TAHO
Tasmanian Archive + Heritage Office

Template Information Security Policy

This template details the mandatory clauses which must be included in an agency's Information Security Policy as per the requirements of the WoG Information Security Policy Manual. In addition, this document also provides context to the mandatory clauses by structuring them within an example Information Security policy, with additional guidance provided on other issues which agencies may wish to consider when developing their policies.

An agency's Information Security policy provides governance for information security management, and direction & support within the agency. The development and approval of an agency's information security policy not only establishes management commitment and governance arrangements, but defines the agency's policy in all aspects of information security, including asset management, human resource management and compliance.

Template Structure

The Whole of Government Information Security Policy Manual will be referred to in this template as 'the manual'.

The manual and supporting Procedures contain mandatory and recommended statements. Terminology is used as follows to indicate whether a Policy or Procedure statement is mandatory, conditional or recommended.

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 item is encouraged or suggested.

'MUST' and 'MUST NOT' statements are highlighted in red throughout this template. Agencies deviating from these MUST advise the Agency ICT Reference Group of the decision to waive particular requirements. Agencies deviating from a 'SHOULD' or 'SHOULD NOT' statement MUST record:

- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- the date at which the decision will be reviewed, and
- whether the deviation has management approval.

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

Department of Education
LINC Tasmania

Tasmania
Explore the possibilities

In this template the mandatory clauses are in red text. Following the mandatory clauses are the non-mandatory clauses as listed in the manual. These are the clauses indicated by the manual that are conditional or recommended, which are suggestions for agencies to consider for inclusion within their own policy. These clauses are listed in green text.

In addition, agencies are encouraged to add more information and policy statements to ensure all their information security and business requirements are met. Information for agencies to consider is highlighted in *blue* text.

Examples are as follows:

Tasmanian Government Mandatory Clauses

This is a mandatory clause and cannot be altered or deleted.

This policy was approved on [*blue italic text indicates where agencies can insert free text eg. dates*]

Agency Clauses

This is a recommended clause and can be altered or deleted.

[*Insert agency specific clauses*].

Agencies should also consider the following:

xxx

xxx

Tasmanian Government Non-Mandatory Clauses

Clauses listed in the Tasmanian Government Information Security policy where statement is suggested, conditional or recommended.

There are also additional sections in the manual that agencies might like to consider incorporating in their policy framework.

In addition, under section 1.1 Information Security Policy – Obligations, there is listed a number of mandatory quality criteria. While these are not mandatory clauses and do not have to be included within the agency's Information Security Policy, they are still activities which agencies must undertake to ensure their Information Security Policy is effective. The mandatory quality criteria are highlighted in red text, an example of which follows:

Mandatory Quality Criteria:

xxx

Agencies are strongly recommended to use this document as a basis/template for their Information Security Policy. As can be seen from the above, agency specific policy statements can be added and the blue text/grey box can be deleted.

Note that the Tasmanian Government Information Security Policy describes requirements at a very high level, and does not include a great deal of detailed advice about the specific policies agencies should implement.

This advice includes details of suggested policy areas that agencies can pick and choose to include in their own framework, depending upon the agency's greatest area of risk.

Information Security Policy Structure

The first section of the agency's information security policy should detail general information about the overall objective of the policy, the scope, who it applies to, legislative obligations, and who is responsible for review and approval of the policy. The sections following this introduction detail the policy requirements structured in line with Tasmanian Government Information Security Policy Manual.

The structure of the policy is at the agency's discretion. Agencies may wish to develop one single Information Security policy document. Alternatively, agencies may choose to develop an overarching broad policy that covers strategic intent at a portfolio or agency level, with each subordinate agency/functional domain having consistent but tailored specific information security policy statements. For example:

High Level Policy – A brief document that sets the strategic directions for security and assigns the broad responsibility for security within the agency.

Guidelines – Document/s that address specific information security issues. Ideally, agencies should document guidelines for each of the mandatory requirements of the Tasmanian Government Information Security Policy Manual.

Technical Standards – These documents deal with general issues and system specifics.

Procedures – Operational documents that enable compliance with the policies and include the technical details and operational specifications, practices and tasks. For example this could include work instructions, guidelines, templates, reports, checklists, assessments and plans.

