Tasmanian Government Information Security Framework

Tasmanian Government Information Security Guidelines

Version 4.1 – 13 July 2009

Department of Premier and Cabinet
Inter Agency Policy And Projects Unit

Tasmania
Explore the possibilities

CONTENTS

1 Introduction 1

1.1 Authority 1
1.2 Overview of the Information Security Framework 1
1.3 Framework governance roles and responsibilities 2
1.4 Information Security Guidelines overview 3
1.5 Using the guidelines 4
1.6 Whole-of-government implementations of the Framework 5

2 Information Security Governance Guidelines 7

2.1 Purpose 7
2.2 Governance Policy 7
2.3 Guidelines for implementing the Governance Policy 7

3 Record Security Guidelines 10

3.1 Purpose 10
3.2 Record Security Policy 10
3.3 Guidelines for implementing the Record Security Policy 10

4 Physical Security Guidelines 16

4.1 Purpose 16
4.2 Physical Security Policy 16
4.3 Guidelines for implementing the Physical Security Policy 16
4.4 Acknowledgment 23

5 Personnel Security Guidelines 24

5.1 Purpose 24
5.2 Personnel Policy 24
5.3 Guidelines for implementing the Personnel Security Policy 24

6 General ICT Guidelines 26

6.1 Purpose 26
6.2 General ICT Policy 26
6.3 Guidelines for Implementing the General ICT Policy 26

7 Incident Management Guidelines 29

7.1 Purpose 29
7.2 Incident Reporting Policy 29
7.3 Guidelines for implementing the Incident Management Policy 29
7.4 Information Security Incident Classification 32

8 Risk Management Guidelines 34

8.1 Purpose 34
8.2 Risk Management Policy Principles 34
8.3 Guidelines for implementing the Risk Management Policy Principles 34

9 References 36

9.1 Security planning, policies & governance 36
9.2 Risk management 36
9.3 General ICT 37
9.4 Record security 39
9.5 Incident reporting 39

10 Document revision history 40

11 Appendices 43

Appendix 1 : Glossary of terms 44

Appendix 2 : Agency obligations under the Archives Act 1983 46

Appendix 3 : State Service Principles 47

Appendix 4 : State Service Code of Conduct 48

Appendix 5 : Information security risk management methodology 49

Appendix 6 : Example information security risk register 57

1 Introduction

This section contains an overview of the *Tasmanian Government Information Security Framework* (the Framework) including the governance of the Framework and the nature of its components.

1.1 Authority

Cabinet approved the *Tasmanian Government Information Security Charter* (the Charter) in May 2003. The Charter outlines information security principles and policies that are to be applied by agencies to achieve appropriate information security within the Tasmanian Government.

1.2 Overview of the Information Security Framework

The Charter, together with The Tasmanian Government Information Security Guidelines (the Guidelines) forms the Framework.

The Charter establishes:

- Information Security Policy Principles that agencies are to adhere to
- Information Security Policies that agencies are to adhere to
- Important legislative requirements
- Primary roles and responsibilities for information security

Heads of agencies are to implement the Charter using the Framework as a guide. The Charter is available from http://www.egovernment.tas.gov.au/.

The Framework uses a risk based approach to implement appropriate levels of information security. Risk assessment and management methodology guidelines are integral to the framework.

The Guidelines point agencies to procedures when implementing the policies and principles of the Charter. The Guidelines draw upon recognised standards where applicable.

The Framework components and the documents are summarised in the diagrams below.

Tasmanian Government Information Security Framework Components				
Principles	Information Security Charter		Whole-of-government implementations of the Framework	Agency implementations of the Framework
Policies				
Procedures	Information Security Guidelines			
Standards				

Tasmanian Government Information Security Framework Documents	
Document Name	**Contents Outline**
Tasmanian Government Information Security Charter	• Legislative requirements • Information security policy principles • Information security policies • Primary roles and responsibilities
Tasmanian Government Information Security Guidelines	• Overview of the Tasmanian Government Information Security Framework • Information security governance • Record security • Physical security • Personnel security • General ICT • Incident management • Information security risk management
Tasmanian Government WAN and Internet Services: Information Security Policies and Standards	A whole-of-government implementation of the framework with polices and standards specific to this topic.
Agency implementations of the Framework	Determined by each agency.

1.3 Framework governance roles and responsibilities

The Charter includes a section on the roles and responsibilities for information security and is expanded upon in this section.

1.3.1 Secretary of the Department of Premier and Cabinet and the Inter Agency Steering Committee

The Inter Agency Steering Committee (IASC) is to oversight and provide guidance to the Secretary of the Department of Premier and Cabinet, who has prime responsibility for the development and maintenance of the Framework.

1.3.2 Inter Agency Policy and Projects Unit

The Inter Agency Policy and Projects Unit (IAPPU) of the Department of Premier and Cabinet is to:

- Maintain the whole-of-government information security charter, policies, standards and guidelines
- Develop and review information security practices and standards for whole-of-government services and contracts
- Publish the information security framework

IAPPU will continue to involve Tasmanian Government agencies and local government bodies in the maintenance of the framework.

In accordance with the Charter, IAPPU will report to and work under the direction of the IASC.

1.3.3 Agencies

Agencies are responsible for the implementation of the Charter. The supporting material, including the policies and guidelines has been developed to assist agencies implement information security in accordance with the Charter.

The Guidelines reference legislation relevant to information security but this does not reduce the requirement for each agency to be aware of the full extent of legislation that applies to the agency.

1.3.4 Agencies delivering services for other agencies

Agencies or business units of agencies, delivering or managing contracts for the delivery of whole-of-government services are responsible for the implementation of the Charter for the whole-of-government components of those services.

An agency or business unit of that Agency that delivers or manages services or contracts on behalf of another Agency is responsible to the agency that is the original provider of the information for information security.

1.4 Information Security Guidelines overview

This section contains an overview of the major themes in the Guidelines.

1.4.1 Policy and procedure guidelines

The Information Security Guidelines (Sections 2 - 7, of this document) provide advice on procedures for the implementation of each of the policies, for example in an Agency Information Security Plan. Each guideline section may refer to standards or other material that is integral to implementing the policy.

1.4.2 Risk management guidelines

The Risk Management Guidelines (Section 8 of this document) establish the risk assessment and management policy. This includes a methodology and a template as appendices for agencies to use in assessing information security risks and developing plans.

The Risk Management Guidelines scope is limited to information security risks. However, it can be easily applied to general business risks within agencies. Agencies may wish to broaden the scope of risk assessments to include information security and other operational risks.

1.4.3 Information security standards

Standards provide commonly recognised guides, controls and processes for implementation of principles and policies. If there is a conflict between a standard and this document then this document takes precedence.

The following standards are used to aid implementation of the Tasmanian Government Information Security Principles and Policies:

- *AS/NZS ISO/IEC 27001:2006 Information technology – Security techniques – Information security management systems – Requirements*

- *AS/NZS ISO/IEC 27002:2006 Information technology – Security techniques – Code of Practice for information security management*

- *AS/NZS 4360:2004 Risk management*

- *AS ISO 15489 –1:2002 Records Management*

IAPPU provides Tasmanian Government public sector bodies with access to these and other standards at http://www.egovernment.tas.gov.au.

1.5 Using the guidelines

The information in this section is intended to assist effective use of the Framework.

1.5.1 Updates

This document is updated occasionally; therefore it is important that agencies use the latest release available from: http://www.egovernment.tas.gov.au

1.5.2 Feedback

IAPPU welcomes feedback on the Tasmanian Government Information Security Framework. Direct feedback or enquiries to:

Email: iappu.enquiries@dpac.tas.gov.au
Web: http://www.egovernment.tas.gov.au
Phone: 03 6232 7633

1.5.3 Target audience

The target audience for the Information Security and Risk Management Guidelines is the following agency personnel:

- Information security advisors

- Security advisors

- Information and communications technology managers and technicians

- Records managers

- Facilities managers

- Those with a responsibility for managing information, custodians of information or information security

1.5.4 Keywords for requirements

Keyword	Interpretation
MUST	The item is mandatory.
MUST NOT	Non-use of the item is mandatory.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
RECOMMENDS RECOMMENDED	The specified recommendation or suggestion.

Agencies deviating from a 'MUST' or 'MUST NOT' statement MUST advise the IASC of the decision to waive particular requirements.

Agencies deviating from a 'SHOULD' or 'SHOULD NOT' statement MUST document:

- The reasons for the deviation
- An assessment of the residual risk resulting from the deviation
- Date at which the decision will be reviewed
- Management approval

Agencies deviating from a RECOMMENDS or RECOMMENDED are encouraged to document the reasons for doing so.

1.6 Whole-of-government implementations of the Framework

Whole-of-government implementations are included in the framework to assist agencies with the preparation of information security plans.

1.6.1 WAN and Internet Services Security

The *Whole-Of-Government Wide Area Network Information Policy and Guidelines* has been developed in accordance with the Framework. Currently this covers the services delivered under the Networking Tasmania (NTII) contract.

The policies are based on *AS/NZS 17799:2001 Information Technology – Code of practice for information security management*.

The plan and policies cover:

- Roles and responsibilities of TMD, agencies and contractors
- Protection of the network from external threats
- Protection for each agency from threats originating from other agencies and/or externally

- Standards to ensure that each agency does not compromise the information security requirements of other agencies
- Incident reporting and management regime
- Confidentiality regime for the supplier(s), its personnel and subcontractors

2 Information Security Governance Guidelines

2.1 Purpose

This section contains minimum information security governance policies and guidelines to be implemented by agencies to achieve appropriate information security within the Tasmanian Government.

2.2 Governance Policy

The Information Security Governance Policy in the Charter requires that:

> 'Agencies are to manage information security through the establishment of a management framework to initiate and control the implementation of information security within the agency.'

2.3 Guidelines for implementing the Governance Policy

Senior management is responsible for integrating a systematic and coordinated framework for identifying, assessing, and treating information security risks into an agency's philosophy and plans.

2.3.1 Information Security Management Systems

Agencies SHOULD govern and manage information security by using AS/NZS ISO/IEC 27001:2006. The objective of this Standard is to specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organization's overall business risks.

2.3.2 Risk assessment and treatment

Agencies SHOULD assess and treat risks by using:

- AS/NZS ISO/IEC 27002:2006, Section 4
- AS/NZS 4360: 2004
- Risk Management Guidelines Section 8 of this document
- Record Security Guidelines Section 3 of this document

Agencies SHOULD have a single risk management approach to all operational risks, including information security see Risk Management Guidelines Section 8 of this document.

2.3.3 Agency information security committee

Agencies MUST utilise senior management to establish an Agency Information Security Committee (or assign the role to an existing senior management committee). The Committee SHOULD include representation from key information security stakeholders and senior managers from the Agency. The role of the committee is to:

- Develop information security plans within the Agency
- Assign responsibilities to individual officers
- Coordinate the implementation of information security across the Agency
- Approve security roles within the Agency
- Oversee the development and implementation of an agency communications plan for information security
- Coordinate routine information security inspections and reviews

2.3.4 Agency security officers

Agencies SHOULD appoint a designated Agency Security Officer(s), whose role is to coordinate:

- Implementation of Agency information security policies
- Delivery of information security communication, education and training
- Investigations of information security incidents

Agencies may have several designated Security Officers covering different areas. For example, they may have separate officers responsible for ICT security, physical security, individual business units, and/or record security.

