronic Commerce Security

Electronic commerce was defined by the US Department of Commerce in 1994 as “something that integrates communications, data management and security services so that business applications in different organisations can automatically exchange information”. Electronic commerce includes EDI, e-mail, FTP transfers and internet commerce.

5.13.1 ELECTRONIC DATA INTERCHANGE (EDI)

EDI is the transfer of information from computer application to application based on a structured format usually between separate organisations. The banking industry has been using EDI for a number of years for fund transfers and ATM networks. The motor vehicle industry has also embraced EDI in that vehicle builders such as Ford and GM now order all parts electronically and pay suppliers electronically.

State Government Agencies have been using the Supply Line service for a number of years.

When using EDI (and in fact any form of electronic commerce) a number of issues must be addressed. These include:

Authentication Verification of each partners identity;
Authorisation Who is authorised to transact business, sign documents etc;
Order processes How are orders taken, confidentiality and integrity maintained, and non-repudiation of an order (contract) guaranteed;

Confidentiality	Who can view sensitive information;
Pricing	How much trust can be placed in the advertised price and confidentiality of discount arrangements;
Verification	How are order details verified;
Settlement	What method of payment is appropriate;
Liability	Who is liable for fraudulent or erroneous transactions.

Electronic commerce between trading partners should be supported by a written agreement that clearly states the terms upon which they are to transact business and address all the security concerns above. Due to the closed nature of EDI arrangements the confidentiality and privacy concerns are not as great as with other forms of electronic commerce where the parties are unknown to each other.

5.13.2 INTERNET COMMERCE

Internet commerce is electronic commerce that takes place over a public network (the Internet) which by its nature provides minimal security and privacy. Messages (data) are sent in clear text and are therefore susceptible to eavesdropping or sniffing. This eavesdropping can occur on any point in the network and because the Internet is a public network this could occur anywhere in the world. Electronic commerce on the Internet therefore has additional risks that can be controlled in an EDI environment. Privacy and confidentiality issues are most serious concerns in internet commerce. Agencies must ensure that they do not breach their legislative requirements in respect of privacy when providing internet commerce facilities.

Security of electronic commerce over the Internet requires consideration of a number of threats such as:

Masquerading	Pretending to be someone else;
Message sequencing	Replaying messages in a different order;
Modification	Changing the content of messages;
Data Integrity	Error introduced by hardware or deliberate act;
Denial of Service	Flooding of the network with messages;
Repudiation	Denial of message origination;
Confidentiality	Unauthorised access to message content.

Controls need to be implemented to mitigate the risk of such threats.

The use of cryptography, firewalls and digital signatures, which are discussed in a later section, can address many of these threats.

AS/NZS 7799.2:2003 A.8.7.3 Electronic Commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.

5.14 Electronic Mail Security

Electronic mail (e-mail) has become one of the main applications of data exchange used between individuals, companies and government agencies. Because e-mail is a form of electronic commerce, the same security threats apply. In addition viruses, which are the major security threat today, use e-mail as the most popular medium of infection.

Agencies should develop a clear e-mail policy that addresses the following:

- When ICT is appropriate to use e-mail;
- What can be said in e-mails on the agency's behalf;
- How to protect e-mail from viruses;
- Caution to be applied when opening e-mail attachments;
- Responsibilities in respect of e-mail usage (not to defame others, not to use profanities, not to send private e-mails, not to send spam mail or harassment);
- Retention policies;
- Use of cryptography to protect confidentiality, integrity and authenticity;
- Use of digital signatures to authenticate originators and provide evidence against repudiation.

AS/NZS 7799.2:2003	<i>A.8.7.4 A policy for the use of electronic mail shall be developed and controls put in place to reduce risks created by electronic mail.</i>
---------------------------	--

5.15 Electronic Office Systems

Electronic office systems include computers, laptops, PDAs, mail, voicemail, fax, multimedia and postal services. These systems provide for speedier distribution of information. Policies need to be implemented to control what is distributed and how ICT is distributed.

Use of mobile phones could lead to confidential information being overheard in public places.

AS/NZS 7799.2:2003	<i>A.8.7.5 Policies and guidelines shall be prepared and implemented to control the business and security risks associated with electronic office systems.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.8.7.7 Procedures and controls shall be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.</i>
---------------------------	---

5.16 Electronic Publishing

Information available on publicly available systems, such as a web server, should be carefully reviewed before publication to ensure the confidentiality and integrity of the data. Agencies must not publish data which has been provided by the public and which is confidential in nature and protected by law. Medical histories, tax data, education records, and private phone numbers are examples of data

that should not be made available over the web. Information must be obtained in accordance with data protection legislation and only divulged where appropriate.

A firewall should be installed between the web server and the external network and also between the internal network and the web server. In effect the web server is maintained in what is termed a “demilitarised zone”. In this configuration the firewall prevents the Web Server from sending packets into the organisations network. If attackers from the Internet penetrate the external Web server they have no more access to the organisations internal network than they had before.

AS/NZS 7799.2:2003	<i>A.8.7.6 There shall be a formal authorisation process before information is made publicly available and the integrity of such information shall be protected to prevent unauthorised modification.</i>
---------------------------	--

5.17 Media

Care of media covers the requirement for the suitable storage of both hardcopy and magnetic media which will ensure that both are secure and useable, preventing damage to assets and interruptions to activities. Accountability for media should be clearly defined, particularly in respect of easily removed media such as floppy disks, back up tapes and paper.

Policy and procedures should be developed and published that specifies the storage standards and environment for media storage, the process for logging movement of media, the access control standards and the guidelines for the proper disposal of media by the Agency.

Media brought into an installation should be added to the inventory immediately upon receipt. Software can be used to maintain a tape inventory.

In maintaining an inventory ICT is essential that removable media items be labelled. Care must be taken not to incorrectly label a item.

All removable media should be stored in a safe, secure environment, such that media is protected from extremes of temperature, weather and unauthorised access.

Where the content of the media is confidential, then the level of security over the media must also be increased to a suitable level. Media that contains confidential or classified data must be distinguished from media assigned to a scratch area. Where the media containing confidential data can be reused, ICT must have the data erased before being reused. Paper documents should be shredded when disposed of.

Media stocktakes should be regularly scheduled so that any lost items are quickly identified and action taken to recover them if possible..

Media stored offsite must:

- Be suitably stored with respect to safety and security.
- Be subject to appropriate handing procedures. These procedures should cover how media is returned from offsite locations, who is authorised to receive media, and identification of personnel. These procedures need to cater for after hours access.
- Where offsite storage is contracted to an outside organisation, personnel and security arrangements must be defined in the contract.

Records should be maintained of all media brought into and taken out of the agency. Vendors distribution media and technicians diagnostic tools should be included. No privately owned media should be allowed on site. Where ICT is deemed necessary to use privately owned media then ICT must be scanned for malicious software when received and viewed for confidential data when being taken out.

Disposal of sensitive media items should be logged to maintain an audit trail.

AS/NZS 7799.2:2003	<i>A.8.6.1 The management of removable computer media such as tapes, disks, cassettes and printed reports shall be controlled.</i>
AS/NZS 7799.2:2003	<i>A.8.6.2 Media shall be disposed of securely and safely when no longer required.</i>
AS/NZS 7799.2:2003	<i>A.8.6.3 Procedures for the handling and storage of information shall be established in order to protect such information from unauthorised disclosure or misuse.</i>
AS/NZS 7799.2:2003	<i>A.8.6.4 Systems documentation shall be protected from unauthorised access.</i>

6. Technical controls

Technical controls must be implemented to ensure confidentiality of data and authorised access to systems is maintained.

Controls must be implemented to restrict access to information, computers, networks, applications, system resources, files and programs.

6.1 Identification and Authentication

Identification is the means by which a user provides a claimed identity to a system. Authentication is the means by which this claim is validated. An identifier or user id is usually a series of non-secret characters that are used to attempt log in to a system. Until the user authenticates himself he will have no access to the system.

The identifier is a mechanism to allow the user access to various resources, files, directories, printers on the system. The identifier must be unique to the user so that he can be held accountable for any actions performed using that identifier. When the user changes his role, is transferred or promoted, then he should have his access rights changed to reflect his new role. When the user leaves the agency, his user identifier should be immediately removed from the system.

Authentication is required before the user can logon to the system. There are three types of "authentication":

- Identification and Authentication based on what a **User knows**. Passwords and phrases are often used to authenticate users;
- Identification and Authentication based on what a **User has**. Tokens such as magnetic cards, and smartcards are examples. A common application of magnetic cards is the use of an ATM where the user must possess the card and provide a pin number. Use of a challenge response system such as RSA Secure ID or RACAL Watchword is an example of the use of a smartcard.;
- Identification and Authentication based on what a **User is**. These are biometric measurements or features such as finger prints, retina scans, voice recognition used to authenticate the user.