See Tables 1.5 and 1.5.1 which suggest a possible structure for agencies to follow.

Information Security Policy

The Information Security policy includes all aspects of management direction and support for information security in accordance with business, legislation and regulatory requirements. Activities will include policy around compliance, but actual compliance actions should be mapped to compliance management (refer section 11).

The following sections detail the mandatory clauses, mandatory quality criteria, and suggested headings and information for agency consideration, when developing the introduction of the agency's Information Security policy.

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email gisu@education.tas.gov.au

Acknowledgements

- Queensland Government Information Security – Mandatory Clauses, Queensland Government ICT Policy and Coordination Office, Department of Public Works
- Tasmanian Government Information Security Policy Manual
- Thanks to Angela Males and the Department of Police and Emergency Management for use of Policy framework tables

Information security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History

Build Status

Version	Date	Author	Reason	Sections
1.0	November 2013	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
		This is the first release of this document.

Issued: November 2013

Ross Latham
State Archivist

Department Name

Information Security Policy

Date Released

Table of Contents

1. **Introduction 8**
1.1 Policy Statement........ 8
1.2 Scope 8
1.3 Objectives........ 8
1.4 Obligations 8
1.5 Information Security Policy Framework Structure 9
1.5.1 Information security policy categories........ 10
1.5.2 Information Security Policy and Related Framework Elements........ 12
1.6 Implementation........ 13
1.7 Policy Owner/Enquiries........ 13
1.8 Policy Approval........ 13
1.9 Policy Review 13

2. **Information Security Governance and Management 14**
2.1 External Party Governance........ 15
2.2 Information Security Plan........ 15
2.3 Information Security Risk Management 15

3. **Resource Management 17**
3.1 Record Security........ 17
3.2 Information Security Classification........ 17
3.3 Information Asset Register 18

4. **Physical Environment Security 19**
4.1 Physical Environmental Controls 19

5. **Information and Communications Technology........ 26**
5.1 Operational Procedures and Responsibilities 26
5.2 Third Party Service Delivery 26
5.3 Capacity Planning and System Acceptance........ 27
5.4 Backup Procedures 27
5.5 Network Security 28
5.6 Information Technology Media Management........ 28
5.7 Electronic Information Transfer -........ 29
5.8 eCommerce........ 29
5.9 Security Audit Logging........ 30
5.10 Malicious and Mobile Code Control 30

6. **Identity and Access Management 32**
6.1 Access Control Policy........ 32
6.2 Authentication........ 32
6.3 Access Control 33
6.4 User access........ 33
6.5 User Responsibilities 33
6.6 Network Access........ 34
6.7 Operating System Access 34

6.8 Application and Information Access ... 35
6.9 Mobile Computing and Telework Access ... 35

7. 7. Information System Acquisition Development and Maintenance ... 37
7.1 System Security Requirements ... 37
7.2 Correct Processing ... 38
7.3 Cryptographic Protocols ... 38
7.4 System Files ... 38
7.5 Secure Development and Support Processes ... 39
7.6 Technical Vulnerability Management ... 39

8. Personnel and Awareness ... 41
8.1 Personnel Procedures ... 41
8.2 Prior to Engagement ... 41
8.3 Assigning Personnel Responsibilities for Information Security – During Employment ... 42
8.4 Post-employment ... 43

9. Incident Management ... 44
9.1 Incident Management Controls ... 44
9.2 Planning for Information Security Incidents ... 45

10. Business Continuity Management ... 46
10.1 Business Continuity ... 46
10 2 ICT Disaster Recovery ... 46

11. Monitoring for Compliance ... 48
11.1 Legal Requirements ... 48
11.2 Policy Requirements ... 48
11.3 Audit Requirements ... 48

1. Introduction

[*Insert agency objectives here*]

This section draws together the structure of the agency's policy, and provides any other pertinent introductory statements required. For example:

A successful Information Security plan consists of establishing a framework comprising security policies, guidelines, standards and procedures.