Agency Security Officers SHOULD report directly to the Agency Information Security Committee on information security matters.

2.3.5 Security policy

Agencies SHOULD manage documentation and review of information security policies using AS/NZS ISO/IEC 27002:2006, Section 5.

2.3.6 Organisation of information security

Agencies SHOULD manage information security within the organisation using AS/NZS ISO/IEC 27002:2006, Section 6.

2.3.7 Asset management

Agencies SHOULD establish and maintain appropriate protection of assets using AS/NZS ISO/IEC 27002:2006, Section 7.

The following Treasurers Instructions issued under the *Financial Management and Audit Act 1990* have similar requirements to maintain asset registers:

- *TI 304 - Recording of Non-current Assets*
- *TI 306 - Intangible Assets*

2.3.8 Compliance

Agencies SHOULD avoid breaches of statutory or contractual obligations and security requirements using AS/NZS ISO/IEC 27002:2006, Section 15.

3 Record Security Guidelines

3.1 Purpose

This section contains minimum record security policies and guidelines to be implemented by agencies to achieve appropriate information security within the Tasmanian Government.

3.2 Record Security Policy

The Information Security Records Policy in the Charter requires that:

'Agencies are to implement appropriate record security policies and procedures as part of their records management policies and procedures to ensure the security of information access, transmission, storage and destruction.'

3.3 Guidelines for implementing the Record Security Policy

These guidelines have been developed to be consistent with the *Archives Act 1983*, guidelines and advices issued under the Act, and *AS ISO 15489 Records Management*. The standard has been endorsed by the State Archivist as a model for best practice record keeping in Tasmanian State and local government organisations. Agencies may have to develop these guidelines further to be fully compliant with AS ISO 15489.

The scope of this document applies to all records, whether paper-based or electronic, and includes information held in databases. A record is described as:

> '…information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.'[1]

Some of the procedures relating physical security and the electronic systems are outlined in sections 4 Physical Security Guidelines and 6 General ICT Guidelines in this document.

When implementing these guidelines, agencies SHOULD analyse business needs, including regulatory requirements and constraints. Accordingly, these guidelines have been developed to be consistent with AS ISO 15489 and consider:

> 'Development of appropriate categories of access rights and restrictions is based on the organisation's regulatory framework analysis, business activity analysis and risk assessment. Reasonable security and access will depend on both the nature and size of the organisation, as well as the content and value of the information requiring security. Reasonable security can be described as the level of security that a reasonable person on the street would believe is needed to protect the information from any unauthorised access, collection, use, disclosure, deletion, alteration and/or destruction.' [2]

These guidelines are intended to be simple to administer, using risk assessment as the basis of identifying standard exceptions to normal procedures. The features and benefits of the model include:

---

[1] Section 3.15 *ISO AS15489.1 Records Management Part 1: General*
[2] Section 4.2.5.2 *ISO AS15489.2 Records Management Part 2: Guidelines*

- The provision of standard procedures relating to information access, transmission, storage and destruction requirements for the majority of information within the agency

- The application of a risk assessment that examines the sensitivity and risks of records and then determines if an exception model is appropriate

- A list of alternate procedures that may be considered by agencies for information justifying a higher level of security

It is RECOMMENDED that agencies implement a methodology to assess when appropriate changes to these guidelines are required.

3.3.1 Risk assessment

A core component of the *Information Security Framework* is the application of a risk assessment for all aspects of information security to determine the appropriate level of security.

Agencies SHOULD identify key groups or types of records and conduct a high-level risk assessment against each that encompasses the operational responsibilities and requirements of the agency. The purpose of the risk assessment is to identify:

- Groups or types of records held by the agency

- Whether particular groups or types of records have any particular risks or security (eg business, political, or legislative) requirements beyond those provided by standard procedures

- Mitigation strategies to be applied to records that present higher levels of risk

Groups or types of records that may present higher levels of risk include those where unauthorised disclosure, loss of integrity, or unavailability may:

- Seriously damage or compromise the success or adversely affect the viability of a commercial venture or law enforcement process

- Cause distress to, or threaten an individual (eg medical patient records or HR personnel records)

- Have specific legislative restrictions or requirements (eg prisoner or adoption records)

- Cause serious financial damage to and/or lead to litigation against the Government

- Seriously damage the economy of Tasmania

- Cause serious loss of public confidence

3.3.2 Standard procedures

The following procedures SHOULD NOT be implemented for the protection of records that have been identified as presenting high risk to an agency. Agencies may wish to supplement the procedures for particular requirements.

Standard Procedures	
Paper Records	**Electronic Records**
Access	
• Available to agency employees who have a business requirement to access the records • Available to authorised third parties	• Available to agency employees who have a business requirement to access the records • Available to authorised third parties • Password policy implemented on systems
Transmission	
• Clearly show a return address in case of unsuccessful delivery • Clearly identify the originating agency • No special designation when passed outside the organisation • May be carried by internal courier service unsecured • May be carried by ordinary postal services or commercial courier firms, provided the envelope/package is sealed	• Clearly show a return address in case of unsuccessful delivery • Clearly identify the originating agency • Can be transmitted across external or public networks (including the Internet) without being encrypted. The level of information contained is to be assessed before transmitting. • Accompanied by an outline of the legal responsibilities and disclaimer if received in error
Storage	
• Stored in lockable cabinets or open shelving secured by normal building security and /or door swipe card systems to prevent public access. Refer to Physical Security Guidelines Section 4 of this document for further information.	• Computer systems controls as per General ICT Guidelines Section 6 of this document
Home Based or Mobile Workers	
• When unattended information is secured as per Physical Security Guidelines Section 4 of this document	• As per Sections 4 Physical Security Guidelines and 6 General ICT Guidelines of this document
Destruction	
• Secure destruction of the record after the time specified for retention, as determined by the State Archivist, has elapsed • For detailed guidelines relating to the disposal of records see www.archives.tas.gov.au • Consider the disposal of paper records via security shredding service eg to maintain client confidentiality	• Secure destruction of the record after the time specified for retention, as determined by the State Archivist, has elapsed • For detailed guidelines relating to the disposal of records see www.archives.tas.gov.au • Electronic media disposal for non-sensitive information as per General ICT Guidelines Section 6 of this document.

3.3.3 Procedures for higher risk records

When developing procedures to mitigate higher levels of risk it is RECOMMENDED that agencies:

- Keep the number of procedural variations to a minimum
- Make it obvious to personnel, which procedures apply in each circumstance
- Where appropriate, apply higher risk procedures for a fixed time or until a specified event or date occurs

- Mitigate the identified risks
- Ensure the procedures comply with appropriate legislation, including the *Archives Act 1983*
- If applicable, ensure that procedures comply with the *Australian Government Protective Security Manual*
- Minimise the agency effort required to meet differing requirements, including archives disposal schedules and other business and legislative requirements

The following procedures SHOULD be implemented for the protection of records that have been identified as presenting higher risk to an agency.

Procedures for higher risk records	
Paper Records	**Electronic Records**
Access	
• Limiting access to permanent records transferred to the Archives Office of Tasmania • Strict controls on which agency staff may have access to the records • Photocopying of documents to be carefully controlled	• Limiting access to permanent records transferred to the Archives Office of Tasmania • Strict controls on which agency staff may have access to the records • Audit trail of all access to information • Separate read and write access controls
Transmission	
• Accompanied by an outline of the legal responsibilities and disclaimer if received in error • Information to be clearly marked indicating high security procedures are required • Security markings are not to be visible in message header or external envelope • Use of sealed envelopes with tamper proof seals when carried by courier • Where the risk is very high, use of double envelopes when posted or carried by commercial courier firms	• Accompanied by an outline of the legal responsibilities and disclaimer if received in error • Information to be clearly marked to indicate alternate procedures are required • Use of encryption when transmitted across external or public networks (including the Internet) • Where the risk is extreme, use of encryption when transmitted between agency sites
Storage	
• Where the risk is very high, use of a nominated security guard or officer • Provision of sealed off, fire resistant area of building for storage of computer systems and/or physical records • Stored separately to other information. • Stored in lockable cabinets or open shelving or a controlled area with security perimeter and restricted access • Refer to Physical Security Guidelines Section 4 of this document for further information	• Where the risk is very high, use of a nominated security guard or officer • Provision of sealed off, fire resistant area of building for storage of computer systems and/or physical records • Computer systems controls as per General ICT Guidelines Section 6 of this document • Encryption when stored in a device or location that is not physically secured

Procedures for higher risk records	
Paper Records	**Electronic Records**
Home Based or Mobile Workers	
• Records being transported, including by employees, are secured in locked containers • As per Physical Security Guidelines Section 4 of this document for sensitive information	• Where the risk is very high, encryption • As per Sections 4 Physical Security Guidelines and 6 General ICT Guidelines of this document
Destruction	
• For detailed guidelines relating to the disposal of records see www.archives.tas.gov.au • Secure destruction by shredding of the record after the time specified for retention, as determined by the State Archivist, has elapsed • Disposal of paper records via security shredding service	• Secure destruction of the record after the time specified for retention, as determined by the State Archivist, has elapsed • For detailed guidelines relating to the disposal of records see www.archives.tas.gov.au • Electronic media disposal for sensitive information as per General ICT Guidelines Section 6 of this document

3.3.4 Application of procedures

Agency personnel are integral in the implementation of records security policies and procedures. See Personnel Security Guidelines Section 5 of this document for further information.

It is RECOMMENDED that the employee who creates or received a record is to apply the appropriate record security procedures. Note that procedures to be applied might change after a time or event has elapsed.

For the sake of simplicity, an agency may develop a single set of record security procedures that are to be applied to all information held by a particular business unit.

3.3.5 Legislative framework

The *Archives Act1983* is the legislation that directly impacts on the management of records in the Tasmanian public sector. One of the main objectives of this Act is to achieve accountability in public administration by prohibiting the unauthorised destruction or manipulation of records. The definition of state records covers information made by, or kept in, agencies and it relates to information held in any format (including information held in electronic systems).

The *Archives Act 1983* stipulates that employees of State or Local government agencies (or any other person) MUST NOT dispose of records of any type without the written authority of the State Archivist. Written authority may take the form of either:

- A Disposal Schedule (a continuing disposal authority listing records by type and identifying appropriate disposal actions); or

- An authorised destruction authority (a one-off authorisation to destroy the specific records listed therein).

The *Freedom of Information Act 1991* gives the public the right to access information held by the State Government and its agencies. A person is entitled to information held by an agency if it relates to that person's affairs. Due to the sensitivity of some information, access by the general public can be exempted in accordance with the Act.

The *State Service Act 2000* Code of Conduct Section 9 (7); states that an employee MUST maintain appropriate confidentiality about dealings of, and information acquired by, the employee in the course of that employee's employment. Similar requirements may exist in other legislative conditions of employment (eg *Police Service Act 2003*).

Each agency MUST take into account legislation that is specific to its business operations. It is RECOMMENDED that agencies refer to the following list of legislation that applies to all agencies when developing record security policy and procedures.