The security and utility of various authenticators is considered below:

6.1.2 PASSWORDS

Passwords are easy to implement, change and are inexpensive. Most user access systems employ them. Unfortunately they are also the easiest to compromise and require well educated and disciplined users to implement effectively. Bad password management practices contribute to weak password controls.

Examples include:

- Use of simple passwords;
- Writing down of passwords;
- Not changing passwords regularly.

An effective password management policy should include:

- Choosing passwords which are not found in the dictionary;
- Choosing passwords that are a combination of alphabetic characters, numbers and special characters !@#%&*() ?;
- Using a combination of upper and lower case characters Ab1E%xcP;
- Choosing passwords with a minimum length of 8 characters;
- Changing passwords every 30 days;
- Not allowing a password that has been used within the last 10 cycles (changes of passwords);
- Unique User ID and passwords for each user to maintain accountability;
- All default User ID's such as Guest should be disabled;
- All User ID's must require a password;
- Not retaining written records of passwords;
- Password confidential must be maintained;
- Passwords not being displayed during entry;
- Requirement to enter old password when changing to new password.

Passwords should be stored in encrypted format using a one way encryption algorithm.

The strength of passwords should be verified by the use of Password cracking programs such as L0phtcrack (available for NT Systems) which can be run by the Systems Administrators. Any weak passwords will be revealed quickly and can then be changed. Other threats to passwords include the use of "sniffers" which eavesdrop on the network and capture password hashes or data for cracking at a later time. Passwords can be compromised simply by viewing what a user types in.

Given the relative weakness of passwords compared to Tokens or Biometrics ICT is strongly recommended that if a system has a high degree of confidentiality attaching to ICT such as payroll, personnel, taxation or medical data, that an authentication method **other** than passwords be implemented. Token or biometric authentication methods are inherently more secure

6.1.2 TOKENS

Tokens provide the capability of having complex one time passwords that the user can never forget. These one time password systems are synchronised with the access system so that only the user possessing the token can gain access.

Token passwords usually require the input of a simple PIN known to the user, as well as the one-time password that is displayed on the token. Use of the PIN provides protection should the token be lost.

Should someone see what the user has entered, when logging into a session, they will not be able to use the password as ICT will be different the next time.

If the user leaves the agency without returning the token then the token can be deactivated.

Tokens provide the one form of authenticator that offers protection from compromise during logon, from a tapped line.

Tokens are usually smartcards, however various versions are now available including a version used with palm tops devices.

The main disadvantage of tokens is that initially they are more expensive than passwords to implement. This cost is continually being reduced. Currently tokens cost approximately \$100 each.

6.1.3 BIOMETRIC DEVICES

While these in theory provide the best authentication, they still present problems in practice. Continual improvement will see this technology gain in acceptance, both as the price of readers goes down and as the accuracy and reliability improves. Finger scanning and handwriting devices are examples of biometric devices that are currently available on the market.

Cost and reliability are the main disadvantages at present.

AS/NZS 7799.2:2003	<i>A.9.3.1 User shall be required to follow good security practices in the selection and use of passwords.</i>
-------------------------------	---

AS/NZS 7799.2:2003	<i>A.9.4.3 Access by remote users shall be subject to authentication.</i>
-------------------------------	--

AS/NZS 7799.2:2003	<i>A.9.4.4 Connections to remote computer systems shall be authenticated.</i>
-------------------------------	--

AS/NZS 7799.2:2003	<i>A.9.5.3 All users shall have a unique identifier for their personal and sole use so that activities can be traced to the responsible individual.</i>
-------------------------------	--

AS/NZS 7799.2:2003	<i>A.9.5.4 A password management program shall be in place to provide an effective, interactive facility which ensures quality passwords.</i>
-------------------------------	--

6.2 Logical Access

Access control is the term given to measures that can be applied to restrict the activities of legitimate computer users by controlling the resources they can access and the types of access permitted. Access control can be enforced by the use of Identification and Authentication details linked to access control lists that define what resources users are authorised to access.

An access control policy should be created which clearly defines, for each user or group of users, their access rights.

This policy should be determined by the organisational or business needs of the Agency. Access should be granted on a need to know basis in other words “as many rights as are necessary, and as few rights as are possible”.

The Access Control policy should:

- Identify security requirements of individual applications;
- Identify the resources that require protection;
- Define how user access will be managed, how new users are added and old users deleted;
- Define how users access will be managed in a distributed environment;
- Ensure consistency between access control and the confidential nature of data;
- Define any legislative obligations or contractual requirements with regard to access;
- Define how access to data, services and applications will be controlled including number of grace logins when incorrect password is entered;
- Define Access review policies.

When a user enters an incorrect user id/password combination then the system should allow no more than two further attempts before locking the user account and requiring the systems administrator to intervene.

AS/NZS 7799.2:2003	<i>A.9.1.1 Business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.9.2.1 There shall be formal user registration and de registration procedures for granting access to all multi-user information systems and services.</i>
---------------------------	--

AS/NZS 7799.2:2003	<i>A.9.2.2 The allocation and use of privileges shall be restricted and controlled.</i>
---------------------------	--

AS/NZS 7799.2:2003	<i>A.9.2.3 The allocation of passwords shall be controlled through a formal management process.</i>
---------------------------	--

6.3 Review of Access rights

All access rights given to users should be reviewed regularly and updated if the security or business needs for access have changed. Privileged access rights should be reviewed more frequently to ensure that they are not misused. Access rights should be withdrawn immediately they are no longer required.

AS/NZS 7799.2:2003	A.9.2.4 A formal process shall be conducted at regular intervals to review users' access rights.
---------------------------	---

6.4 Unattended User Hardware

All user workstations should be located in secure areas. When users leave their workstations or terminals they should log off the system or lock the terminals either physically by use of key locks etc or logically using software such as password protected screen savers. Sometimes features built into the operating system can be used to lock a workstation eg, Windows NT. An unattended workstation can be used by an attacker to:

- Gain unauthorised access to data;
- Be used to perform an unauthorised transaction for which the user who was logged in will be accountable for;
- Insert malicious software ;
- Steal the workstation or parts of it.

Inactive terminals in high risk areas should have automatic shutdown following a period of inactivity.

AS/NZS 7799.2:2003	A.9.3.2 Users shall be required to ensure unattended equipment has appropriate protection.
---------------------------	---

AS/NZS 7799.2:2003	A.9.5.7 Inactive terminals in high risk locations or serving high risk systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons.
---------------------------	---

6.5 Network Management

6.5.1 OPERATIONAL PROCEDURES

Networks have four main vulnerabilities to attackers: These are

- Through connection to public networks (The Internet);
- User workstations;
- Dial in lines;
- Communications facilities.

To ensure the security and confidentiality of information in networks and the protection of the supporting infrastructure the organisation should establish operational procedures and responsibilities to ensure the correct operation of the networks. Access to both internal and external networks should be controlled.

An intranet is a network composed of servers and workstations managed by a single organisation. Intranet nodes should be covered by a common network policy. This policy should include:

- The network and network services which can be accessed;
- Procedures for authorising access to networks and network services;
- Management controls and procedures to protect the access to networks and network services.

An extranet is a network composed of entities from a number of different organisations. Extranet nodes may have different ICT Security policies and may reside on different security management domains.

Requests for connection to a computer system can be made from a remote host on the network. The user is authenticated by the remote host and then requests a session with another host on the same network. Establishment of a network connection of this kind generally requires consideration of whether the user needs to be re-authenticated. By trusting the remote host the local host is assuming that the authentication processes on the remote host is secure.

Access by remote users should require re-authentication. Use of tokens or challenge/response system to authenticate users should be considered.

6.5.2 PREDEFINED USER ACCESS PATHS.

Workstation or terminal access to the network can be controlled by predefined access routes. This will limit the ability of the terminal to be used to provide unauthorised access or perform unauthorised function. Finance Division terminals should be restricted to finance system functions, Personnel to the personnel system etc. In addition by segregating the network into specific domain names, groups of users can be segregated and restricted to the data and applications they need access to. Firewalls can be used to actively control the flow of communications over the network.

6.5.3 DIAL IN ACCESS CONTROLS

Dial in access should be governed by a security policy that includes:

- Inventory listing of existing dial in lines.
- Consolidate all dial up activity to a central modem bank, locate the modem bank in an untrusted connection off the internal network and protect the network by intrusion detection and firewall technology.
- Do not publish analogue phone line numbers.
- Verify that telecommunication cabinets are secure.
- Regularly monitor dial in access logs for failed attempts etc.
- Do not display Banner information when connection is made. Use a very simple and inconspicuous logon prompt that says nothing about

your organisation. Issue a warning message that unauthorised use will be prosecuted.