1.1 Policy Statement

[Insert agency statement here]

The policy statement should be a concise statement of 'what' the policy is intended to accomplish. It should be two to three sentences long and should clearly reflect the overall government direction, the agency's direction and what the policy is hoping to achieve. The statement should be general enough to provide some flexibility and accommodate periodic changes in agency and whole-of-Government related requirements and standards.

1.2 Scope

[Insert agency scope here]

The scope details any limitations or constraints on the applicability of the policy to situations or entities within the agency. This policy should be developed in conjunction (or consultation) with relevant business areas such as finance, audit and senior business management. Agencies should also ensure this policy (and associated processes) adequately addresses security considerations relating to off-site work arrangements (e.g. home-based, mobile, regional, interstate and overseas).

1.3 Objectives

[Insert agency objectives here]

This section details the agency's policy objectives, how these policy objectives will be achieved and what resourcing will be supplied to support the implementation of the policy. For example, the agency's objectives could be to:

- *protect the agency's information assets through safeguarding its confidentiality, integrity and availability*
- *establish effective governance arrangements including accountability and responsibility for information security within the agency*
- *maintain an appropriate level of employee awareness, knowledge and skill to minimise the occurrence and severity of information security incidents*
- *ensure the agency is able to continue and/or rapidly recover its business operations in the event of a detrimental information security incident.*

1.4 Obligations

[Insert agency obligations here]

A number of regulatory or legal frameworks, guidelines or policies will impact on the development and implementation of the policy. The following mandatory quality criteria have been provided to ensure the agency's Information Security Policy adheres to the requirements of WoG IS Policy:

Mandatory Quality Criteria:

- *the policy MUST contain the mandatory clauses detailed in the Tasmanian Government Information Security Policy – Mandatory Clauses document*
- *the policy MUST be prepared on an agency wide basis and linked to agency security risks*
- *the policy is consistent with the requirements of relevant legislation and policies*
- *the policy is aligned with agency business planning, the agency's general security plan, and risk assessment findings*
- *endorsement for the policy is obtained from the relevant governance body*
- *approval for the policy is obtained from the relevant senior executives*
- *processes relating to IT change management (including maintenance of network systems) and configuration management processes are established and updated as required*
- *a policy to control email has been developed, implemented and endorsed*
- *policies and controls have been developed to manage all aspects of online and internet activities including anonymity/privacy, data confidentiality, use of cookies, applications/plug-ins, types of language used, practices for downloading executable, web server security configuration, auditing, access controls and encryption.*

1.5 Information Security Policy Framework Structure

Below is a suggested Information Security Policy Framework, based on an agency example. The Tasmanian Government Information Security Policy Manual includes as mandatory the development of an agency Information Security Policy, the structure of the policy framework is up to the individual agency.

The framework states why information security is important, defines what has to be done to secure communications and information technology resources, how security rules are to be implemented and who is responsible for their implementation.

Framework element	**Purpose and content**	**Role Responsible for Approval**
Policies	Information security policies are the high level mandatory rules that state why information security is important and define the objectives and strategies for protecting the confidentiality, integrity and availability of ICT resources.	Commissioner/Secretary
Guidelines	Guidelines contain detailed security requirements and criteria for meeting information security policy objectives and strategies.	Deputy Commissioner
Technical Standards	Technical Standards contain detailed security requirements and criteria for meeting guidelines and policy objectives. Technical Standards may incorporate information security checklists.	Director Corporate Services or relevant Commander
Procedures	Procedures explain in detail how the security requirements are to be implemented.	Managers and Officers in Charge

1.5.1 Information security policy categories

The information security plan framework is built around the following policy categories.