Act	**Topic**
Archives Act 1983	Responsibilities for the creation, maintenance, retention and disposal of records.
Criminal Code Act 1924	Criminal activity, including fraud.
Personal Information Protection Act 2004	Management of personal information collected by agencies.
Electronic Transactions Act 2000	Enables the acceptance of transactions in electronic form including signatures.
Evidence Act 2001	Enables records kept in electronic format to be admissible as evidence in court proceedings.
Financial Management and Audit Act 1990	Accounting and audit requirements.
Freedom of Information Act 1991	Public access to information held by the agency.
Government Business Enterprises Act 1995	Accounting and auditing requirements undertaken by statutory bodies not covered under the *Financial Management and Audit Act 1990*.
Libraries Act 1984	Legal deposit. Copies of published documents are to be provided to the State Library in Tasmania.
Ombudsman Act 1978	Investigation of complaints with respect to administrative action taken by or on behalf of certain government agencies.
Public Account Act 1986	Management of the Public Account of the State.
State Service Act 2000	Human resource management.
Workplace Health & Safety Act 1995	Requirement to maintain records for plant and equipment, etc and accident records.

4 Physical Security Guidelines

4.1 Purpose

This section contains minimum physical security policies and guidelines to be implemented by agencies to achieve appropriate information security within the Tasmanian Government.

4.2 Physical Security Policy

The Physical Security for Information Security Policy in the Charter requires that:

> 'Agencies are to ensure appropriate physical security measures are adopted to prevent unauthorised access, damage, loss or interference to agency information, information systems, services or equipment.'

The appropriate level of physical security measures SHOULD be determined following a risk assessment. The risk assessment SHOULD include information resources held within a site and external information resources that can be accessed (electronically) from a site.

4.3 Guidelines for implementing the Physical Security Policy

The scope of factors that impact on physical security is wider than information security requirements. Therefore, agencies need to consider wider issues and risks when developing agency and site-specific physical security plans for information security.

When implementing these guidelines agencies SHOULD determine the level of risk and other operational requirements, including:

- The need for, method and extent of public access to the workplace (eg schools, libraries, and health facilities all have high levels of public access)
- Emergency Evacuation Procedures, and how they link to and possibly benefit through the existence of access control procedures
- Cost of risk mitigation (monetary and non-monetary) compared to the level of risk
- Restrictions and requirements for multi-tenanted sites (ie sites shared with other organisations)
- Cross agency requirements for sites that are shared with other agencies
- Review of risk assessments when the use of a building or the level of risk changes

Agencies SHOULD use AS/NZS ISO/IEC 27002: 2006 Section 9 for physical and environmental security controls.

Perimeter defences SHOULD NOT contain any obvious weakness that could tempt exploitation.

Physical security defences are primarily designed to meet the threat to security posed by the ill-intentioned person who already has authority to enter the building rather than the intruder from outside. The primary defences are those nearest the information requiring protection.

An agency with a substantial quantity of sensitive information to protect, may find other precautions are necessary to give depth to defences and to guard against human error. These include control of entry, both day and night, and limitations on the free movement of visitors.

Control of entry to buildings is best exercised by admitting visitors and personnel through only one entrance, either by recognition, an identity pass, or by a security key or an automatic access control system. An identity pass system does not automatically ensure security. Indeed, if it becomes no more than a routine formality, it can become a positive danger to security.

4.3.1 Precautions within buildings

Agencies SHOULD develop and maintain documented precautions within work areas to protect the information held within, or accessible from, the work area.

Agencies SHOULD implement precautionary measures and practices including surveys, risk assessments, and security within the workplace, including:

- Review when the use of a building or the level of risk changes
- Securing workplaces after hours
- Ensuring sensitive information is secured when not in actual use
- Practices for staff challenging unescorted strangers
- The use of secure zones within buildings, where warranted

4.3.2 Home-based work environments

Agencies SHOULD ensure that home based employees have suitable security arrangements in place for the storage and use of all official information, both electronic and paper.

4.3.3 Instructions to doorkeepers

Doorkeepers that carry out security functions SHOULD be issued with written instructions on their duties, together with details of those passes whose holders may be admitted. The instructions SHOULD contain the names and telephone numbers of those persons to whom the doorkeepers report incidents of security significance, both during and outside working hours.

The instructions to doorkeepers SHOULD be designed to meet the particular conditions for every entrance to every building.

It is RECOMMENDED that close liaison between those controlling doorkeepers and the agency security organisation be maintained to ensure that the written instructions are understood, observed and kept up to date; and that the doorkeepers carry out their duties efficiently.

4.3.4 Access control by personal recognition

Where the number of personnel is small, it is RECOMMENDED that the safest means of controlling entry is by individual recognition, provided that:

- Alert and responsible doorkeepers are regularly employed on the same duty and they are of sufficient calibre to resist any attempts by persons of self-assumed importance to evade their control

- The rate of personnel turnover is low and personnel are initially introduced to the doorkeepers who are informed when individuals cease to be employed in the building

This method SHOULD NOT be used for controlling the entry of large numbers of personnel.

4.3.5 Access control by identity pass

Agencies SHOULD implement the following when an identity pass system is used:

- Each pass is to be serially numbered and a record kept of the person to whom it was issued

- Everyone receiving a pass to be required to sign for it immediately in the presence of the issuing officer

- The pass to not identify the premises to which it gives access

- The graphic design of passes used by agencies to be changed from time to time

Personnel SHOULD be instructed as follows when an identity pass is issued:

- Immediately report the loss of a pass to the issuing officer

- Return the pass to the issuing officer, or an Agency Security Officer, as appropriate when going on leave

- Not to carry the pass out of Tasmania

- Not to keep their passes with other documents that may disclose their place of work

- It is their personal responsibility to return the pass when they cease to hold the appointment or occupation for which the pass was issued, or when the period of validity of the pass has expired. Similar instructions, as appropriate, apply to holders of period or temporary passes

Personnel SHOULD be required to show their passes each time they enter the premises and, at the discretion of agencies, when they leave. This exposes an intruder to risks of detection, brings lost or mislaid passes to early notice, and ensures the collection of day passes. In addition:

- Personnel leaving outside normal working hours SHOULD be required to produce their passes on departure to the doorkeeper

- If there is no doorkeeper after normal working hours, other options for recording departures SHOULD be considered. Possibilities include using a logbook or an automatic access control system

4.3.6 Types of Identity Passes

Agencies SHOULD issue different types of passes for permanent employees, ancillary personnel, regular and casual visitors. It is RECOMMENDED that different passes be used as follows:

- Permanent staff passes – issued to members of the staff and others working permanently in a building

- Ancillary personnel passes – it is advisable to issue passes, which can be distinguished from those used by permanent employees, to regular ancillary personnel such as canteen workers, cleaners etc

- Period (or temporary) passes - be a different type and marked with the date of expiry; to be issued to regular visitors, such as officials from other agency, maintenance engineers etc, whose need and suitability has been established, eg by certificate from sponsoring official or agency. Such passes remain valid only for the period for which they are required.

- Day (or visitor) passes – can be on ordinary paper made up into counterfoil books with a warning printed on the pass that it is to be given up on leaving. It is important to keep a record of the issue of each pass so that a check can be made of returned passes each evening to ensure that all visitors have left the premises.

- Holders of day passes are to be escorted unless the officer to be visited confirms that this is unnecessary

4.3.7 Automatic access control system

In some circumstances automatic access control systems using specially coded cards with electronic card readers can be used as an alternative to doorkeepers and pass systems.

4.3.8 Visitors

The procedures for visitor access will vary, depending upon the nature of the business and level of risk in each work area.

At a minimum, except for designated public areas, doorkeepers SHOULD allow visitors to enter a work area only if the visitor is on recognised business (ie a meeting) or is cleared by a host official.

4.3.9 Visitor controls in high risk areas

It is RECOMMENDED that agencies have accommodation plans that discourage the need for staff to have visitors in high-risk areas.

Where the risk is high or extreme, visitors to areas housing a substantial amount of sensitive information SHOULD NOT be allowed uncontrolled freedom of movement. In areas that necessitate access pass control, visitors SHOULD be escorted when on the premises. It is RECOMMENDED that prior notice be given to the doorkeeper of the expected visitor and whether the visitor needs to be escorted within the building.

On arrival visitors SHOULD, if appropriate, be issued with a pass and conducted either to a waiting room (that is observable by an officer or the doorkeeper) or to the host official.

The visitor control record SHOULD be covered to prevent visitors from seeing the details of other visitors.

Visitors SHOULD be advised that no photographs or recordings of any type may be taken at any time during the visit. It is RECOMMENDED that visitors be asked to deposit mobile phones and other equipment to the reception desk.

The ‘host’ official SHOULD be contacted by telephone and asked if they will receive the visitor if the official concerned has not given prior notice of the visit. If calling on more than one official, visitors SHOULD be escorted between offices.

Responsibility for ensuring that the visitor leaves the building when their business is concluded, and that any pass issued is duly returned to the doorkeeper, rests with the official last visited. They SHOULD either conduct the visitor to the entrance, or arrange for another member of the staff to act as escort. Access and exit from visiting areas SHOULD be arranged to avoid entry to working areas where sensitive material may be on display or accessible.

In agencies with a substantial flow of enquiries or visitors, it is RECOMMENDED that agencies have a reception desk close to the main entrance.

4.3.10 Identification of personnel keeping unusual hours

Agencies SHOULD determine if there are any information security risks involved in relation to personnel keeping unusual hours. It is RECOMMENDED that risk assessments be conducted to manage the risk on the basis that there is not necessarily anything sinister in an officer working unusual hours.

Agency policies and practices regarding personnel working unusual hours will also be determined by other factors, including occupational health and safety issues.

Agencies SHOULD maintain a record of personnel who have after-hours access as a minimum.

If risks warrant, appropriate procedures RECOMMENDED include:

- Maintaining logs of all after-hours access (including late departures and early arrivals)
- Developing an understanding of which members of personnel make a habit of and have a need to access the workplace after hours

If it is revealed that an officer is regularly keeping unusual hours without the reasons being evident, it is RECOMMENDED that the Agency Security Officer make discreet enquiries to determine the reason.

4.3.11 Room security

It is RECOMMENDED that locked security containers be used to protect sensitive documents during working hours. It is the responsibility of individual officers and of supervisors in large units such as registries to ensure that the documents cannot be read, handled or removed by persons not authorised to see them.

Security containers include lockable draws, lockable filing cabinets, safes etc. It is RECOMMENDED that the selection of security containers is to be based on the level of risk, and remembering that cleaners normally have unsupervised access to locked offices.

Sensitive documents SHOULD be locked up whenever they are not in actual use. If a room is to be left unoccupied, sensitive documents (including waste) SHOULD be locked in security containers during any absence of more than a period to be specified in agency security instructions. In deciding what period to specify, it is RECOMMENDED that agencies have regard to the nature of other security precautions within the building.

When sensitive documents are not locked away because a room will be left unattended for less than the specified minimum period, the doors to the room SHOULD be locked, all sensitive documents SHOULD be protected from being read from outside, and windows SHOULD be closed and secured. When cleaners or other workers might have access from outside, all sensitive documents SHOULD be locked away whenever a room is vacated.

The degree of protection needed for material such as internal telephone directories varies with agency responsibilities and is a matter for the discretion of the agency, taking into account the amount of job description contained in the directory.