- Require use of one time password tokens for authentication.
- Review of use of dial back modems. If the user is dialling in from a home base or other predictable number then dial back authentication should be feasible. The dial back modem must ensure that the user who dialled in has been disconnected otherwise the dial back will connect back with the user who is holding the line open.
- All dial in activity should be logged.
- Ensuring that help desk staff are aware of the danger of resetting remote access login authentication.
- Requiring all requests for dial in access to be authorised by senior management, and be implemented by a central ICT group.
- Consider the use of war dialling. War dialling involves the use of software to automate the dialling of the agencies phone numbers on a trial and error bases, noting any responses received from modems. Ranges of phone numbers can be entered restricting the number of calls made. This is a good way to find any unauthorised dial in lines.

Many organisations use remote dial up access for performing maintenance and support services. Such access should be strictly controlled with appropriate physical and logical controls employed. The hardware used to provide this service should be physically locked in a secure area. The modem providing dial in access should be disconnected when not required. All access should be logged.

6.5.4 NETWORK PLANNING

Advance planning and monitoring should be undertaken to enable reliable functioning and performance of the networks. Changes to the network should be controlled and any impacts on existing controls evaluated and appropriate action taken.

6.5.5 NETWORK CONFIGURATION

A standard approach for the configuration of the network should be established, including any special protection by firewalls. This includes a standardised approach to the configuration of servers throughout the agency. Documentation of the network must also be up to date so that the network can be maintained. Documentation is also important in ensuring that adequate security measures are in place. Any changes to the configuration of any component on the network must be subject to configuration management. Servers that are used as firewalls should be dedicated to that task, ie, no other software should be running on them.

6.5.6 SEGREGATION OF NETWORKS

With the widespread use of networks by many different areas within an agency, the risks and possibilities of misuse and unauthorised access are increased. Critical business units to be on the network should be kept separate both physically and logically. The use of separate logical domains can be used to segregate two areas within the agency (eg, Finance and

Marketing). Use can be made of a secure gateway or firewall between the two domains to control access and data flow. In addition development facilities should be segregated from operational facilities.

6.5.7. FIREWALLS

The Defence Signals Directorate (DSD) has defined a firewall in these terms: “The purpose of a firewall is to provide a point of defence and a controlled and audited access to services, both inside and outside the organisation’s private network, by permitting, denying and / or redirecting the flow of data across the firewall.”

Firewalls can be either application proxies or packet filtering gateways. Application proxies are considered more secure than packet filtering gateways although there is a performance trade-off. Where there are high security requirements ICT is often appropriate to use the two types in series.

It is recommended that Web Servers be separated from the rest of the Agency’s networks by using an internal firewall. If an attacker penetrates the Web Server, the rest of the network is still protected.

A firewall must:

- Be immune to penetration.
- All traffic between the internal and external networks must pass through the firewall.
- Only authorised traffic, defined by a firewall security policy, will be allowed to pass.
- The default firewall policies must deny all connections to and from the internal network. Only specifically authorised connections should be allowed.
- Provide a trusted path for its management.
- Audit capability to detect breaches and attempted network intrusions.
- Secure implementation must be verified.

Firewalls should have both TCP/IP level filtering and application proxy mediation.

The firewall security policy should be defined by the firewall / network administrator defining the allowed connections into the firewall. If there are no rules defined for a connection then the connection should be denied.

The firewall should have an alarm capability such that when a specified event is detected an alarm is sent to the firewall administrator. An audit trail should be available, and reviewed. ICT should include all connection attempts (both successful and unsuccessful) and administrator actions.

To effectively implement a firewall the following must be considered:

- Definition of the Firewall Security Policy defining its functionality, configuration and security management.
- Configuration of the firewall must be regularly verified and controlled via a Configuration Control Board. All changes in configuration must be authorized.
- All Firewall software patches should be applied and updated.
- Firewalls should be tested regularly for weaknesses.
- Audit logs must be reviewed regularly to uncover break-ins.
- Security incident response procedures must be implemented.

6.5.8 MONITORING OF NETWORK

Monitoring of the network allows for the identification of weaknesses within the existing network configuration. Routes of messages should be regularly monitored, so that weaknesses in existing configurations can be identified and re arrangements can be made due to the traffic analysis. Monitoring also provides the ability to identify attackers and can be used to tune the network.

6.5.9 INTRUSION DETECTION

Any attempt to gain entry to information systems or networks, or any successful unauthorised entry should be detected quickly so that the agency can respond in an appropriate and effective manner. Use of intrusion detection software such as RealSecure from ISS or SessionWall-3 from Abirnet should be considered.

6.5.10 INTERNET CONNECTION POLICIES

Connection to a public network such as the Internet raises the risk of hacker attack. All network connections to the Internet must be protected by a suitable Firewall. In addition, policies in respect of email, file transfers and downloads, accessing of sites etc need to be developed and implemented via the Firewall or email scanning software. Typical Internet connection policies would state that:

- All emails sent should relate to work activities.
- While the confidentiality of emails is respected they are subject to monitoring.
- Attachment to emails should not be larger than say 1 megabyte in size;
- No unsuitable material should be sent via email attachment eg, pornography, harassing language.
- No unsuitable sites should be accessed such as pornographic sites, unless in the course of the agency's normal activities.
- No software should be downloaded without express permission of the network administrator. Downloaded software is one of the main sources of malicious software (Viruses and Trojan Horses).

AS/NZS 7799.2:20030	<i>A.8.5.1 A range of controls shall be implemented to achieve and maintain security in networks.</i>
----------------------------	--

AS/NZS 7799.2:2003	<i>A.9.4.1 Users shall only have direct access to the services that they are specifically authorised to use.</i>
---------------------------	---

AS/NZS 7799.2:2003	A.9.4.2 The path from the user terminal to the computer service shall be controlled.
---------------------------	---

AS/NZS 7799.2:2003	A.9.4.5 Access to diagnostic ports shall be securely controlled. Users shall only have direct access to the services that they are specifically authorised to use.
---------------------------	---

AS/NZS 7799.2:2003	A.9.4.6 Controls shall be introduced in networks to segregate groups of information services, users and information systems.
---------------------------	---

AS/NZS 7799.2:2003	A.9.4.7 The connection capability of users shall be restricted in shared networks in accordance with the access control policy specified in 4.7.1.1.
---------------------------	---

AS/NZS 7799.2:2003	A.9.4.8 Shared networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.
---------------------------	--

AS/NZS 7799.2:2003	A.9.4.9 A clear description of the security attributes of all network services used by the organisation shall be provided.
---------------------------	---

6.6 Operating System Access Control

To prevent unauthorised computer access, security facilities at the operating system level should be used to restrict access to computer resources. These facilities should be capable of:

- Identifying and verifying the identity, and if required, the location of the authorised users;
- Recording successful and failed system access attempts ;
- Providing authentication processes;
- Where appropriate, restricting the times of connection to users.

Typically the operating system controls who can use an application, have access to a directory or print to a specific printer etc. These operating system controls provide an initial line of defence identifying who is a legitimate user. Application Access controls ([see 7.1](#)) determine what functions within the application each user can perform.

6.6.1 IDENTIFICATION OF TERMINALS AND WORKSTATIONS

Terminal / workstation identification can be used to restrict access to an application or function to a specific terminal or group of terminals. Users are therefore restricted to a set of specific terminals for logging in to a specific function eg, only terminals in the Human Resources area can access the Personnel application.

AS/NZS 7799.2:2003	A.9.5.1 Automatic terminal identification shall be used to authenticate connections to specific locations and to portable equipment.
---------------------------	---

6.6.2 SECURE LOGON PROCEDURES

Logging into a terminal or workstation should be through a secure log on procedure. This procedure should minimise the risk of unauthorised access.

Typically a good log on procedure should:

- Not display any system or application identifiers or banners;
- Warn those logging in that unauthorised system access will be prosecuted;
- Not provide any help to the user logging in;
- Restricting unsuccessful logins to three before disabling the users account;
- Log all unsuccessful login attempts;
- Validate login information on completion of input;
- Enforce entry of password in a non-display mode;
- On completion of successful login advise date and time of last successful login and details of any unsuccessful logins attempts since last successful login.

AS/NZS 7799.2:2003 A.9.5.2 Access to information services shall use a secure log on process.