Category	Objective
Information Security Governance & Managment	Define roles and responsibilities within the Agency for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security.
Record Security	To ensure that controls are established to achieve best practice record keeping to protect the creation, preservation, disposal, transfer, release and access to agency Government records
Information Security Classification	To ensure that official information is protected commensurately with the consequences of unauthorised disclosure, misuse or compromise.
Physical Environment Security	To ensure that controls are in place to protect the physical security of all communication and information technology resources. The level and types of controls implemented should minimise the risk of equipment or information being rendered inoperable or inaccessible, or accessed or removed without appropriate authorisation.
Asset Management	To ensure that security-classified agency communication and information technology resources are identified and recorded in registers so that responsibility can be assigned for maintaining appropriate security controls.
Personnel and Awareness	To ensure that employees, contractors and third parties understand their responsibilities and are suitable for the roles they are considered for and to reduce the risk of theft fraud or misuse of agency information and ICT facilities.
Operational Procedures and Responsibilities	To ensure that security controls MUST be in place to safeguard all operations of agency information facilities and systems.
Network Security	To ensure that security controls are established to protect agency networks and infrastructures from unauthorised access and to safeguard information confidentiality and integrity.
Electronic Information Transfer	To ensure that appropriate security controls are in place to protected information when being transferred electronically. To prevent the loss, modification or misuse of Agency data, stored or transmitted on computerised communications systems.
Identity & Access Management	To prevent unauthorised computer access.
Security audit logging	To ensure that information related to security relevant activities is recognised, recorded, stored and analysed in order to minimise future security incidents and to provide evidence of past security incidents.
Information Systems acquisition, development and maintenance	To define security requirements of information systems during all stages of the information system life cycle.

Category	**Objective**
Business Continuity Management	To have business continuity plans available to counteract interruptions to AGENCY information systems and business activities from the effects of major failures or disasters.
Information Technology Media Management	To prevent unauthorised use, disclosure, modification, removal or destruction of fixed and removable information technology media
Cryptography	To ensure that approved cryptographic systems and techniques are used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.
Malicious and mobile code control	To protect the integrity of AGENCY software, data and information from the threat of computer malicious code and unauthorised mobile code infection.
Monitoring for Compliance	To define requirements for monitoring use of information processing facilities in accordance with AGENCY policy, statutory law, common law, international law and contractual requirements.
Incident Management	To ensure that effective processes are established for detecting, reporting, recording and resolving information security incidents.
Information Security Risk Management	Regular risk assessments and system audits should be conducted to ensure the security of Communication and Information Technology (CIT) resources.

1.5.2 Information Security Policy and Related Framework Elements

Policy	Guidelines	Technical Standards	Procedures
Information Security Governance & Management	Yes		Yes
Record security	Yes		Yes
Information Security Classification	Yes		
Physical Environment Security	Yes	Yes	Yes
Asset Management	Yes		Yes
Personnel and Awareness			Yes
Operational Procedures and Responsibilities		Yes	Yes
Network Security		Yes	Yes
Article I. Electronic Information Transfer	Article II. es	Yes	Yes
Identity and Access Management	Yes	Yes	Yes
Security Audit Logging	Yes	Yes	Yes
Information Systems Acquisition, Development and Maintenance		Yes	Yes
Business Continuity Management	Yes		Yes
Information Technology Media Management	Yes	Yes	Yes
Cryptography		Yes	
Malicious and mobile code control	Yes	Yes	Yes
Monitoring for Compliance			Yes
Incident Management	Yes		
Information Security Risk Management	Yes		

1.6 Implementation

[*Insert agency implementation requirements here*].

Tasmanian Government Mandatory Clauses

This policy will be communicated on an ongoing basis and be accessible to all employees.

Agency Clauses

[*Insert agency specific clauses*].

The implementation and review section details how the policy will be implemented including how the policy will be communicated and be accessible to all appropriate agency employees.

Details the performance measures or review mechanisms established to ensure the policy is being implemented effectively.

1.7 Policy Owner/Enquiries

[*Insert agency text here*].

Agencies should identify the owner of the Information Security Policy and who is responsible for the development and ongoing review of the policy. Contact details for enquiries should be listed in this section.

1.8 Policy Approval

[*Insert agency policy approval here*]

Tasmanian Government Mandatory Clauses

This policy [insert version number] was endorsed by [*insert name of governance body*] on [*insert date*].

This policy [*insert version number*] was approved by [*insert name and role title*] on [*insert date*].

Agency Clauses

[*Insert agency specific clauses*].

This section details the specific delegations for approval of security policies.

Agencies should obtain appropriate approval/endorsement/signoff from the agency Chief Executive Officer and their Information Steering Committee (or similar agency governance body).