4.3.12 Room checks by occupants at close of work

Occupants SHOULD check all rooms at the close of work to ensure that sensitive documents, including sensitive waste, have been properly locked away in security containers and security keys mustered. Even conscientious personnel can occasionally fail in this respect and it is RECOMMENDED to institute a room check on a roster system before offices are vacated.

In agencies holding a substantial amount of highly sensitive information, a check of rooms by an Agency Security Officer after the departure of occupants and before entry of cleaners or guard patrols is RECOMMENDED.

4.3.13 Conferences and meetings

When officers are required to take material into meetings, the following precautions are RECOMMENDED:

- Prior to commencing the meeting, ensure that unauthorised people are not present
- Ensure that no sensitive information or waste remains in the room at the close of the meeting
- When representatives of outside organisations are present, preclude the possibility of official documents being overviewed by unauthorised people by planning appropriate seating arrangements

If special security arrangements are considered to be necessary, agency security staff SHOULD be consulted.

When a person from outside the agency is attending a meeting, refer to Sections 4.3.8 Visitors and 4.3.9 Visitor controls in high risk areas of this document.

4.3.14 Planning accommodation

Careful planning of layout within a building can reduce security problems.

Offices SHOULD be selected that do not share walls with other tenants and are removed from common user corridors and stairways where protection against eavesdropping is required.

The siting of registries near to the offices they serve facilitates the secure movement and control of sensitive documents.

Staff engaged in sensitive work SHOULD be located out of range of direct vision to reduce the risk of documents or computer screens being read by unauthorised persons.

To encourage proper storage and disposal of information, security facilities such as lockable filing cabinets and shredders, SHOULD be conveniently located for staff members that are required to use the facilities.

Security requirements SHOULD be specifically referred to in any accommodation brief.

4.3.15 Secure zones within buildings

When varying degrees of security protection are required within the same building, high risk activities SHOULD be concentrated in one area and segregated as a secure zone. Access to such zones SHOULD be adequately secured and the entrance confined to staff with authorised access.

Staff themselves can control entry to the secure zone. Entrances SHOULD be reduced to one or two doors, locked during working hours and with a visitor's bell outside.

Where a normal locking system is used, it is RECOMMENDED that keys used by staff during working hours are mustered and locked away in a security container at the close of work. Alternatively, an automatic code lock or card access control system can be used.

4.3.16 Overhearing/eavesdropping

Under normal working conditions, ordinary speech is not intelligible beyond a range of 15 metres. Exceptions where this distance may be exceeded include, conditions of quietness, or where sound waves could be ducted by building structural anomalies or with technical aids.

In considering the risk of overhearing (as distinct from eavesdropping by technical means), it is RECOMMENDED that other sounds which may mask speech in sensitive rooms is taken into account. The risk of overhearing is obviously increased when windows are open, especially at ground level.

Dictation is more easily overheard than ordinary conversation and it is RECOMMENDED not to dictate very sensitive letters or telegrams. Where dictation is essential, particular care is to be taken when very sensitive items are involved.

4.3.17 Over-viewing from outside

Telephotography can be used for the photographing of documents from any position at an angle greater than 15 degrees above horizontal. The effective range depends on the equipment used and the conditions prevailing at the time. All windows of offices or rooms where sensitive work is undertaken SHOULD be regarded as vulnerable to telephotography from outside.

Net curtains or opaque glass may provide protection. When a room is artificially lit, net curtains do not always provide protection, and it is RECOMMENDED that curtains or blinds (including venetian blinds) are drawn or closed to minimise risk.

4.3.18 Ancillary staff

The security vetting of ancillary staff does not negate the need for physical security measures. In implementing protective measures and security education for those handling sensitive information, agencies SHOULD ensure that ancillary staff (guards, cleaners, decorators, maintenance workers, canteen staff etc) do not have access to sensitive documents or equipment, and do not overhear discussions or dictation involving sensitive matters.

In short, the need-to-know principle SHOULD be preserved whether or not ancillary staff has been vetted.

4.3.19 Mail and other deliveries

The planning of accommodation and associated procedures SHOULD address risks associated with the receipt and dispatch of mail and other items, including:

- Ensuring adequate protection from unauthorised access to items awaiting delivery or to items that have been delivered
- Ensuring adequate protection from unauthorised access to mail and parcel items, including items using internal couriers
- Appropriate procedures relating to the handling of suspicious deliveries

Where appropriate, agencies SHOULD consult with Tasmania Police.

4.4 Acknowledgment

Much of this guideline is based on the New Zealand Government publication *Security in Government Departments (1994)*. This document has been replaced by the publication *Security in the Government Sector (2002)*. For more information see http://www.security.govt.nz/.

5 Personnel Security Guidelines

5.1 Purpose

This section contains minimum personnel security policies and guidelines to be implemented by agencies to achieve appropriate information security within the Tasmanian Government.

5.2 Personnel Policy

The Personnel Policy for Information Security in the Charter requires that:

> 'Agencies are to actively inform personnel who have access to agency information resources of their roles and responsibilities in regard to information security.'

The term 'personnel' is defined to include employees (including officers as defined by the *State Service Act 2000*), contractors, volunteers and students in this document.

5.3 Guidelines for implementing the Personnel Security Policy

5.3.1 General human resources security

Agencies SHOULD use AS/NZS ISO/IEC 27002: 2006 Section 8 to implement the Personnel Security Policy.

5.3.2 Legislative and policy constraints

Agencies MUST take into account legislation and policy that governs employment and conditions of personnel. Where appropriate, agencies MUST take into account legislation, policy, and contracts that govern students and contractors who have access to agency information resources.

Acts that may be applicable to agencies in the development and implementation of policies and procedures include:

- *Industrial Relations Act 1984*
- *Anti-Discrimination Act 1998*
- *State Service Act 2000* – applies to employees employed under the Act.
- *Police Service Act 2003*
- *Education Act 1994*

Other acts may also be applicable to agencies in the development and implementation of this policy.

5.3.3 Prior to employment

Pre-employment checks may be considered for employees that are likely to be handling sensitive material. However, there are a number of legislative restrictions. In general, pre-employment checks SHOULD only be used where there is a legislative requirement or clearly identified risk that can be reduced by such checks. Within the State Service the Office of the State Service Commissioner MUST approve use of pre-employment checks.

5.3.4 Assigning personnel responsibilities for information security

All personnel are to be responsible for disclosing and taking reasonable steps to avoid any conflict of interest in connection with their work in accordance with the *State Service Act 2000* or the *Police Service Act 2003*.

Where appropriate, agencies SHOULD assign to individual personnel or positions specific responsibilities for information security. For example agencies, may consider assigning:

- Responsibility for information security to business owners
- Individual personnel with responsibility for information they access that has special requirements (eg where there is a high business risk or legislation that requires high level of confidentiality to be maintained)
- The role of monitoring and reporting on information security policies, procedures and risks to specified personnel or positions

5.3.5 Informing personnel of their responsibilities

Agencies SHOULD actively inform personnel of their information security responsibilities by a combination of techniques including:

- Highlighting to personnel relevant parts of their Statement of Duties
- Providing personnel with a copy of the *State Service Code of Conduct*
- Providing regular reminders to personnel of their information security responsibilities. These may include:
    - Newsletters to personnel on their responsibilities and highlighting current issues and risks
    - Displaying prominent messages, eg on computer login screens, on file covers, on filing cabinets

Agencies SHOULD ensure that personnel with privileged access to resources have been made aware of their additional information security responsibilities. Examples of positions with higher privileges include Records Staff, ICT Administrators and Facilities Managers.

5.3.6 Compliance and monitoring

Monitoring of personnel for compliance with information security policies and procedures MUST only be carried out in accordance with appropriate legislation and policies.

6 General ICT Guidelines

6.1 Purpose

This section contains minimum general information and communications technology (ICT) policies and guidelines to be implemented by agencies to achieve appropriate information security within the Tasmanian Government.

6.2 General ICT Policy

The General IT Security Policy in the Charter requires that:

> 'Agencies are to have a comprehensive framework governing all aspects of information and communication technologies security.'

6.3 Guidelines for Implementing the General ICT Policy

6.3.1 Communications and operations management

Agencies SHOULD use AS/NZS ISO/IEC 27002:2006 Section 10 to manage communications and operations management.

6.3.2 Access control

Agencies SHOULD provide access to information on the basis of business requirements including the sensitivity of information and the risk associated with delivery of a business service.

Agencies SHOULD use AS/NZS ISO/IEC 27002:2006 Section 11 to manage access control.

Agencies SHOULD ensure that controls applied to privileged users and associated audit logs are more comprehensive than for other users. Privileged users have the potential to impersonate other users therefore secure audit trails on their activities are essential.

Audit logs are records under the *Archive Act 1983* and MUST NOT be disposed of without the written authority of the State Archivist.

Agencies SHOULD ensure that there are appropriate network access control interfaces between the agency's LAN and the Networking Tasmania network.

Where a business application that is managed by an agency:

- Has users external to the agency that manages the application, or
- The application accesses information provided by another agency, and
- A moderate to high level of risk is identified by any of the users, application manager or information providers;

Then it is RECOMMENDED that the following be implemented by the agency that manages the business application:

- A risk assessment to establish the level of risk for the application manager, users and information providers

- Staff identities from the respective agencies are registered and maintained in an appropriate manner

- Authentication mechanisms employed are commensurate with the level of risk determined by the risk assessment

- Administrators and privileged account holders of the system and related infrastructure understand their responsibilities and sign an acceptable use agreement

- Appropriate audit logs are in place to protect the confidentiality and integrity of all information accessed by an application

6.3.3 Information systems acquisition, development and maintenance

Agencies SHOULD use AS/NZS ISO/IEC 27002:2006 Section 12 to manage information systems acquisition, development and maintenance.

Agencies SHOULD conduct risk assessments on the use and disposal of new and emerging technologies to ensure information security polices are maintained.

6.3.4 Business continuity management

Agencies SHOULD use AS/NZS ISO/IEC 27002:2006 Section 14 to manage business continuity.

6.3.5 Media handling and security

Agency procedures SHOULD cover the repair and maintenance of media, including the exchange of media with a supplier as part of a warranty and/or maintenance agreement.

When disposing of media, agencies MUST ensure all information held on the media is either retained or disposed of in accordance with:

- *Archives Act 1983,* and

- *Treasurer's Instruction 1301 – Disposals* issued under the *Financial Management and Audit Act 1990*.

Information can be leaked to outside persons through careless disposal of media, including exchange of media as part of a warranty and/or maintenance agreement. The method of media disposal SHOULD be based on the risks associated with the content held on the media.

Agencies SHOULD address the need for sanitisation or destruction of all media prior to reuse in a new environment or disposal. Disposal includes removal of media off site under warranty or hardware service agreements. Media sanitisation and disposal guidelines are suggested in the table below. For more details see *ACSI33* Chapter 4 – Hardware Security.