6.6.3 SYSTEM UTILITIES

The operating system will have utilities which can circumvent system and application controls. Use of these utilities should be restricted and controlled. Only authorised staff should have access to such utilities and their use must be authorised, monitored and logged. When not required, consideration should be given to removing them from the system.

AS/NZS 7799.2:2003 A.9.5.5 Use of system utility programs shall be restricted and tightly controlled.

6.6.4 DURESS ALARM

Users subject to outside influences or pressure may require the provision of a duress alarm. Procedures should be drawn up to define responsibilities for responding to a duress alarm.

AS/NZS 7799.2:2003 A.6.5.6 Duress alarms shall be provided for users who might be the target of coercion.

6.6.5 TIME RESTRICTION

Users should be restricted from connecting to the system outside of normal business hours unless authorised. Most system users would probably not require access before 7am or beyond 7pm Monday to Friday. Access for users who do require longer access should be provided after management approval has been obtained. This would be the case for users who need to work overtime or have a deadline to meet.

Limiting the time for user access narrows the window of opportunity for unauthorised access. Novell and Windows NT both provide the capability to restrict access times to networks.

AS/NZS 7799.2:2003	<i>A.9.5.8 Restrictions on connection times shall be used to provide additional security for high-risk applications.</i>
---------------------------	---

6.7 Application Access Control

6.7.1 APPLICATION ACCESS RESTRICTION

User access to applications should be restricted in accordance with the Access Control Policy defined (see [7.2](#)). Logical access to software and information should be restricted to authorised users. Application systems should control user access to information and application systems, provide protection from unauthorised access, not compromise the security of other systems with which information is shared and be able to provide access to information to the owner and to other nominated individuals or groups. Application access control should be integrated with the operating system access controls

As part the development process of in-house systems, standards should be put in place to require developers to make use of operating system access controls in the applications they build. Typically the operating system controls ([see 7.2](#)) who can use an application, have access to a directory or print to a specific printer etc. These operating system controls provide an initial line of defence identifying who is a legitimate user. Application access controls determine what functions within the application each user can perform. This provides an additional level of granularity and allows access to be defined to a lower level.

For example the Operating system can authenticate a user and determine that he is a member of the Finance group. The application controls can then determine that the user is authorised to access the Accounts Payable application and enter suppliers invoice details but not draw cheques.

AS/NZS 7799.2:2003	<i>A.9.6.1 Access to information and application system functions shall be restricted in accordance with the access control policy.</i>
---------------------------	--

6.7.2 ISOLATION OF SENSITIVE APPLICATIONS

Some applications may be considered so sensitive that they warrant running on a separate dedicated computer system. This sensitivity may be due to the confidential nature of the data being processed eg, Criminal records, medical records or due to financial sensitivity such as State Government budget papers.

Sensitive applications should:

- Be explicitly identified and documented;
- Where they are to be run within a shared environment the other applications running within the same shared environment should be identified and agreed with the owner of the sensitive application.

6.8 Audit Trails and Logs

The System should maintain an audit trail of events related to access control. Audit logs should be retained for an agreed period of time so that investigation of specific incidents can be pursued. Without appropriate audit records ICT is difficult to hold users accountable for their actions.

Some automated logs may be kept such as:

Console logs:

- Application Audit trails;
- Backup and Recovery logs.

Audit logs should include:

- Date and time of access;
- User ID;
- Terminal/workstation id and location;
- Success or failure of system access;
- Files accessed;
- Application functions accessed;
- Before and after images of any changes made for especially sensitive applications.

Audit logs should be routinely monitored. Unusual events should be identified and investigated for:

- Privileged access eg, supervisor or root access;
- Unauthorised access attempts;
- System alerts or failures.

The files containing audit trails should be protected by the operating system against alteration or deletion. ICT should be recognised that in some situations the System Supervisor can alter log files (Unix Root access). Audit trails should be implemented such that there can be no loss of records. If disk space is unavailable then the system should stop processing.

Audit trails should be archived regularly onto magnetic media and kept for as long as possible (minimum 12 months). Audit logs retained for a short period (a week or two) are unlikely to serve their purpose. Two archive copies of all logs should be kept one locally and one at the designated offsite backup.

events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

AS/NZS 7799.2:2003

A.9.7.2 Procedures for monitoring information processing facilities shall be established and the results of the monitoring reviewed regularly.

To ensure accuracy of audit log data, the computer system clocks should be synchronised. This is important especially when daylight saving changes occur, normally in late October and March.

AS/NZS 7799.2:2003

A.9.7.3 Computer clocks shall be synchronised for accurate recording.

7. Systems development and maintenance controls

7.1 Application Security

Application controls should be designed into systems to provide some assurance in respect of the accuracy and integrity of the data held. Even when developed to rigorous standards applications are still reliant on the quality of data to ensure the integrity of the processed results. Application controls must be developed to ensure:

- Completeness of input and processing;
- Accuracy of input and processing;
- Accuracy of output ;
- Validity of standing data.

AS/NZS 7799:2:2003	<i>A.10.1.1 Business requirements for new systems, or enhancements to existing systems shall specify the requirements for controls.</i>
---------------------------	--

AS/NZS 7799:2:2003	<i>A.10.5.2 Application systems shall be reviewed and tested when changes occur.</i>
---------------------------	---

Threats that need to be addressed include:

- Unauthorised data entry caused by lack of segregation of duties;
- Inconsistent entry of data;
- Incomplete entry of data;
- Tampering with stored data;
- Inadvertent corruption or destruction of data;
- Incomplete processing due to software faults, or equipment failures;
- Data corruption caused by equipment or media failure;
- Insertion of spurious data during transmission.

To address these threats the following controls can be implemented:

INPUT DATA VALIDATION CONTROLS

These controls are designed to detect the input of incomplete or inaccurate data.

- Batch totals eg, (8 documents in batch);
- Control totals eg, (\$200,000 worth of invoices in batch);
- Range checks eg, (postcodes between 1-9999);
- Check digits on important fields eg, (Tax File Numbers);
- Sequence checks eg, (invoice numbers should be consecutive);
- Consistency checks eg, (age must be > 15);
- Invalid characters eg, (numerics in an alpha field);
- Matching of data with master file eg, (customer doesn't exist on file);
- One for one checking of input with output report;
- Scanning of preprinted data eg, (bar codes).

PROCESSING CONTROLS

These controls are designed to detect errors in the completeness and accuracy of processing and in the update of a system. Controls that may be implemented include:

- Computer sequence check eg, (next transaction number).;
- One for one checking of output reports eg, (review output report against transactions entered);
- Batch controls to reconcile data file balances after transaction update;
- Balancing controls eg, (opening balance plus invoices posted, less payments posted equals closing balance);
- Data base integrity and consistency controls.

MESSAGE AUTHENTICATION

Agencies are referred to NSW Government Office of Information Technology guidelines [Authentication – Digital Signatures](#) issued in May 2002.

Message authentication is a method of ensuring the integrity of electronic messages. ICT provides:

- Authentication of the origin of a message;
- Authentication of the parties communicating the message;
- Non-repudiation;
- Assurance that the message content has not been altered.

Message authentication is achieved by sealing a message or by signing a message. Sealing a message involves the calculation of a cryptographic check sum known as a Message Authentication Code. Signing a message involves hashing the content and security label of a message and generating a digital signature by encrypting the message digest using the originators private key with an asymmetric algorithm. This process produces three keys:

- A shared secret key for sealing and verification;
- A private key used by the originator for signing;
- A public key for verification.

For non-repudiation there needs to be a trusted mechanism which binds the message sender's public key to their identity.

When NSW State Government Agencies are dealing with Commonwealth agencies they should be aware that the Defence Signals Directorate will only accept the following message authentication standards:

- CBC-MAC in accordance with AS 2805.4;

- DSA in accordance with the Digital Signatures Standards US FIPS PUB 186 and ANSI X9.30 (part 1), using SHA-1 hash function in accordance with US FIPS PUB 180-1 and ANSI X9.30 (part 2);
- RSA digital signature in accordance with AS 2805.5.3, using MD5 Message Digest algorithm in accordance with Internet RFC 1321.

(ACSI 33 Security Guideline for Australian Government ICT Systems December 2002)

Message authentication should be considered for applications where there is a security requirement to protect the integrity of the message content. This would apply to most electronic commerce transactions. Agencies should perform a risk assessment of their applications to determine if message authentication is required.

Agencies should also be aware of the requirements of the NSW “Electronic Transactions Act 2000” and the Commonwealth Government’s “Electronic Transactions Act 1999”. These Acts of Parliament (State and Federal) effectively validate the use of electronic transactions and signatures.