1.9 Policy Review

[*Insert agency review details here*]

Tasmanian Government Mandatory Clauses

This policy is reviewed [*annually*].The next scheduled review is [*insert date*].

This policy will also be reviewed and evaluated in line with changes to business and information security risks to reflect the current agency risk profile.

Agency Clauses

[*Insert agency specific clauses*].

The agency should review their policy periodically (at least annually) and as a result of significant changes to the agency business or structure, machinery-of-Government changes, information security risk analysis, information security compliance assessment and reports of security incidents.

2. Information Security Governance and Management

The governance domain includes all activities related to the governance, authorisation and auditing of information security arrangements within the organisation. Roles and responsibilities relating to information security within the agency should also be defined.

Tasmanian Government Mandatory Clauses

Policy:

The Head of each agency MUST convene an Information Security Committee composed of senior management, or assign the role to an existing senior management committee. This Committee is responsible for ensuring the Policy is applied.

Mandatory procedures:

Each agency MUST govern its application of the Policy with an Information Security Committee composed of senior management, or assign the role to an existing senior management committee. The role of the Committee is to:

- direct the development and maintenance of an agency Information Security Plan,
- direct the implementation of the Information Security Plan across the agency,
- assign responsibilities to individual officers,
- approve information security roles within the agency,
- oversee the maintenance and implementation of an agency communications plan for information security, and
- oversee routine information security inspections and reviews.

Agency Clauses

[*Insert agency specific clauses*].

See TAHO Advice 35 Part 3 for details relating to the mandatory requirements. Agencies should also consider the following:

- *Detail the agency's internal governance arrangements. Information security governance arrangements must be established and documented (including roles and responsibilities) to implement, maintain and control operational information security within the agency,* – e.g. *an information security committee (ISC) or existing committee within the agency*
- *Information security controls should address all relevant business requirements and considerations*
- *Information security controls should be integrated with all agency processes to create a coherent approach to agency business*
- *Agencies should consider implementing an information security management system.*

  Designated Information security officers should be appointed whose role is to coordinate:

  - *implementation of agency information security policies and plans;*
  - *delivery of information security communication, education and training; and*
  - *investigations of information security incidents.*
- *Agencies may have several designated Information Security Officers covering different areas. For example, separate officers may be responsible for ICT security, physical security, individual business units and/or record security.*
- *Agency Information Security Officers SHOULD report directly to the Agency Information Security Committee on information security matters.*

- *Accountability and responsibilities for information security should be clearly outlined including the implications of breaches of security policy*
- *Endorsement for the information security internal governance arrangements should be obtained from the relevant senior executives and governance body.*

2.1 External Party Governance

Agencies should also consider external party governance arrangements they have in place. This includes all activities related to the governance, authorisation and auditing of information security arrangements for external parties that handle organisational information.

Information security external governance arrangements should be established and documented to ensure that third party service level agreements, operational level agreements, hosting agreements or similar contracts clearly articulate the level of security required and are regularly monitored.

Endorsement for the information security external governance arrangements must be obtained from the relevant senior executives and governance body.

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *detail agency participation in external/whole-of-Government information security committees*
- *detail the external organisations that handle the organisation's information*
- *are there policies and processes in place at these external organisations?*

Further information on information security roles and responsibilities is detailed in the TAHO Information management Advice 35 Part 3 - Information Security Governance.

2.2 Information Security Plan

The information security plan includes all activities relating to developing and maintaining information security plans, and ensuring that plans are communicated and accessible to employees as necessary.

Tasmanian Government Mandatory Clauses

An Information Security Plan MUST be developed and MUST align with agency business planning, general security plan and risk assessment findings.

Endorsement for the Information Security Plan MUST be obtained from the relevant senior executives and governance body.

A threat and risk assessment MUST be conducted for all ICT assets that create, store, process or transmit security classified information at least annually or after any significant change has occurred, such as machinery-of-Government.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should provide a brief summary of their Information Security Plan including a link to where the plan is located.

2.3 Information Security Risk Management

Information security risks are threats or vulnerabilities that introduce uncertainty regarding the availability, confidentiality or integrity of information. Structured risk assessments help to prioritise risks and implement appropriate risk management procedures.