	Media Reuse or Disposal Method	
Media Type	**Media Contains Non Sensitive Business Information**	**Media Contains Sensitive Information**
• Optical disks eg CD or DVD • Microfilm • Microfiche	• Disposal without physical destruction	One, or a combination of: • Physical destruction, (shredding) • Incineration
• Electrostatic devices eg laser printer or copier drums (Note: many modern photocopiers also have magnetic disks)	• Reuse or disposal without destruction or sanitisation	One, or a combination of: • Sanitised by printing a quantity of non-sensitive information prior to disposal (or recycling) • Physical destruction
• Magnetic media eg hard disk drives, floppy disks, tapes	• Low-level formatting or similar activity (do not use 'quick' format methods)	One, or a combination of: • Low-level formatting or similar activity (do not use 'quick' format methods) • Demagnetised and so rendered useless • Physical destruction
• Personal electronic devices or flash ROM eg mobile phones, SIM cards, USB flash drives, memory stick, camera cards	• Low-level formatting or similar activity (do not use 'quick' format methods)	One, or a combination of: • Low-level formatting or similar activity (do not use 'quick' format methods) • Physical destruction

6.3.6 Access by external parties

Agency web sites SHOULD be designed to avoid features that may be viewed by external organisations as a security risk.

Also refer to Information Security Governance Guidelines Section 2 of this document.

7 Incident Management Guidelines

7.1 Purpose

This section contains minimum information security incident management policies and guidelines to be implemented by agencies to achieve appropriate information security within the Tasmanian Government.

7.2 Incident Reporting Policy

The Incident Reporting Policy in the Charter requires that:

> 'Agencies are to minimise the damage from information security incidents and monitor and learn from such incidents.'

7.3 Guidelines for implementing the Incident Management Policy

7.3.1 Reporting and management of security incidents

Agencies SHOULD investigate, report and conclude investigations of security incidents in a thorough, sensitive and timely manner. In some situations, especially information and communication technology based incidents, it is appropriate to commence investigation while the incident is still underway.

Agencies SHOULD conduct periodic reviews of breaches to enable identification and rectification of any recurring problems.

Agencies SHOULD use AS/NZS ISO/IEC 27002:2006 Section 13 to manage:

- Reporting of security events and weaknesses, and
- Security incidents and improvements to management of incidents.

7.3.2 Legal action

When criminal activity affecting information security is identified, agencies MUST liaise with Tasmania Police. Any decision to notify Tasmania Police of criminal activity SHOULD be made the earliest opportunity. In these cases, the agency investigator and any other relevant agency representative SHOULD NOT prejudice further police investigations and possible prosecution.

A decision of invoke legal action may alter the priorities and procedures that are followed. For example, retention of evidence in a form to support a police investigation and possible prosecution may delay the resolution of any incident, or delay the implementation of any preventative measures.

7.3.3 Planning for information security incidents

Agencies SHOULD develop information security incident management plans. The Agency Information Security Committee and/or the Secretary/Head of Agency SHOULD approve security incident management plans.

An agency security incident management plan SHOULD include general priorities for action during an incident. The priorities may change depending on the nature of the incident, including the visibility and impact of the incident on staff and/or the public.

RECOMMENDED priorities are:

1. Protection of human life and people's safety
2. Protection of sensitive information
3. Protection of other information
4. Prevention of irreparable damage to systems
5. Internal and external communication of the incident
6. Minimising disruption to services
7. Pursuing legal action (see Legal action Section 7.3.2 of this document)

Establish roles and responsibilities to ensure that incident responses are appropriately managed. It is RECOMMENDED that contact lists of the following are prepared:

1. Agency staff responsible for each site
2. External property managers (for leased sites)
3. Agency business owners of systems and sites
4. ICT system managers, including appropriate contracted suppliers
5. Agency/Government media liaison staff
6. Agency senior managers
7. Tasmania Police contacts, to be used if legal action is to be pursued

The following procedures are RECOMMENDED during an incident. Procedures may vary depending on the severity or classification of the incident (see Information Security Incident Classification below), including:

1. Evaluation of an incident (which may include classification of the incident)
2. Who and when to notify about the incident
3. Escalation processes
4. Record keeping requirements, including records to support possible legal action.
5. Investigation procedures
6. General criteria for when, or if, legal action will be taken

The following procedures are RECOMMENDED after an incident. Procedures may vary depending on the severity or classification of the incident, including:

1. Communication procedure upon return to normal

2. Notification procedures, including whom to contact, which may include impacted third parties, and priorities

3. Immediate prevention measures

4. Review procedures regarding the incident itself and the wider risks involved

5. Communication to other agencies of any new or emerging threats

The following procedures are RECOMMENDED to determine if and when legal action is to be pursued including:

1. Internal processes to approve referral to the Tasmania Police

2. Rules to assist in determining when incidents will be referred to the Tasmania Police

3. Procedures and rules to ensure that evidence is retained in a form suitable for investigation and prosecution

The following procedures are RECOMMENDED to determine appropriate publicity, including:

1. Visibility and impact of the incident on staff

2. Visibility and impact of the incident on services with other agencies and the public

3. Potential media interest in the incident

4. Potential political impact of the incident

7.3.4 Minor information security incidents

For minor incidents, where the preventative measures have blocked an attack, or the incident has had minimal or no impact (eg Category 1 or Category 2 incidents as classified below), the agency may elect to not apply all aspects of the security plan, or to have a minor information security incident plan.

Agencies SHOULD log minor incidents so that information can be used for future reviews of agency information security risks, mitigation strategies, and incident plans. Lack of information on minor incidents can lead to a false sense of security.

It is RECOMMENDED that periodic reviews of event or incident logging consider any change to the security environment, value of information assets or the exposure of assets. The security incident threshold, level of detail and retention requirements will influence the resources required for storage and analysis of logs.

7.3.5 Investigation and documentation

Documentation is important to assist in reviewing incidents and to support legal action. For both purposes, the documentation SHOULD be sufficiently comprehensive and precise to reconstruct the chain of events.

For documents to be used as evidence, it also needs to be clear that the documents themselves were not tampered with during or after the incident.

7.3.6 Periodic reviews and incident register

To assist in determining the level of risk and the appropriateness of mitigation strategies, agencies SHOULD maintain a register and statistics on information security incidents (see Information Security Incident Classification below on ways of classifying incidents).

7.3.7 Treasurer's instructions

Treasurer's Instructions are issued under the *Financial Management and Audit Act 1990*. Treasurer's Instructions cover the principles, practices and procedures to be observed in the financial management of all agencies. They are published on the Department of Treasury and Finance web site (http://www.treasury.tas.gov.au/).

Where applicable, the Treasurer's Instructions MUST be considered when agencies develop Information Security Incident Reporting procedures, including:

- *TI 301- Reporting procedure in cases of illegal entry and/or damage or loss of property or money*
- *TI 302- Recording of losses*

7.4 Information Security Incident Classification

The following is a RECOMMENDED information security incident severity classification scheme to be used as is, or modified by agencies to assist in developing information security incident plans and aiding in understanding risks and exposures.

To assist in future risk assessments, agencies may also consider other ways of classifying incidents, including:

- Source of the incident – external/internal
- Accidental/malicious
- Electronic, physical etc
- Location

The classification scheme outlined below is based on the Commonwealth's ISIDRAS scheme that is used to classify and report on information system security incidents (see http://www.dsd.gov.au/).

Information Security Incident Classification	
Category 1	Incidents include events which cannot be definitively identified as attacks, and have no effect on operations, such as: • False activation of intrusion detection systems (eg burglar alarms) • Isolated and non-repeated scans or 'pings' from an external uncontrolled network • Malware detected and removed prior to being placed on an operational system or network • Inappropriate content on a machine • Abuse of privileges (including computer and physical access privileges) or password confidentiality by Agency employee (not extending to superuser or root or administration privileges)
Category 2	Incidents that also have no effect on operations, and comprise identified but unsuccessful attempts to actively breach an information security policy. Such events include: • Multiple repetitions of category 1 incidents • Accidental failure to secure premises overnight • Attempt to gain unauthorised access to agency resources or premises • Repeated active probes or port mapping from an external network • Unsuccessful DOS/DDOS attempts (blocked at firewall or router) • Malware found on a single system that has been successfully contained or removed
Category 3	Incidents include any successful attempt to actively breach an information security policy, and may result in a minor or moderate effect on operations. These could include: • Unauthorised disclosure, loss, alteration or damage of information either as an accidental or malicious act • Unauthorised visitor/access by one or more people • Abuse of privileges or password confidentiality by Agency employee, extending to superuser, root or administration privileges • Malware found on more than one system, or an inability to contain and remove the code from a single system • Defacement, alteration or deletion of web server files • A successful attack against system services -eg NIS, DNS, NFS, email, WWW etc, including denial of service attacks • A prank or hoax perpetrated from an external source • Unauthorised access to a firewall • Unauthorised modification to system files and system access controls • Unauthorised modification to system hardware or software without the owner's knowledge or permission • Theft or accidental equipment loss
Category 4	Incidents include any situation in excess of the examples given above, particularly where high-level intervention or crisis management is required. Such incidents will usually have a major effect on operations.

8 Risk Management Guidelines

8.1 Purpose

This section contains minimum information security risk management policies and guidelines to be implemented by agencies to achieve appropriate information security within the Tasmanian Government.

8.2 Risk Management Policy Principles

The Incident Reporting Policy Principles in the Charter require that:

> ‘Each agency must develop and implement an Agency Information Security Plan that is appropriate to the agency’s functions and the risks that it faces.’
>
> ‘The Agency Information Security Plan needs to be monitored and reviewed to minimise information security risks.’
>
> ‘Each agency is to conduct regular information security risk assessments.’

8.3 Guidelines for implementing the Risk Management Policy Principles

Risk management is the process of conducting risk assessments and implementing the agreed mitigation strategies.

Information security risks are threats that can impact on the availability, confidentially, or integrity of information.

This document provides agencies with a consistent framework to assess information security risks. The guidelines and methodology expand on *AS/NZS 4360:2004 Risk Management*.

Agencies SHOULD conduct regular information security risk assessments covering:

- Physical security risks
- Deficiencies in personnel knowledge, training and practices
- Record security practices
- ICT security

Following the identification of risks, risk mitigation strategies and changes to agency information security policies and procedures there is some residual information security risks where the agency has:

- Elected to accept a risk by doing nothing, or
- A mitigation strategy has not completely eliminated a risk.

Residual risks SHOULD be openly stated in an agency information security plan.

To avoid duplication of effort and to facilitate the comparison of different risk assessments agencies SHOULD:

- Combine information security risk assessments with other business related risk assessments, and
- Adopt a consistent risk management framework for all risk management activities within the agency.

8.3.1 Methodology

Agencies SHOULD use *AS/NZS 4360:2004 Risk Management* as the methodology to conduct risk assessments.

Appendix 5: Information security risk management methodology expands on the Standard to provide a consistent framework for agencies to assess information security risks.

An example of an information security risk register is provided in Appendix 6 of this document.

8.3.2 Update and review of risk assessments

Risk assessments SHOULD be regularly updated and reviewed by agencies.

Updates may be initiated by minor changes to existing risks. These include changes resulting from the implementation and/or removal of a mitigation strategy, or when the effectiveness of a mitigation strategy changes. It is RECOMMENDED that risk assessments are updated when:

- Each mitigation strategy is implemented
- An incident(s) highlights a minor discrepancy in the risk register, eg likelihood or seriousness of a risk needs minor adjusting or the effectiveness of a mitigation strategy requires adjusting
- A risk is no longer applicable
- A new risk emerges

Reviews are the formal process of redeveloping the risk assessment. It is RECOMMENDED that risk assessment reviews occur:

- Annually
- After a serious information security incident that highlights issues
- When cumulative updates indicate that the risk assessment requires a review
- An event, or series of events indicate that a review is required (these could include incidents, events elsewhere, changes to business operations etc)
- Infrastructure changes, such as building and/or software upgrades
- Changed business, including legislative, requirements

9 References

9.1 Security planning, policies & governance

9.1.1 Primary references

Attorney-General's Department, 2005, *Protective Security Manual (PSM),* Protective Security Coordination Centre, Canberra.