In summary, these acts state:

- A transaction is not invalid because ICT took place by means of one or more electronic communications;
- Validates the use of electronic forms where there is a requirement to:
 - give information in writing;
 - provide a signature;
 - produce a document;
 - retain a document.
- Provision is made for determining the time and place of the dispatch and receipt of electronic communication;
- Binds the purported originator of an electronic communication, only if the communication was sent by the purported originator or with the authority of the purported originator.

OUTPUT DATA CONTROLS

Output from application systems needs to be validated not only to ensure accuracy of processing but to ensure accuracy of the information being output or reported. Controls can be implemented to validate output. These include:

- Exception reports ie, reports which are run to highlight exceptional records, eg, Debtors that have exceeded their credit limits or have negative balances;
- One for one checking of reports to ensure accuracy of output;
- Control totals generated when transactions output from one system are interfaced to another system;
- Control reports used to reconcile detailed report totals.

AS/NZS 7799.2:2003	A.10.2.1 Data input to application systems shall be validated to ensure that ICT is correct and appropriate.
---------------------------	---

AS/NZS 7799.2:2003	A.10.2.2 Validation checks shall be incorporated into systems to detect corruption of the data processed.
---------------------------	--

AS/NZS 7799.2:2003	A.10.2.3 Message authentication shall be used for applications where there is a security requirement to protect the integrity of the message content.
---------------------------	--

AS/NZS 7799.2:2003	A.10.2.4 Data output from the application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
---------------------------	---

7.2 Cryptography

Cryptography is the art and science of keeping messages secure. Cryptography is a mathematical means of transforming data to provide security. Cryptography can be used to provide:

- Confidentiality;
- Integrity;
- Non-repudiation;
- Authentication.

When applying cryptographic techniques care should be taken to comply with the various legal requirements that may vary from country to country. The issue of key management must also be addressed.

CONFIDENTIALITY

Where confidentiality is an important requirement, encryption of data in files and over communication lines should be considered. Encryption is the use of a mathematical algorithm to scramble data. Decryption is the use of the same mathematical algorithm to unscramble the data. Encryption makes data unreadable to an unauthorised user, however use of a key allows authorised users to decrypt the data.

It is particularly useful in maintaining the confidentiality of emails where data is normally sent as clear text and is subject to eavesdropping and in the protection of confidential data held in files (eg, Tax File or passport numbers).

One of the most popular and secure methods of encryption is public/private key encryption. The private key can encrypt a message that only the corresponding public key can decrypt. Once the private/public keys are generated they remain associated with the person who generated the two keys.

When considering encryption account should be taken of :

Relevant government laws and regulations;
The requirements of key management;
The suitability of the encryption mechanisms used for deployment.

DATA INTEGRITY

In circumstances where integrity of data is important, hash functions, digital signatures and integrity controls should be considered. Integrity Controls such as Message Authentication Codes (MACS, see 8.1), provide protection against accidental or deliberate alteration, addition or deletion of a message. Digital Signatures can check whether the contents of a document have been changed.

NON-REPUDIATION

When an electronic transaction is sent by the originator and the other parties act on that transaction, a method is required to stop the originator repudiating or denying that he sent the transaction. Non-repudiation is the process of assuring that the originator sent the message. Use of Digital signatures can provide this non-repudiation capability.

A digital signature is an electronic method of signing an electronic document that is reliable, convenient and secure. The most widely used method of digital signature relies on Public/private key encryption. Digital signatures are not digital representations or images of a person's signature but a message that has been encrypted using a private key and decrypted using a corresponding public key. ICT authenticates the document because the document could only have been enciphered using the private key, securely held by its owner, which assures everyone that the message could only have come from the owner. Use of a Certification Authority, a trusted organisation that issues digital certificates to end entities and other Certification authorities, can also resolve repudiation disputes.

Care should be taken to maintain the confidentiality of private keys as these can be used to sign documents. The legal status of digital signatures has recently been clarified by the NSW "Electronic Transactions Act 2000" and the Commonwealth Government's "Electronic Transactions Act 1999". Agencies must refer to these Acts.

Agencies are referred to NSW Government Office of Information Technology guidelines [Authentication – Digital Signatures](#) issued May 2002 for a more in depth discussion on Digital Signatures.

DATA AUTHENTICITY

Digital signatures provide proof of authenticity and of the validity of data and messages.

KEY MANAGEMENT

Key Management includes the technical, organisational and procedural aspects that are required to support the use of Cryptography. The main objective of key management is the secure administration and management of cryptographic keys and related information. Key management includes the generation, registration, certification, de-registration, distribution, installation, storage, archiving, revocation, derivation and destruction of keys. Any compromise or loss of cryptographic keys could compromise the confidentiality, integrity or authenticity of information. Equipment used to generate, store and archive keys should be physically protected.

AS/NZS 7799.2:2003	<i>A.10.3.1 A policy on the use of cryptographic controls for the protection of information shall be developed and followed.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.10.3.2 Encryption shall be applied to protect the confidentiality of sensitive or critical information.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.10.3.3 Digital signatures shall be applied to protect the authenticity and integrity of electronic information.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.10.3.4 Non repudiation services shall be used to resolve disputes about occurrence or non occurrence of an event or action.</i>
---------------------------	---

AS/NZS 7799.2:2003	<i>A.10.3.5 A key management system based on agreed standards, procedures and methods shall be used to support the use of cryptographic techniques.</i>
---------------------------	--

7.3 Restrictions to Software Package Modifications

Changes to software packages should be discouraged. One of the benefits of using software packages is that in-house staff are not required to support application software. Modifications to packaged software should therefore be kept to a minimum and where required performed in compliance with established configuration management standards.

AS/NZS 7799.2:2003	<i>A.10.5.3 Modifications to software packages shall be discouraged and essential changes strictly controlled.</i>
---------------------------	---

APPENDIX 1: CLASSIFICATION OF CONTROLS

This list classifies the controls by control types and references the controls to the relevant clauses in AS/NZS 7799.2:2003. This Appendix should be used as a guide only.

SECTION	Reference to AS/NZS 7799.2:2003 Annex A	Control Type				
		Pro- tect	Deter	De- tect	Res- pond	Re- cover
3. ORGANISATIONAL AND MANAGEMENT CONTROLS						
3.1 INFORMATION SECURITY POLICY	3.1	✓				
3.2 INFORMATION SECURITY INFRASTRUCTURE	4.1	✓				
SPECIALIST INFORMATION SECURITY ADVICE	4. 1.5	✓			✓	
CO-OPERATION BETWEEN ORGANISATIONS	4. 1.6	✓		✓	✓	
INDEPENDENT REVIEW OF INFORMATION SECURITY	4. 1.7	✓	✓	✓	✓	
3.3 SECURITY OF THIRD PARTY ACCESS	4.2	✓	✓			
3.4 OUTSOURCING	4. 3	✓	✓			
3.5 MOBILE COMPUTING	9.8.1	✓				
3.6 TELEWORKING	9.8.2	✓				
3.7 ASSET CLASSIFICATION AND CONTROL	5.1, 5.2	✓	✓			
CLASSIFICATION GUIDELINES	5.2.1	✓				
INFORMATION LABELLING AND HANDLING	5.2.2	✓	✓	✓		
3.8 PERSONNEL PRACTICES						
3.8.1 JOB DESCRIPTIONS	6.1.1	✓	✓			
3.8.2 SEGREGATION OF DUTIES	8.1.4	✓	✓			
3.8.3 RECRUITMENT	6.1.2	✓	✓			
3.8.4 TERMS AND CONDITIONS OF EMPLOYMENT	6.1.3, 6.1.4	✓	✓			
3.8.5 MONITORING OF PERSONNEL	-			✓		
3.8.6 TERMINATIONS AND JOB CHANGES	-	✓				
3.9 SECURITY AWARENESS AND TRAINING	6.2.1	✓	✓			
3.10 COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENTS	12.1	✓				
IDENTIFICATION OF APPLICABLE LEGISLATION	12.1.1	✓				
INTELLECTUAL PROPERTY RIGHTS (IPR)	12.1.2	✓				
SAFEGUARDING OF ORGANISATIONAL RECORDS	12.1.3	✓			✓	✓
DATA PROTECTION AND PRIVACY OF PERSONAL INFORMATION	12.1.4	✓				
PREVENTION OF MISUSE OF INFORMATION PROCESSING FACILITIES	12.1.5	✓	✓			