Each agency is to consider legislation and policy relevant to its business that could impact on how it manages information security risks. Information security risk management can be undertaken as part of a broader agency risk management approach.

Tasmanian Government Mandatory Clauses

Each agency MUST identify, quantify and prioritise risks against risk acceptance criteria and determine appropriate controls to protect against risks.

Agency Clauses

Agencies SHOULD use AS/NZS ISO 31000:2009 to guide risk management.

Agencies SHOULD also refer to Standards Australia HB 231:2004 for specific guidance about managing information security risks.

Agencies should also consider the following:

- *To avoid duplication of effort and increase effectiveness of risk assessments, it is RECOMMENDED that agencies:*
    - *combine information security risk assessments with other business-related risk assessments, and*
    - *adopt a consistent risk management framework for all risk management activities.*

3. Resource Management

Each agency MUST maintain and apply appropriate protective policies and procedures for resources, including:

- protecting records of business activities,
- applying information security classifications where applicable,
- controlling physical access to information assets, and
- controlling the use of information and communications technology

3.1 Record Security

Tasmanian Government Mandatory Clauses

Section 11 of the Archives Act 1983 requires that Heads of Agency, officers or employees of government departments MUST maintain appropriate custody of records on behalf of the Crown until dealt with in accordance with the Act.

In addition to the Archives Act 1983, each agency MUST take into account legislation that is specific to its business operations when managing record security.

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).

Agencies MUST transfer records to the Tasmanian Archive & Heritage Office in accordance with Section 11 of the Archives Act. In addition, at the time of transfer, agencies MUST allocate appropriate access restrictions for these records in accordance with Section 15 of the Archives Act 1983 and TAHO Guideline 4 – Agency determination of access restrictions.

Agencies MUST comply with the following TAHO Guidelines prior to transferring records to non-Tasmanian Government entities:

- Guideline 10 – Outsourcing of government business: recordkeeping issues
- Guideline 14 – Privatisation of government business: recordkeeping issues

Disposal of information MUST be conducted according to guidelines set out by the State Archivist.

Agency Clauses

- *Each agency must have an active Records Management Program*
- *Each agency must have an identified Records Manager*
- *Each agency must have an information asset register that contains the details of all of the agencies assets regardless of format. This register must identify the information asset owner & custodian, and all assets must have a disposal category and information classification assigned.*

3.2 Information Security Classification

Information security classification includes all activities that ensure information is appropriately classified.

Tasmanian Government Mandatory Clauses

All information assets MUST be assigned appropriate security classification and control in accordance with the Tasmanian Government Information Security Policy Manual.

If an agency is not obliged to use other information security classification marking and handling then it MUST conduct a risk assessment to determine the appropriate marking and handling from the Tasmanian Government Information Security Policy Manual.

Information Security Classification schemes do not limit the provision of relevant legislation under which the [agency/department/entity] operates.

Agency Clauses

[*Insert agency specific clauses*].

The level of security controls should be commensurate to the classification level, value and degree of reliance on the information and systems. Agencies should provide information about how the agency's information assets are classified, e.g. Are they recorded in the agency's information asset register?

In many cases, it is not practical to classify each item or document. It is RECOMMENDED that agencies consider applying an information security domain to a set of assets. An information security domain is a logical grouping of items that require a similar level of protection, for example all personnel records may be given the same record security classification.

3.3 Information Asset Register

The asset protection responsibility domain includes all activities that implement and maintain appropriate protection of organisational assets.

Tasmanian Government Mandatory Clauses

Agencies SHOULD maintain security classified record/information asset registers to record details of each classified asset that is classified PROTECTED or HIGHLY PROTECTED.

Security classified record registers may be part of an overall information asset register or managed separately.The register itself is an information asset that SHOULD be classified as X-IN-CONFIDENCE.

All ICT assets that create, store, process or transmit security classified information MUST be assigned appropriate controls in accordance with the Tasmanian Government Information Security Classification.

All ICT assets (including hardware, software and services) and information assets should be identified, documented and assigned ICT asset custodians for the maintenance of security controls.