Interdepartmental Committee on Security, 2002, *Security in the Government Sector,* Department of the Prime Minister and Cabinet, Wellington, New Zealand. Viewed February 2008, <www.security.govt.nz/sigs/index.html>.

Standards Australia International, 2006, *Information Technology: Security Techniques: Information Security Management Systems: Requirements*, (AS/NZS ISO/IEC 27001:2006), SAI, Sydney. [3]

Standards Australia International, 2006, *Information Technology: Security Techniques: Code of Practice for Information Security Management*, (AS/NZS ISO/IEC 27002:2006), SAI, Sydney. [3]

9.1.2 Secondary references

Organisation for Economic Co-operation and Development, 2002, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,* OECD, Paris.

9.2 Risk management

9.2.1 Primary references

Inter Agency Policy and Project Unit, 2005, *Tasmanian Government Project Management Guidelines,* Version 6.0 – March 2005, Inter Agency Policy and Project Unit, Department of Premier and Cabinet, Hobart, viewed February 2008, <http://www.stors.tas.gov.au/au-7-0020-00169>.

Standards Australia International, 2004, *Risk Management, (*AS/NZS 4360:2004), SAI, Sydney. [3]

Standards Australia International, 2004, *Risk Management Guidelines: Companion to AS/NZS 4360:2004: Handbook, (*HB 436:2004), SAI, Sydney. [3]

Standards Australia International, 2004, *Information Security Risk Management Guidelines,* (HB 231:2004), SAI, Sydney. [3]

9.2.2 Secondary references

HM Treasury, 2004, The Orange Book: Management of Risk: Principles and Concepts, October 2004, HMSO, Norwich. Viewed February 2008, <http://www.hm-treasury.gov.uk>.

[3] Available within the Tasmanian Government IP address domain via <http://www.egovernment.tas.gov.au/themes/interoperability/common_node/services/private/standards_select_online_service>

National Institute of Standards and Technology, 2004, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004, (FIPS PUB 199), NIST, Gaithersburg, MD. Viewed February 2008, <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

CERT, OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk-based strategic assessment and planning technique for security, Software Engineering Institute Carnegie Mellon University, Pittsburgh, PA. Viewed February 2008, <http://www.cert.org/octave/ >.

9.3 General ICT

9.3.1 Primary references

Defence Signals Directorate, 2007, *Australian Government Information Technology Security Manual*: *ACSI 33*, September 2007, Australian Government, Canberra. Viewed February 2008, <http://www.dsd.gov.au/_lib/pdf_doc/acsi33/acsi33_u_0907.pdf>.

Standards Australia International, 2006, *Information Technology: Security Techniques: Code of Practice for Information Security Management*, (AS/NZS ISO/IEC 27002:2006), SAI, Sydney.[4]

9.3.2 Secondary references

AusCERT: Australian Computer Emergency Response Team, University of Queensland, Brisbane. Viewed February 2008, <http://www.auscert.org.au/>.

Australian Government Information Management Office, *Authentication*, Australian Government, Canberra. Viewed February 2008, <http://www.agimo.gov.au/infrastructure/authentication> (Contains useful information on authenticating external customers over the Internet. Content is aimed at Federal government agencies, and covers the authentication options, including user IDs, one time tokens, PKI and identification issues).

Australian Government Information Management Office, *Online Security,* Australian Government, Canberra. Viewed February 2008, <http://www.agimo.gov.au/infrastructure/government> (Contains useful general information on security).

Attorney-General's Department, 2005, *Protective Security Manual (PSM),* Protective Security Coordination Centre, Canberra.

National Institute of Standards and Technology, Computer Security Resource Center, NIST, Gaithersburg, MD. Viewed February 2008 <http://csrc.nist.gov/> (Contains useful guides and publications relating to IT security).

INFOSEC: Defence Signals Directorate, Information Security Group, Australian Government, Canberra. Viewed February 2008, <http://www.dsd.gov.au/infosec/> (Contains useful publications including a DSD security advisory: *Cookies Providing Automated Access*; and INFOSEC policy documents: *The Security of Electronic Payment Systems*, and *DSD Security Policy Advisory on the use of SSL*).

[4] Available within the Tasmanian Government IP address domain via <http://www.egovernment.tas.gov.au/themes/interoperability/common_node/services/private/standards_select_online_service>

National Institute of Standards and Technology, *National Vulnerability Database,* NIST, Gaithersburg, MD. Viewed February 2008, <http://www.nvd.nist.gov/> (A searchable index of information on computer vulnerabilities and patch information).

ISACA: Information Systems Audit and Control Association, Rolling Meadows, Illinois, access to resources on Control Objectives for Information and related Technology (COBIT). Viewed February 2008, <http://www.isaca.org/cobit>.

International Organization for Standardization, 2004, *Information Technology: Security Techniques: Management of Information and Communications Technology Security: Part 1: Concepts and Models for Information and Communications Technology Security Management*, (ISO/IEC 13335-1:2004), IOS, Geneva.

International Organization for Standardization, 1998, *Information Technology: Guidelines for the Management of IT Security: Part 2: Managing and Planning IT Security (*ISO/IEC TR 13335-2:1998), IOS, Geneva.

International Organization for Standardization, 1998, *Information Technology: Guidelines for the Management of IT Security: Part 3: Techniques for the Managing of IT Security (*ISO/IEC TR 13335-3:1998), IOS, Geneva.

International Organization for Standardization, 2000, *Information Technology: Guidelines for the Management of IT Security: Part 4: Selection of Safeguards, (*ISO/IEC TR 13335-4:2000), IOS, Geneva.

International Organization for Standardization, 2000, *Information Technology: Guidelines for the Management of IT Security: Part 5: Management Guidance on Network Security (*ISO/IEC TR 13335-5:2001), IOS, Geneva.

Open Web Application Security Project (OWASP). Viewed February 2008, <http://www.owasp.org> (Includes a guide on building secure web applications).

Standards Australia International, 2004, *Information Security Risk Management Guidelines,* (HB 231:2004), SAI, Sydney.[5]

Standards Australia International, 2001, *Organisational Experiences in Implementing Information Security Management Systems, (*HB 248:2001), SAI, Sydney.

United States National Security Agency. Viewed February 2008, <http://www.nsa.gov/>. (Contains useful information and guides on computer security, including configuration guides).

US-CERT: United States Computer Emergency Readiness Team, Washington, DC. Viewed February 2008, < http://www.us-cert.gov>.

PCI Security Standards Council: Payment Card Industry Security Standards Council, Delaware. Viewed February 2008, <https://www.pcisecuritystandards.org> (Standards for the protection of payment account information).

[5] Available within the Tasmanian Government IP address domain via <http://www.egovernment.tas.gov.au/themes/interoperability/common_node/services/private/standards_select_online_service>

9.4 Record security

9.4.1 Primary references

Archives Office of Tasmania, *State Records, Guidelines and Recordkeeping Advices*, Hobart, viewed February 2008, <http://www.archives.tas.gov.au/legislative/staterecords>.

Standards Australia International, 2002, *Records management: Part 1: General, (*AS ISO 15489.1:2002), SAI, Sydney.[6]

Standards Australia International, 2002, *Records management: Part 2: Guidelines,* (AS ISO 15489.2:2002), SAI, Sydney.[6]

9.4.2 Secondary references

Attorney-General's Department, 2005, *Protective Security Manual (PSM), Part C: Information Security,* Protective Security Coordination Centre, Canberra.

Interdepartmental Committee on Security, 2002, *Security in the Government Sector,* Department of the Prime Minister and Cabinet, Wellington, NZ, viewed February 2008, <www.security.govt.nz/sigs/index.html>.

9.5 Incident reporting

Standards Australia International, 2006, Information Technology: Security Techniques: Information Security Incident Management, (AS/NZS ISO/IEC 18044: 2006), SAI, Sydney.[6]

Standards Australia International, 2003, Guidelines for the Management of IT Evidence, (HB 171-2003), SAI, Sydney.

[6] Available within the Tasmanian Government IP address domain via <http://www.egovernment.tas.gov.au/themes/interoperability/common_node/services/private/standards_select_online_service>

10 Document revision history

Date	Section	Version Change	Update
May 2009	All	4.0 to 4.1	Updated with redesignation of AS/NZ ISO/IEC 17799:2006 to AS/NZ ISO/IEC 27002:2006.
Feb 2008	All	3.0 to 4.0	Previously separate sections combined into a single document. Incorporation of AS 17799:2006. Introduction of keywords for requirements
	1. Introduction		Complete rewrite.
	2. Information Security Governance Guidelines		Incorporated AS 27001:2006.
	3. Record Security Guidelines		Addition of: *Personal Information Protection Act 2004*.
	4. Physical Security Guidelines		See update for all sections.
	5. Personnel Security Guidelines		Added control regarding personnel with privileged access to resources.
	6. General ICT Guidelines		Added controls and recommended actions regarding privileged access and cross agency access controls
	7. Incident Management Guidelines		Name of section changed from Incident Reporting Guidelines. A Category 3 incident includes alteration of web server files. New recommended actions.
	8. Risk Management Guidelines		Methodology and example risk register moved to appendices.
	Appendices		Appendices on risk management methodology and risk register were previously in the Risk Management Guidelines Section. Added Monitor and Review section to Appendix 5 Information security risk management methodology.
Nov 2005	1. Agency Information Security: General ICT	2.0 to 3.0	Minor revisions relating to wireless networks. Added note that ACSI 33 may be updated twice a year.

Date	Section	Version Change	Update
	2. Information Security: Risk Management Guidelines	1.0 to 2.0	Clarify that agencies should consider a consistent risk management methodology for all business risk assessments. Rewrite to become a guide on how to apply AS/NZS 4360:2004 : Risk Management Ensure consistency with the Risk Management section of the Project Management Guidelines Incorporate US publication Standards for Security Categorization of Federal Information and Information Systems as a guide in establishing the Risk Context
Sep 2004	3. Agency Information Security: Physical Security Guidelines	1.0 to 2.0	Added section 'Mail and Other Deliveries'
	4. Agency Information Security: General ICT	1.0 to 2.0	Update all references to 2004 release of ACSI 33. Minor changes to Media Handling and Security (disposal of media) guidelines regarding: Replacement of media via warranty or maintenance contracts Treasurer's Instructions Photocopiers. Added the direct application of AS/NZS 17799 as an alternate set of Guidelines.
	5. Agency Information Security: Incident Reporting	1.0 to 2.0	Add section highlighting Treasurer's Instructions
Feb 2003	All Sections	Draft to 1.0	Initial Release.

This page is intentionally blank.