SECTION	Reference to AS/NZS 7799.2:2003 Annex A	Control Type				
		Pro- tect	Deter	De- tect	Res- pond	Re- cover
REGULATION OF CRYPTOGRAPHIC CONTROLS	12.1.6	✓				
COLLECTION OF EVIDENCE	12.1.7	✓	✓		✓	
3.11 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS	12.2		✓	✓		
3.12 INCIDENT HANDLING	6.3.1 to 6.3.4				✓	
3.13 DISCIPLINARY PROCESS	6.3.5		✓			
3.14 BUSINESS CONTINUITY MANAGEMENT	11.1, 8.4.1	✓			✓	✓
3.15 SYSTEM AUDITS						
3.15.1 AUDITS OF OPERATIONAL SYSTEMS	12.3.1		✓	✓		
3.15.2 SYSTEM AUDIT TOOLS	12.3.2	✓		✓		
4. PHYSICAL AND ENVIRONMENTAL CONTROLS						
4.1 SECURE AREAS	7.1	✓				
PHYSICAL SECURITY PERIMETER	7.1.1	✓	✓			
PHYSICAL ENTRY CONTROLS	7.1.2	✓	✓	✓		
SECURING OFFICES, ROOMS AND FACILITIES	7.1.3	✓	✓	✓		
WORKING IN SECURE AREAS	7.1.4	✓	✓			
ISOLATED DELIVERY AND LOADING AREAS	7.1.5	✓	✓			
4.2 EQUIPMENT SECURITY	7.2	✓				
EQUIPMENT SITING AND PROTECTION	7.2.1	✓		✓		
POWER SUPPLIES	7.2.2	✓			✓	✓
CABLING SECURITY	7.2.3	✓				
EQUIPMENT MAINTENANCE	7.2.4	✓		✓		
SECURITY OF EQUIPMENT OFF-PREMISES	7.2.5	✓				
SECURITY DISPOSAL OR RE-USE OF EQUIPMENT	7.2.6	✓	✓			
4.3 CLEAR DESK AND SCREEN POLICY	7.3.1	✓	✓			
4.4 REMOVAL OF PROPERTY	7.3.2		✓	✓		
5. OPERATIONAL CONTROLS						
5.1 DOCUMENTATION	8.1.1	✓			✓	✓
5.2 CONFIGURATION AND CHANGE MANAGEMENT	8.1.2	✓	✓			
5.3 INCIDENT MANAGEMENT	8.1.3		✓		✓	✓
5.4 SOFTWARE DEVELOPMENT AND TEST ENVIRONMENT	8.1.5	✓	✓			
5.5 OUTSOURCED FACILITIES	8.1.6	✓				
5.6 SYSTEMS PLANNING	8.2.1	✓				

SECTION	Reference to AS/NZS 7799.2:2003 Annex A	Control Type				
		Protect	Deter	Detect	Respond	Recover
5.7 SYSTEMS AND ACCEPTANCE TESTING	8.2.2, 10.4.2	✓		✓		
5.8 PROTECTION AGAINST MALICIOUS CODE	8.3.1, 10.5.4	✓	✓	✓	✓	✓
5.9 DATA BACKUP	8.4.1	✓				✓
5.10 LOGGING	8.4.2, 8.4.3		✓	✓		
5.11 SOFTWARE AND INFORMATION EXCHANGE	8.7.1	✓				
5.12 SECURITY OF MEDIA IN TRANSIT	8.7.2	✓				
5.13 ELECTRONIC COMMERCE SECURITY	8.7.3	✓	✓			
5.13.1 ELECTRONIC DATA INTERCHANGE(EDI)		✓	✓			
5.13.2 INTERNET COMMERCE		✓	✓			
5.14 ELECTRONIC MAIL SECURITY	8.7.4	✓	✓			
5.15 ELECTRONIC OFFICE SYSTEMS	8.7.5, 8.7.7	✓	✓			✓
5.16 ELECTRONIC PUBLISHING	8.7.6	✓				
5.17 MEDIA	8.6	✓				✓
6. TECHNICAL CONTROLS		✓				
6.1 IDENTIFICATION AND AUTHENTICATION	9.3.1, 9.4.3, 9.4.4, 9.5.3 9.5.4	✓	✓			
6.1.1 PASSWORDS	9.2.3, 9.3.1, 9.4.3, 9.5.4	✓	✓			
6.1.2 TOKENS	9.4.3	✓	✓			
6.1.3 BIOMETRIC DEVICES	9.4.3	✓	✓			
6.2 LOGICAL ACCESS	9.1.1, 9.2.1, 9.2.2, 9.2.3	✓	✓			
6.3 REVIEW OF ACCESS RIGHTS	9.2.4	✓	✓	✓		
6.4 UNATTENDED USER HARDWARE	9.3.2, 9.5.7	✓	✓			
6.5 NETWORK MANAGEMENT	9.5.1, 9.4.1,					
6.5.1 OPERATIONAL PROCEDURES	9.4.1, 9.4.5	✓				
6.5.2 PREDEFINED USER ACCESS PATHS	9.4.2	✓	✓			
6.5.3 DIAL IN ACCESS CONTROLS	9.4.3	✓	✓			
6.5.4 NETWORK PLANNING	8.5.1	✓				
6.5.5 NETWORK CONFIGURATION	8.5.1	✓				
6.5.6 SEGREGATION OF NETWORKS	9.4.6	✓	✓			
6.5.7 MONITORING OF NETWORK	8.5.1		✓	✓		
6.5.8 INTRUSION DETECTION	9.4.8		✓	✓		
6.5.9 INTERNET CONNECTION POLICIES	9.4.1, 9.4.7	✓	✓			
6.6 OPERATING SYSTEM ACCESS CONTROL						

SECTION	Reference to AS/NZS 7799.2:2003 Annex A	Control Type				
		Protect	Deter	Detect	Respond	Recover
6.6.1	AUTOMATIC IDENTIFICATION OF TERMINALS AND WORKSTATIONS			✓		
6.6.2	SECURE LOGON PROCEDURES	✓	✓			
6.6.3	USE OF SYSTEM UTILITIES	✓				
6.6.4	DURESS ALARM	✓	✓		✓	
6.6.5	TIME RESTRICTION		✓			
6.7	APPLICATION ACCESS CONTROL					
6.7.1	APPLICATION ACCESS RESTRICTION	✓	✓			
6.7.2	ISOLATION OF SENSITIVE APPLICATIONS	✓	✓			
6.8	AUDIT TRAILS AND LOGS			✓		
7.	SYSTEMS DEVELOPMENT AND MAINTENANCE CONTROLS					
7.1	APPLICATION SECURITY	✓	✓			
7.2	CRYPTOGRAPHY	✓	✓	✓		
7.3	RESTRICTIONS TO SOFTWARE PACKAGE MODIFICATIONS	✓		✓		

APPENDIX 2: CONTROL TOPICS BY SECURITY CONCERN

This list shows control topics that addresses the security concerns and the relevant references to clauses in AS/NZS 4444.2:2000. This Appendix should be used as a guide only.

SECTION	Reference to AS/NZS 7799.2:2003 Annex A	Security Concern					
		Confidentiality	Integrity	Availability	Accountability	Authenticity	Reliability
3. ORGANISATIONAL AND MANAGEMENT CONTROLS							
3.1 INFORMATION SECURITY POLICY	3.1	✓	✓	✓	✓		
3.2 INFORMATION SECURITY INFRASTRUCTURE	4.1	✓	✓	✓	✓		
SPECIALIST INFORMATION SECURITY ADVICE	4.1.5						
CO-OPERATION BETWEEN ORGANISATIONS	4.1.6						
INDEPENDENT REVIEW OF INFORMATION SECURITY	4.1.7						
3.3 SECURITY OF THIRD PARTY ACCESS	4.2	✓	✓	✓	✓		✓
3.4 OUTSOURCING	4.3	✓	✓	✓	✓		✓
3.5 MOBILE COMPUTING	9.8.1	✓					
3.6 TELEWORKING	9.8.2						
3.7 ASSET CLASSIFICATION AND CONTROL	5.1	✓	✓	✓	✓		
CLASSIFICATION GUIDELINES	5.2.1						
INFORMATION LABELLING AND HANDLING	5.2.2						
3.8 PERSONNEL PRACTICES							
3.8.1 JOB DESCRIPTIONS	6.1.1	✓	✓	✓	✓		
3.8.2 SEGREGATION OF DUTIES			✓				
3.8.3 RECRUITMENT	6.1.2	✓	✓	✓			
3.8.4 TERMS AND CONDITIONS OF EMPLOYMENT	6.1.3, 6.1.4	✓	✓	✓	✓		
3.8.5 MONITORING OF PERSONNEL		✓	✓	✓	✓		
3.8.6 TERMINATIONS AND JOB CHANGES		✓	✓	✓			
3.9 SECURITY AWARENESS AND TRAINING	6.2.1	✓	✓	✓	✓		
3.10 COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENTS	12.1						
IDENTIFICATION OF APPLICABLE LEGISLATION	12.1.1	✓	✓	✓			