All ICT assets that provide underpinning and ancillary services must be protected from internal and external threats (eg. mail gateways, domain name resolution, time, reverse proxies, remote access and web servers).

Agency Clauses

[*Insert agency specific clauses*].

Information should be provided about the agency's information asset register (or similar registers for security classified information), including what information assets are identified, documented, the owners/custodians etc.

Further information on the requirements of information asset registers can be located in TAHO Information Management Advice 39: Developing an Information Asset Register

4. Physical Environment Security

Prevention of unauthorised physical access to Tasmanian Government information assets requires protection of facilities, information and people from damage or interference. Protecting physical assets from unauthorised access includes issues such as:

- the need for, method and extent of public access to the workplace (e.g. schools, libraries, and health facilities all have high levels of public access);
- emergency evacuation procedures and how they link to access control procedures;
- protection against ill intentions of authorised personnel inside facilities in addition to intruders;
- restrictions and requirements for multi-tenanted sites (i.e. sites shared with other organisations);
- requirements for sites that are shared with other agencies; and
- the review of risk assessments when the use of a building, or the level of risk, changes.

4.1 Physical Environmental Controls

Physical environment controls include all activities that ensure information security is not compromised by unauthorised physical access, damage or interference to premises or information.

Tasmanian Government Mandatory Clauses

Agencies MUST implement and maintain a comprehensive set of physical environment controls that meet requirements identified by a risk assessment.

Building and entry controls for areas used in the processing and storage of security classified information must be established and maintained.

Physical security protection (commensurate with the security classification information levels) MUST be implemented for all offices, rooms, storage facilities and cabling infrastructure.

Control policies (including clear desk/clear screen) MUST be implemented in information processing areas that deal with security classified information.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What are the agency's control policies?*
- *What areas need physical entry and perimeter controls (eg. computer rooms, document storage)?*
- *How are all other areas (eg. offices, workstations, delivery facilities, third party access) to be secured?*
- *What type of access mechanisms should be used (eg. beyond just a locked door)?*
- *Each agency is to also consider legislation and policy relevant to its business or activities that could impact on the physical environment.*

4.1.1 Entry Control and Visitor Control

Tasmanian Government Mandatory Clauses

It is RECOMMENDED that control of entry to buildings is 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; if it is treated as no more than a routine formality, it can become a danger to security.

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

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

Protocols for staff to challenge unescorted strangers are RECOMMENDED.

4.1.2 Entry Control by Personal Recognition

Tasmanian Government Mandatory Clauses

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 capable of resisting attempts by persons to evade their control; and
- the rate of personnel turnover is low and personnel are initially introduced to the doorkeeper and that the doorkeeper is 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.

4.1.3. Entry Control by Identity Pass

Tasmanian Government Mandatory Clauses

Agencies SHOULD issue different types of entry passes for permanent employees, ancillary personnel, regular and casual visitors.

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

- Each pass is serially numbered and a record kept of the person to whom it was issued.
- Everyone receiving a pass is required to sign for it immediately in the presence of the issuing officer.
- The pass does not identify the premises to which it gives access.
- The graphic design of passes used by agencies is changed from time to time.

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

- to immediately report the loss of a pass to the issuing officer;
- to return the pass to the issuing officer, or an agency security officer, as appropriate, when going on leave;
- not to keep their passes with other documents that may disclose their place of work; and
- 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 include using a logbook or an automatic access control system.

4.1.4 Visitor control in high-risk areas

Tasmanian Government Mandatory Clauses

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.
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 escorted 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 are to be taken at any time during the visit. It is RECOMMENDED that visitors be asked to deposit mobile phones and other equipment at 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.

The person last visited SHOULD be responsible for ensuring that the visitor leaves the building when their business is concluded, and any pass issued is duly returned to the agency. They SHOULD either escort the visitor to the entrance or arrange for another member of 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 a reception desk is located close to the main entrance.

4.1.5. Identification of Personnel Keeping Unusual Hours

Tasmanian Government Mandatory Clauses

Agencies SHOULD determine if there is any information security risk involved with personnel keeping 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 it, procedures may include:

- maintaining logs of all after-hours access (including late departures and early arrivals), and/or

- 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 an agency information security officer make discreet enquiries to determine the reason.