11 Appendices

Appendix 1: Glossary of terms

AusCert	Australian Computer Emergency Response Team, mission is to support and improve community awareness, representation and communication regarding computer security, both locally and internationally, by being the leading source of impartial and reliable computer security information and expertise for the members. Funded by subscription and some federal funding. Part of The University of Queensland. www.auscert.org.au.
CERT	Computer Emergency Response Team, US Federally funded organisation, a centre of Internet security expertise. www.cert.org.
COBIT	An information technology governance framework and supporting toolset that seeks to bridge the gap between control requirements, technical issues and business risks. It emphasizes regulatory compliance, helps organizations to increase the value attained from information technology an enables alignment with business needs.
DSD	Defence Signals Directorate.
IAPPU	Inter Agency Policy & Projects Unit of the Department of Premier & Cabinet.
IASC	Inter Agency Steering Committee of the Tasmanian Government.
ICT	Information and communication technology, covers both information technology and communications technology.
Information security risks	Threats to information held or required by the organisation that can impact on one or more the following to the information: • Availability • Confidentiality • Integrity
ISIDRAS	The Information Security Incident Detection, Reporting and Analysis Scheme has been established by the Department of Defence, Defence Signals Directorate to collect information on security incidents which affect the security or functionality of Australian Commonwealth Government computer and communication systems.
LAN	Local Area Network, computer network that spans a relatively small area, normally confined to a single building.
LGAT	Local Government Association of Tasmania.
NT, NTII	Networking Tasmania, the Tasmanian Government's outsourced computer network services contract, administered by TMD.
PSCC	Protective Security Coordination Centre supports the Attorney-General and the Minister for Justice and Customs by providing policy advice and implementing government decisions in the field of protective security. This includes security awareness activities and education through training programs on physical, computer and personnel security, and the production, marketing and maintenance of the Protective Security Manual.
PSM	Commonwealth's Protective Security Manual, sets out policies, practices and procedures on protective security. The policy is mandatory for all Commonwealth agencies.
PSPC	Protective Security Policy Committee, Commonwealth committee, chaired and coordinated by Commonwealth Attorney General's Department, coordinates protective security within the Commonwealth.

TMD	A division of the Department of Premier and Cabinet and provides: • telecommunications & computing services to Agencies including Human Resource and Finance Systems Management • manages the Networking Tasmania Contract on behalf of the Tasmanian State Government • advice to Government and Agencies on telecommunications and information technology issues • manages appropriate technical standards • whole-of-government infrastructure project support.
WAN	Wide Area Network, computer network that spans a relatively large geographical area.

Appendix 2: Agency obligations under the Archives Act 1983

Below is a brief summary of the important aspects of the *Archives Act 1993* (the Act), as it relates to agency operations generally and the obligations of officers in all agencies.

Detailed guidelines for the Disposal of State Records are available at: http://www.archives.tas.gov.au/.

Section 3 - (1) of the Act defines a 'record' as meaning: '...a document or an object that is, or has been, made or kept by reason of any information or matter that it contains or can be obtained from it or by reason of its connection with any event person, circumstance, or thing;'

Section 3 - (5) states that ' Without limiting the generality of the definition of the expression 'record' in subsection (1) - (a) the reference to a document in that definition includes a reference to any printed or written material; and (b) the reference to a sound recording, coded storage device, magnetic tape or disc, microfilm, photograph, film, map, plan, or model or painting or other pictorial or graphic work.' The above definition clearly encompasses computer and other electronic records stored on a coded device. The device could be hard or floppy disc.

Section 10 of the Act deals with the preservation and acquisition of State and other records. It states that records made for the purpose or in connection with the administration of a Government department or authority must be preserved until dealt with by the Act.

Section 11 of the Act deals with the transfer of State records to the Archives Office. This section states that when a record ceases to be used or referred to by an agency, or required to be available for public use, that record must be transferred to the Archives Office. Records in existence for 25 years, unless exempted by writing, must be deposited in the Archives Office.

Section 15 of the Act deals with the ability of a Head of Agency to restrict access to records that have been transferred to the Archives Office (except for Cabinet records or records of the Executive Council which have specific access restrictions applied under the provisions of the act). It is implicit within the legislation that access to records will be un-restricted unless a restriction is specified by the Head of Agency at the time of transfer. A Head of Agency may restrict access for given periods of time and/or restrict access to specific groups of users. Access to records may not be restricted for more than 75 years after the making of the record.

Section 20 of the Act deals with the disposal and destruction of records held by agencies. Section 20 - (1) states that persons must not destroy records in their possession. A person who contravenes this section is subject to financial penalty.

Section 20 - (5) states that a record used by means of any mechanical or electronic device or equipment, including a computer, a record if treated or modified in such a way that would prevent information being obtained, will be deemed to be destruction of the record.

Appendix 3: State Service Principles

Section 7 (1) of *State Service Act 2000*.

(a) the State Service is apolitical, performing its functions in an impartial, ethical and professional manner;

(b) the State Service is a public service in which employment decisions are based on merit;

(c) the State Service provides a workplace that is free from discrimination and recognises and utilises the diversity of the community it serves;

(d) the State Service is accountable for its actions and performance, within the framework of Ministerial responsibility, to the Government, the Parliament and the community;

(e) the State Service is responsive to the Government in providing honest, comprehensive, accurate and timely advice and in implementing the Government's policies and programs;

(f) the State Service delivers services fairly and impartially to the community;

(g) the State Service develops leadership of the highest quality;

(h) the State Service establishes workplace practices that encourage communication, consultation, cooperation and input from employees on matters that affect their work and workplace;

(i) the State Service provides a fair, flexible, safe and rewarding workplace;

(j) the State Service focuses on managing its performance and achieving results;

(k) the State Service promotes equity in employment;

(l) the State Service provides a reasonable opportunity to members of the community to apply for State Service employment;

(m) the State Service provides a fair system of review of decisions taken in respect of employees.

Appendix 4: State Service Code of Conduct

Section 9 of *State Service Act 2000*.

1. An employee must behave honestly and with integrity in the course of State Service employment.
2. An employee must act with care and diligence in the course of State Service employment.
3. An employee, when acting in the course of State Service employment, must treat everyone with respect and without harassment, victimisation or discrimination.
4. An employee, when acting in the course of State Service employment, must comply with all applicable Australian law.
5. For the purpose of subsection (4), 'Australian law' means –

   (a) any Act (including this Act) or any instrument made under an Act; or

   (b) any law of the Commonwealth or a State or Territory, including any instrument made under such a law.

6. An employee must comply with any standing orders made under section 34(2) and with any lawful and reasonable direction given by a person having authority to give the direction.
7. An employee must maintain appropriate confidentiality about dealings of, and information acquired by, the employee in the course of that employee's State Service employment.
8. An employee must disclose, and take reasonable steps to avoid, any conflict of interest in connection with the employee's State Service employment.
9. An employee must use Tasmanian Government resources in a proper manner.
10. An employee must not knowingly provide false or misleading information in connection with the employee's State Service employment.
11. An employee must not make improper use of –

    (a) information gained in the course of his or her employment; or

    (b) the employee's duties, status, power or authority –

    in order to gain, or seek to gain, a gift, benefit or advantage for the employee or for any other person.

12. An employee who receives a gift in the course of his or her employment or in relation to his or her employment must declare that gift as prescribed by the regulations.
13. An employee, when acting in the course of State Service employment, must behave in a way that upholds the State Service Principles.
14. An employee must at all times behave in a way that does not adversely affect the integrity and good reputation of the State Service.
15. An employee must comply with any other conduct requirement that is prescribed by the regulations.

Appendix 5: Information security risk management methodology

Risk management is the process of conducting risk assessments and implementing the agreed mitigation strategies. The risk assessment process consists of the following stages:

1. Communication and consultation
2. Establishing the context
3. Identifying the risks
4. Analysing the risks
5. Evaluate risks
6. Treat the risks
7. Monitor and Review

Documentation that is developed is to be retained at all stages of the process.

5.1 Communication and consultation

Communication and consultation with stakeholders are important considerations as part of the risk management process.

Appropriate communication and consultation seeks to:

- Improve understanding of risks and the risk management process
- Ensure that the varied views of stakeholders are considered
- Ensure that all participants are aware of their roles and responsibilities

HB 436:2004 *Risk Management Guidelines - Companion to AS/NZS 4360* expands on the communication and consultation process and how it adds value to risk management.

5.2 Establishing the context

The risk management context summarises how the risk assessment fits within the organisation's strategic and organisational environment.

The following steps are a guide to establishing the risk assessment context:

Step	Context	Answer these questions
1	Risk management	Who is going to conduct the risk assessment? What are the objectives of this risk assessment? What are the boundaries for this risk assessment?
2	Strategic	What are the strengths and weaknesses? What are the priorities? Who are the stakeholders? What are the major threats and opportunities? What are the external drivers?
3	Organisational	What are the objectives/purposes of the information asset or system? What are the internal drivers? What is the key to the success? Are there shared risks with other agencies or organisations? What resources are available? How does the information asset or system contribute to the agency's wider goals and priorities?
4	Evaluation Criteria	Are there legal requirements? What kinds of consequences will be considered? What are the financial, human resources, operational implications? How will likelihood be defined? How will it be determined if a risk level requires further treatment? What are the costs and benefits of actions? What level of risk is acceptable?
5	Structure	What are the assets types involved? How are the assets to be used? What are the phases (time) or elements (structure) of any activities?

The context statement is to be incorporated into the agency's information security plan.

The risk context statements for the agency information security risk assessment is to be consist with, or may be same as, the context statement for the agency's general risk assessment. In particular, to facilitate the consistent management of major risks of an agency it is highly desirable to single approach to determining and grading of likelihood, consequence, and risk levels for all risk assessments conducted by the agency. Section 11 of *HB 436:2004, Risk Management Guidelines - Companion to AS/NZS 4360* describes one approach to establishing an agency wide risk management policy.

5.2.1 Identifying the risks

For each asset identified in Step 5 in the establishment of the Context, identify all possible risks, or classes of risks and record:

1. What the risk is

2. How it can occur

3. The consequences of the risk occurring

5.2.2 Analysing the risks

The aim of analysing the risks is to:

1. Separate the acceptable risks from the unacceptable risks
2. Prioritise the risks
3. Provide information for the evaluation and mitigation of risks

This is achieved by:

1. Determining the consequences if the risk eventuates
2. Determining the likelihood of the risk occurring, including documenting how this was estimated
3. Determining the overall level of the risk by combining the consequences and likelihood

5.2.3 Consequence rating

The following table describes a suggested five level consequences rating model. If appropriate, agencies may adopt a four or three level consequences rating model. Agencies may develop a standard consequence-rating model for all risk assessments conducted within the agency.

Grade	Rating	Description
E	Catastrophic	The loss of confidentiality, integrity, or availability could be expected to have a catastrophic adverse effect on government operations, assets or individuals, such as: • The inability of the government to perform one or more of its major functions • Catastrophic damage to assets • Catastrophic financial loss • Severe harm to many individuals involving loss of life or serious life threatening injuries • Ministerial or Cabinet intervention will be required
H	High	The loss of confidentiality, integrity, or availability could be expected to have a severe or major adverse effect on agency operations, assets or individuals, such as: • The inability of the agency to perform one or more of its functions • Major damage to organisational assets • Major financial loss • Severe harm to individuals involving loss of life or serious life threatening injuries • Major public loss in confidence of the agency to perform its functions • Top-level management or ministerial intervention would be required

Grade	Rating	Description
M	Moderate	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on agency operations, assets or individuals, such as: • Significant degradation of the capability of the agency to perform one or more of its functions • Significant damage to organisational assets • Significant financial loss • Significant harm to individuals • Significant public loss in confidence of the agency to perform its functions • Moderate loss of confidence in the agency to perform one or some of its functions
L	Low	The loss of confidentiality, integrity, or availability could be expected to have a low adverse effect on agency operations, assets or individuals, such as: • Degradation of the capability (ie efficiency or effectiveness) of the agency to perform one or more of its functions • Minor damage to organisational assets • Minor financial loss • Minor harm to individuals • Minor public loss in confidence of the agency to perform its functions
N	Insignificant	Insignificant impact on confidentiality, integrity or availability that is dealt with by routine operations.