SECTION	Reference to AS/NZS 7799.2:2003 Annex A	Security Concern					
		Confidentiality	Integrity	Availability	Accountability	Authenticity	Reliability
INTELLECTUAL PROPERTY RIGHTS (IPR)	12.1.2	✓					
SAFEGUARDING OF ORGANISATIONAL RECORDS	12.1.3		✓	✓	✓	✓	
DATA PROTECTION AND PRIVACY OF PERSONAL INFORMATION	12.1.4	✓	✓				
PREVENTION OF MISUSE OF INFORMATION PROCESSING FACILITIES	12.1.5		✓	✓			✓
REGULATION OF CRYPTOGRAPHIC CONTROLS	12.1.6		✓				
COLLECTION OF EVIDENCE	12.1.7		✓		✓	✓	
3.11 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS	12.2	✓	✓	✓	✓		
3.12 INCIDENT HANDLING	6.3.1 to 6.3.4	✓	✓	✓			
3.13 DISCIPLINARY PROCESS	6.3.5	✓	✓	✓			
3.14 BUSINESS CONTINUITY MANAGEMENT	11.1			✓			✓
3.15 SYSTEM AUDITS							
3.15.1 AUDITS OF OPERATIONAL SYSTEMS	12.3.1		✓				✓
3.15.2 SYSTEM AUDIT TOOLS	12.3.2		✓				✓
4. PHYSICAL AND ENVIRONMENTAL CONTROLS							
4.1 SECURE AREAS	7.1	✓	✓	✓			
PHYSICAL SECURITY PERIMETER	7.1.1	✓	✓	✓			
PHYSICAL ENTRY CONTROLS	7.1.2	✓	✓	✓		✓	
SECURING OFFICES, ROOMS AND FACILITIES	7.1.3	✓	✓	✓			
WORKING IN SECURE AREAS	7.1.4	✓	✓	✓			
ISOLATED DELIVERY AND LOADING AREAS	7.1.5	✓	✓	✓			
4.2 EQUIPMENT SECURITY	7.2						
EQUIPMENT SITING AND PROTECTION	7.2.1	✓		✓			✓
POWER SUPPLIES	7.2.2			✓			✓
CABLING SECURITY	7.2.3	✓	✓	✓			✓
EQUIPMENT MAINTENANCE	4.5.2.4		✓	✓			✓
SECURITY OF EQUIPMENT OFF-PREMISES	7.2.5	✓	✓	✓			
SECURITY DISPOSAL OR RE-USE OF EQUIPMENT	7.2.6	✓					
4.3 CLEAR DESK AND SCREEN POLICY	7.3.1						
4.4 REMOVAL OF PROPERTY	7.3.2						

SECTION	Reference to AS/NZS 7799.2:2003 Annex A	Security Concern					
		Confidentiality	Integrity	Availability	Accountability	Authenticity	Reliability
5. OPERATIONAL CONTROLS							
5.1 DOCUMENTATION	8.1.1		✓		✓		
5.2 CONFIGURATION AND CHANGE MANAGEMENT	8.1.2		✓		✓		✓
5.3 INCIDENT MANAGEMENT	8.1.3	✓	✓	✓			
5.4 SOFTWARE DEVELOPMENT AND TEST ENVIRONMENT	8.1.5	✓	✓	✓	✓		✓
5.5 OUTSOURCED FACILITIES	8.1.6	✓	✓	✓			
5.6 SYSTEMS PLANNING	8.2		✓	✓			✓
5.7 SYSTEMS AND ACCEPTANCE TESTING	8.2		✓	✓			✓
5.8 PROTECTION AGAINST MALICIOUS CODE	8.3.1	✓	✓	✓			
5.9 DATA BACKUP	8.4.1		✓	✓			
5.10 LOGGING	8.4.2, 8.4.3			✓	✓		
5.11 SOFTWARE AND INFORMATION EXCHANGE	8.7.1	✓	✓	✓	✓		
5.12 SECURITY OF MEDIA IN TRANSIT	8.7.2	✓	✓	✓			✓
5.13 ELECTRONIC COMMERCE SECURITY	8.7.3	✓	✓			✓	
5.13.1 ELECTRONIC DATA INTERCHANGE(EDI)	-	✓	✓			✓	
5.13.2 INTERNET COMMERCE	-	✓	✓			✓	
5.14 ELECTRONIC MAIL SECURITY	4.6.7.4	✓	✓			✓	
5.15 ELECTRONIC OFFICE SYSTEMS	8.7.5	✓		✓			
5.16 ELECTRONIC PUBLISHING	8.7.6	✓	✓				
5.17 MEDIA HANDLING AND SECURITY	8.6	✓	✓	✓			
6. TECHNICAL CONTROLS							
6.1 IDENTIFICATION AND AUTHENTICATION	9.3.1, 9.4.3, 9.4.4, 9.5.3, 9.5.4	✓	✓	✓	✓	✓	
6.1.1 PASSWORDS	9.2.3, 9.3.1, 9.4.3, 9.5.4	✓	✓		✓	✓	
6.1.2 TOKENS	9.4.3	✓	✓		✓	✓	
6.1.3 BIOMETRIC DEVICES	9.4.3	✓	✓		✓	✓	
6.2 LOGICAL ACCESS	9.1.1, 9.2.1, 9.2.2, 9.2.3	✓	✓	✓	✓		
6.3 REVIEW OF ACCESS RIGHTS	9.2.4.	✓	✓	✓	✓		
6.4 UNATTENDED USER HARDWARE	9.3.2. 9.5.7.	✓	✓	✓			

SECTION	Reference to AS/NZS 7799.2:2003 Annex A	Security Concern						
		Confidentiality	Integrity	Availability	Accountability	Authenticity	Reliability	
6.5	NETWORK MANAGEMENT	-						
6.5.1	OPERATIONAL PROCEDURES	8.5.1, 9.4.1	✓	✓	✓			
6.5.2	PREDEFINED USER ACCESS PATHS	9.4.2	✓	✓				
6.5.3	DIAL IN ACCESS CONTROLS	9.4.3		✓			✓	
6.5.4	NETWORK PLANNING	8.5.1			✓			✓
6.5.5	NETWORK CONFIGURATION	8.5.1			✓			✓
6.5.6	SEGREGATION OF NETWORKS	9.4.6	✓	✓				
6.5.7	MONITORING OF NETWORK	8.5.1				✓		
6.5.8	INTRUSION DETECTION	9.4.8		✓				
6.5.9	INTERNET CONNECTION POLICIES	9.4.1, 9.4.7	✓	✓				
6.6	OPERATING SYSTEM ACCESS CONTROL							
6.6.1	AUTOMATIC IDENTIFICATION OF TERMINALS AND WORKSTATIONS	9.5.1	✓	✓		✓	✓	
6.6.2	SECURE LOGON PROCEDURES	9.5.2	✓	✓				
6.6.3	USE OF SYSTEM UTILITIES	9.5.5	✓	✓			✓	
6.6.4	DURESS ALARM	9.5.6	✓	✓	✓			
6.6.5	TIME RESTRICTION	9.5.8	✓	✓	✓			
6.7	APPLICATION ACCESS CONTROL							
6.7.1	APPLICATION ACCESS RESTRICTION	9.6.1	✓	✓				
6.7.2	ISOLATION OF SENSITIVE APPLICATIONS	9.6.2	✓	✓				
6.8	AUDIT TRAILS AND LOGS	9.7.1, 9.7.2, 9.7.3	✓	✓		✓		
7.	SYSTEMS DEVELOPMENT AND MAINTENANCE CONTROLS							
7.1	APPLICATION SECURITY	10.2.1, 10.2.2, 10.2.3, 10.2.4	✓	✓				
7.2	CRYPTOGRAPHY	10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5	✓	✓			✓	
7.3	RESTRICTIONS TO SOFTWARE PACKAGE MODIFICATIONS	10.5.3		✓				✓

APPENDIX 3: EXAMPLES OF THREATS AND MITIGATING CONTROLS

This list shows examples of threats and the controls that may mitigate these threats.