HB 436:2004, Risk Management Guidelines - Companion to AS/NZS 4360 has further examples of approaches to measuring or rating consequences that include other types of consequences, such as social/cultural heritage.

5.2.4 Likelihood determination

The following table describes a suggested five level likelihood rating. If appropriate, agencies may adopt a four or three level likelihood determination model. Agencies may develop a standard likelihood determination model for all risk assessments conducted within the agency.

Grade	Rating	Description
E	Almost certain	The risk would be expected to eventuate at regular frequent intervals – eg several times a year.
H	Likely	The risk will probably occur in most circumstances.
M	Possible	The risk might eventuate at some time and may have a number of external influences – eg possibly once every one or two years.
L	Unlikely	The risk could eventuate some time – eg may occur once every 5 or so years.
N	Rare	The risk may eventuate, but only in exceptional circumstances.

HB 436:2004 *Risk Management Guidelines - Companion to AS/NZS 4360* has further examples of approaches to measuring or rating likelihood.

5.2.5 Risk matrix

The table below describes a suggested rating for risk level. The ratings are used in the risk matrix. Agencies may develop a standard risk level model for all risk assessments conducted within the agency.

Level	Rating	Description
E	Extreme	Requires detailed research, management and planning at executive level.
H	High	Requires senior management attention.
M	Moderate	Can be managed by specific monitoring or response procedures.
L	Low	Can be managed by routine procedures.

The matrix below is a guide in determining risk level based on the likelihood and consequence of each risk. Agencies may develop a standard risk matrix for all risk assessments conducted within the agency.

Likelihood	**Consequences**				
	E Catastrophic	**H High**	**M Moderate**	**L Low**	**N Insignificant**
E – Almost Certain	E – Extreme	E – Extreme	E – Extreme	H – High	M – Moderate
H –Likely	E – Extreme	E – Extreme	H – High	H – High	M – Moderate
M – Possible	E – Extreme	E – Extreme	H – High	M – Moderate	L – Low
L – Unlikely	E – Extreme	H – High	M – Moderate	L – Low	L – Low
N – Rare	H – High	H – High	M – Moderate	L – Low	L – Low

HB 436:2004 Risk Management Guidelines - Companion to AS/NZS 4360 has further examples of approaches to measuring or rating levels of risks.

Risk Level rating change – since last risk assessment:

Change to Grade since last assessment			
New	New risk	↑	Grading increased
–	No change to grade	↓	Grading decreased

5.2.6 Evaluate risks

The evaluation of the risks is to prioritise the risks that are to be addressed by treatment or mitigation plans. This is done by assessing the level of risk against:

1. Predetermined standards
2. Target risk levels
3. Other criteria

The process to achieve this is:

1. Documenting the predetermined standards, target risk levels and/or other criteria that determine what is an acceptable or unacceptable risk

2. Assessing each risk against the criteria documented in step 1 to determine whether the risk is acceptable or unacceptable, and recording where a risk is acceptable

3. Using the criteria documented in step 1, prioritise the unacceptable risks, and recording the priority

HB 436:2004 Risk Management Guidelines - Companion to AS/NZS 4360 has further information on risk evaluation.

5.2.7 Treat the risks

For each of the unacceptable risks identified above, mitigation options must be developed to either (or both) reduce the:

- Likelihood of the risk occurring.

- Consequences if the risk does eventuate

A number of general strategies can be used to achieve this; possibilities include:

- Changing procedures or the business model to avoid the risk altogether (eg change premises)

- Implement changed or new procedures that will reduce the chances of the risk occurring and may also reduce the consequences if the risk does occur

- Purchase products or services that will reduce the chances of the risk occurring and may also reduce the consequences if the risk does occur

Many risk management guides discuss the option of transferring a risk. Strictly speaking this is only possible if the ownership and responsibility of the business function is transferred.

The steps to develop and determine the appropriate risk mitigation options or controls are to:

1. Consolidate the unacceptable identified risks in priority order

2. Develop one or more appropriate options, or controls, for each risk

3. Summarise the costs and benefits of each control and hence determine the viable controls, accept or reject each identified control

4. Calculate the residual risk taking into consideration the effect of the accepted controls (see Analysing the risks above)

5. Assess the residual risk (see Evaluate risks above)

6. Record the accepted controls, seek formal approval to implement the controls, including determining implementation responsibilities, timetable and monitoring

Mitigation costs are an estimate of the capital (initial outlays to implement the strategy, is generally required for all preventative mitigations and many contingent mitigations), recurrent (outlays to maintain the mitigation plan) and contingent (estimate of costs to activate the mitigation plan, including recovery plans, if the event occurs) costs. For some risks, these may be difficult to estimate, or they may be a marginal cost only. For others, it may be a real zero dollar cost.

HB 436:2004 Risk Management Guidelines - Companion to AS/NZS 4360 has further information on treating risks.

5.2.8 Monitor and Review

Ongoing monitoring and review of risk management processes ensures that the management plan is relevant. Factors that may impact on the relevance of an established plan include:

- Changes to the organisation context or objectives
- The environment in which an organisation operates eg emergence of new threats
- Changes to known risks and levels of risk
- The effectiveness of risk treatments
- Post event analysis eg learn from success, failure or near misses

HB 436:2004 Risk Management Guidelines - Companion to AS/NZS 4360 has further information on monitoring and review of risks.

5.2.9 Documentation

The information security risk assessment process will result in updates to the Agency Information Security Plan and the Risk Register.

The Agency Information Security Plan ought to include:

- The risk context statement (either explicitly or implicitly)
- A summary of the risk register consisting of at least –
    - The unacceptable risks
    - Identified controls
    - Implementation plans for each identified control

The Risk Register summarises the risk assessment process and ought to include:

- The risk context statement
- The model used for the risk analysis, including:
    - Consequence ratings
    - Likelihood ratings

    - Risk matrix
    - Method to determine acceptable and unacceptable risks
- Risk treatment analysis (including rejected controls)
- Risk register table

Appendix 6: Example information security risk register

6.1 Risk context

Document the Risk Context, see Appendix 5.2 Establishing the context for guidance on completing this section.

6.2 Ratings & matrix

Tables that outline the classification of consequences, likelihood, risk level ratings and risk matrix are included here. The guidelines provided in the sections above may be altered to suit the particular purposes.

6.3 Determination of unacceptable & acceptable risks

Describe the criteria for determining which risks are acceptable or unacceptable. At a minimum this should be based on the Risk Level. Other criteria may also be used and these must be documented.

The following is an example only, and is incomplete and unverified. It is for a hypothetical Human Resources (HR) Branch, including its associated business systems. Actioned mitigation strategies may result in a formal project and/or other supporting documentation.

6.4 Risks – pre-mitigation actions

Risk ID	Description of Risk and Consequences	Likelihood	Seriousness	Grade	Change	Mitigation Action & ID	Responsible Officer
1	Unauthorised access of workplace during working hours resulting in theft of equipment (laptops), money, unauthorised disclosure of documents. Consequences – in serious case, loss of equipment and/or unauthorised disclosure of personal information.	H	L	H	New	Identified: 1 – Install more secure reception counter. 2 – Train staff in security procedures. 3 – Install screen saver passwords.	HR manager / IT Manager
2	Break-in, burglary after hours. Consequences – in serious case, loss of equipment and/or unauthorised disclosure of personal information.	M	M	H	New	Existing locks etc deemed adequate. Identified: 2 – Train staff in security procedures.	HR Manager
3	Unavailability of systems because access to suitable office is denied during critical pay run period, but HR system still available. Consequence – worst case, late pay run.	L	E	E	New	Identified: 4 – Arrange access from alternate site.	HR Manager / IT Manager
4	Unavailability of systems due to system failure during critical pay run period. Consequence – worst case late pay run.	M	E	E	New	Identified: 5 – Arrange ability to use last pay-run outputs. 6 – Arrange access to a cold site.	HR Manager / IT Manager

6.5 Mitigation actions

Mitigation Action ID	Description of Mitigation Action	Capital Cost	Recurrent Cost	Contingency Cost	Responsible Officer
1	Install more secure reception counter.	~$15,000	Marginal	N/A	HR Manager
2	Train staff in security procedures – questioning visitors, securing documents etc.	Marginal	Marginal	N/A	HR Manager
3	Install screen saver passwords	Marginal	N/A	N/A	IT Manager
4	Arrange access to HR systems from alternate site. Use existing Agency site, however will have to install some extra equipment & purchase some extra licences.	~$20,000	$2,000	$5,000	HR Manger / IT Manager
5	Arrange ability to use last pay-run outputs. Requires storing key information offsite and arrangements with banks.	~$5,000	$1,000	$20,000	HR Manger / IT Manager
6	Arrange access to a cold site. Requires buying service and testing each year.	$5,000	$20,000	$10,000	HR Manger / IT Manager

6.6 Risks – post-mitigation actions

Risk ID	Description of Risk	Likelihood	Seriousness	Grade	Change	Mitigation Action & ID	Responsible Officer
1	Unauthorised access of workplace during working hours resulting in theft of equipment (laptops), money, unauthorised disclosure of documents. Consequences – in serious case, loss of equipment and/or unauthorised disclosure of personal information.	M	L	M	↓	Implemented: 1 – Install more secure reception counter. 2 – Train staff in security procedures. 3 – Install screen saver passwords.	HR manager / IT Manger
2	Break-in, burglary after hours. Consequences – in serious case, loss of equipment and/or unauthorised disclosure of personal information.	M	L	M	↓	Existing locks etc deemed adequate. Implemented: 2 – Train staff in security procedures.	HR manager
3	Unavailability of systems because access to suitable office is	L	L	L	↓	Implemented:	HR Manager / IT

Risk ID	Description of Risk	Likelihood	Seriousness	Grade	Change	Mitigation Action & ID	Responsible Officer
	denied during critical pay run period, but HR system still available. Consequence – worst case, late pay run.					4 – Arrange access from alternate site.	Manager
4	Unavailability of systems due to system failure during critical pay run period. Consequence – worst case late pay run.	M	M	H	↓	Implemented: 5 – Arrange ability to use last pay-run outputs. Identified, not actioned: 6 – Arrange access to a cold site.	HR Manager / IT Manager

Tasmania
Explore the possibilities

Inter Agency Policy and Projects Unit
Department of Premier and Cabinet

Post: GPO Box 123
Hobart TAS 7001
Phone: 03 6232 7633
Email: iappu.enquiries@dpac.tas.gov.au
Web: www.egovernment.tas.gov.au

Published July 2009
ISBN 978 0 7246 5585 9
© State of Tasmania