Controls	Threat									
	Fire	Denial of Service	Malicious Code	Malicious Destruction of Data & Facilities	Masquerade	Theft & Fraud	Web Site Intrusion	Failure of Communication Services	Loss of Key Personnel	Operational Staff or User Error
3. ORGANISATIONAL AND MANAGEMENT CONTROLS										
3.1 INFORMATION SECURITY POLICY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.2 INFORMATION SECURITY INFRASTRUCTURE			✓							
SPECIALIST INFORMATION SECURITY ADVICE			✓							
CO-OPERATION BETWEEN ORGANISATIONS			✓							
INDEPENDENT REVIEW OF INFORMATION SECURITY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.3 SECURITY OF THIRD PARTY ACCESS		✓		✓		✓				
3.4 OUTSOURCING							✓		✓	
3.5 MOBILE COMPUTING						✓				
3.6 TELEWORKING				✓	✓	✓				
3.7 ASSET CLASSIFICATION AND CONTROL	✓		✓	✓		✓		✓		✓
CLASSIFICATION GUIDELINES										
INFORMATION LABELLING AND HANDLING										
3.8 PERSONNEL PRACTICES										
3.8.1 JOB DESCRIPTIONS						✓				
3.8.2 SEGREGATION OF DUTIES						✓				
3.8.3 RECRUITMENT						✓				
3.8.4 TERMS AND CONDITIONS OF EMPLOYMENT						✓				

Controls		Threat									
		Fire	Denial of Service	Malicious Code	Malicious Destruction of Data & Facilities	Masquerade	Theft & Fraud	Web Site Intrusion	Failure of Communication Services	Loss of Key Personnel	Operational Staff or User Error
3.8.5	MONITORING OF PERSONNEL	✓		✓	✓		✓			✓	✓
3.8.6	TERMINATIONS AND JOB CHANGES						✓				
3.9	SECURITY AWARENESS AND TRAINING	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.10	COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENTS										
	IDENTIFICATION OF APPLICABLE LEGISLATION	✓									
	INTELLECTUAL PROPERTY RIGHTS (IPR)										
	SAFEGUARDING OF ORGANISATIONAL RECORDS			✓	✓		✓				
	DATA PROTECTION AND PRIVACY OF PERSONAL INFORMATION										
	PREVENTION OF MISUSE OF INFORMATION PROCESSING FACILITIES										
	REGULATION OF CRYPTOGRAPHIC CONTROLS				✓						
	COLLECTION OF EVIDENCE		✓	✓	✓	✓	✓	✓			
3.11	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.12	INCIDENT HANDLING			✓							✓
3.13	DISCIPLINARY PROCESS			✓	✓		✓				
3.14	BUSINESS CONTINUITY MANAGEMENT	✓	✓	✓	✓		✓		✓		✓
3.15	SYSTEM AUDITS										
3.15.1	AUDITS OF OPERATIONAL SYSTEMS				✓		✓				✓
3.15.2	SYSTEM AUDIT TOOLS						✓				✓
4.	PHYSICAL AND ENVIRONMENTAL CONTROLS										

Controls	Threat									
	Fire	Denial of Service	Malicious Code	Malicious Destruction of Data & Facilities	Masquerade	Theft & Fraud	Web Site Intrusion	Failure of Communication Services	Loss of Key Personnel	Operational Staff or User Error
4.1	SECURE AREAS									
	✓			✓		✓		✓		
	✓			✓		✓		✓		
	✓			✓		✓		✓		
				✓		✓			✓	
				✓		✓				
4.2	EQUIPMENT SECURITY									
	✓			✓	✓	✓		✓		
	✓			✓						
				✓				✓		
	✓									
				✓		✓				
						✓				
4.3				✓	✓	✓				
4.4						✓				
5.	OPERATIONAL CONTROLS									
5.1				✓					✓	✓
5.2			✓	✓						
5.3			✓							✓
5.4				✓						✓
5.5										
5.6			✓					✓		
5.7			✓					✓		
5.8		✓	✓	✓						
5.9	✓		✓	✓	✓			✓		✓

Controls		Threat									
		Fire	Denial of Service	Malicious Code	Malicious Destruction of Data & Facilities	Masquerade	Theft & Fraud	Web Site Intrusion	Failure of Communication Services	Loss of Key Personnel	Operational Staff or User Error
5.10	LOGGING							✓			✓
5.11	SOFTWARE AND INFORMATION EXCHANGE						✓				
5.12	SECURITY OF MEDIA IN TRANSIT			✓	✓		✓				
5.13	ELECTRONIC COMMERCE SECURITY										
5.13.1	ELECTRONIC DATA INTERCHANGE(EDI)						✓				
5.13.2	INTERNET COMMERCE						✓	✓			
5.14	ELECTRONIC MAIL SECURITY		✓	✓	✓						✓
5.15	ELECTRONIC OFFICE SYSTEMS										✓
5.16	ELECTRONIC PUBLISHING							✓			
5.17	MEDIA HANDLING AND SECURITY				✓		✓				✓
6.	TECHNICAL CONTROLS										
6.1	IDENTIFICATION AND AUTHENTICATION			✓	✓	✓	✓				
6.1.1	PASSWORDS			✓		✓		✓			
6.1.2	TOKENS					✓		✓			
6.1.3	BIOMETRIC DEVICES					✓		✓			
6.2	LOGICAL ACCESS			✓	✓	✓					
6.3	REVIEW OF ACCESS RIGHTS			✓	✓	✓					
6.4	UNATTENDED USER HARDWARE			✓	✓	✓	✓				
6.5	NETWORK MANAGEMENT										
6.5.1	OPERATIONAL PROCEDURES					✓		✓	✓	✓	✓
6.5.2	PREDEFINED USER ACCESS PATHS			✓	✓	✓					
6.5.3	DIAL IN ACCESS CONTROLS		✓	✓	✓	✓		✓			
6.5.4	NETWORK PLANNING							✓		✓	
6.5.5	NETWORK CONFIGURATION							✓		✓	
6.5.6	SEGREGATION OF NETWORKS		✓	✓	✓	✓		✓	✓		✓

Controls		Threat									
		Fire	Denial of Service	Malicious Code	Malicious Destruction of Data & Facilities	Masquerade	Theft & Fraud	Web Site Intrusion	Failure of Communication Services	Loss of Key Personnel	Operational Staff or User Error
6.5.7	MONITORING OF NETWORK		✓	✓	✓	✓		✓	✓		✓
6.5.8	INTRUSION DETECTION		✓	✓	✓	✓		✓	✓		
6.5.9	INTERNET CONNECTION POLICIES		✓	✓	✓	✓					✓
6.6	OPERATING SYSTEM ACCESS CONTROL										
6.6.1	AUTOMATIC IDENTIFICATION OF TERMINALS AND WORKSTATIONS			✓	✓	✓	✓				
6.6.2	SECURE LOGON PROCEDURES			✓	✓	✓	✓				
6.6.3	USE OF SYSTEM UTILITIES			✓	✓	✓	✓				
6.6.4	DURESS ALARM				✓		✓			✓	
6.6.5	TIME RESTRICTION			✓	✓	✓	✓				
6.7	APPLICATION ACCESS CONTROL										
6.7.1	APPLICATION ACCESS RESTRICTION			✓	✓	✓	✓				✓
6.7.2	ISOLATION OF SENSITIVE APPLICATIONS			✓	✓	✓	✓				✓
6.8	AUDIT TRAILS AND LOGS			✓	✓	✓	✓				✓
7.	SYSTEMS DEVELOPMENT AND MAINTENANCE CONTROLS										
7.1	APPLICATION SECURITY			✓		✓	✓	✓			✓
7.2	CRYPTOGRAPHY				✓	✓	✓	✓			
7.3	RESTRICTIONS TO SOFTWARE PACKAGE MODIFICATIONS			✓	✓		✓	✓			

APPENDIX 4: REFERENCES

Handbook on Information Security Risk Management (HB 231:2000), Standards Australia.

Organisational experiences in implementing information security management systems (HB 246:2001), Standards Australia.

Standard on Information Security Management Parts 1 and 2 (ISO/IEC.AS/NZS 17799.1:2001 and AS/NZS 7799.2:2003).

ICT Threat Identification and Risk Assessment – A Framework for Agencies in the New South Wales Government – 1997.

Australian Communications-Electronic Security Instruction 33 (ACSI-33)-Security Guideline for Australian Government ICT Systems, Defence Signals Directorate, December 2000.

Commonwealth Protective Security Manual, Attorney General's Department, 2000.

Information Technology - Guidelines for the Management of ICT Security – Parts 1 to 5 (ISO/IEC TR 13335-1, 13335-2, 13335-3, 13335-4, 13335-5).

ICT Baseline Protection Manual, German Information Security Agency, June 1998.

National Institute of Standards and Technology (NIST) Special Publication 800-18, Guide For Developing Security Plans For Information Technology Systems, December 1998.

Defending Your Digital Assets by Randall K. Nichols, Daniel J. Ryan, Julie J. C. H. Ryan, McGraw-Hill, 2000.

Hacking Exposed by Stuart McClure, Joel Scambray, George Kurtz, Osborne/McGraw-Hill, 1999.