4.1.6 Buildings and Secure Areas

Tasmanian Government Mandatory Clauses

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

4.1.7 Planning Accommodation

Tasmanian Government Mandatory Clauses

Security requirements SHOULD be specifically referred to in any accommodation brief.
Careful planning of layout within a building can reduce security problems, for example:
Where protection against eavesdropping is required offices SHOULD be selected that do not share walls with other tenants and not be situated close to common use corridors and stairways.

- Registries SHOULD be located near to the offices they serve to facilitate the secure movement and control of sensitive documents.
- To reduce the risk of unauthorised people reading documents or computer screens, staff engaged in sensitive work SHOULD NOT be working in view of others.
- 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.

4.1.8 Secure Zones within Buildings

Tasmanian Government Mandatory Clauses

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 visitors' 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.

4.1.9 Managing the Risk of Overhearing

Tasmanian Government Mandatory Clauses

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 are 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 communications.

4.1.10 Telephone/video call or conference

Tasmanian Government Mandatory Clauses
Video conferencing is a form of real-time communication, like a telephone call, and presents the same risks of overhearing. It is recommended that precautions are taken to:

- ensure there is no sensitive or inappropriate material or activity visible in the frame of a video call,
- assess potential security risks arising from the office design and what may be visible or audible during a call,
- consider the risk of overhearing/eavesdropping if the conversation is broadcast through speakers, and
- ensure video and voice calls are only recorded with the express permission of all participants.

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.

4.1.11 Ancillary staff

Tasmanian Government Mandatory Clauses
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.

4.1.12 Managing the Risk of Over-viewing from Outside

Tasmanian Government Mandatory Clauses

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

4.1.13 Room Security

Tasmanian Government Mandatory Clauses
It is RECOMMENDED that locked security containers are be used to protect sensitive documents during working hours. It is the responsibility of individual officers and 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 drawers, lockable filing cabinets, safes etc. It is RECOMMENDED that the selection of security containers be based on the level of risk, 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) are to 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 suggested that agencies have regard to the nature of other security precautions within the building.

When a room is left unattended for less than the specified minimum period and sensitive documents are not locked away, the following SHOULD occur:
Doors and windows to the room are closed and secured.
Sensitive documents are protected from being read from outside.
If cleaners or other workers might have access from outside, all sensitive documents are to 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 details of job description contained in the directory.

4.1.14 Room Checks by Occupants at Close of Work

Tasmanian Government Mandatory Clauses
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. To ensure that this task is carried out regularly, a roster system can be implemented before offices are vacated.
It is RECOMMENDED that in agencies holding a substantial amount of highly sensitive information, an agency security officer checks rooms after the departure of occupants and before entry of cleaners or guard patrols.

4.1. 15 Conferences and Meetings

Tasmanian Government Mandatory Clauses
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 over-viewed by unauthorised people by planning appropriate seating arrangements.

Prior to leaving a meeting room it is RECOMMENDED that:

- whiteboards are cleared of sensitive information,
- USB drives and other portable electronic devices are removed, and
- any sensitive documents are removed and disposed of securely.

If special security arrangements are considered necessary for a meeting, agency security staff SHOULD be consulted.

4.1.16 Home-based work environments

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

4.1.17 Mail and other delivery areas

Tasmanian Government Mandatory Clauses

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; and
- appropriate procedures relating to the handling of suspicious deliveries.

Where appropriate, agencies SHOULD consult with Tasmania Police.

4.1.18 Asset Management

Asset Management includes equipment security and all the activities that ensure information security is not compromised by loss, damage, theft or other compromise of the organisation's physical equipment assets.

Tasmanian Government Mandatory Clauses

All ICT assets that store or process information MUST be located in secure areas with access control mechanisms in place to restrict use to authorised personnel only.

Policies and processes MUST be implemented to monitor and protect the use and/or maintenance of information assets and ICT assets away from premises.

Policies and processes MUST be implemented to securely dispose and/or reuse ICT assets, commensurate with the information asset's security classification level.

The following Treasurer's Instructions, issued under the Financial Management and Audit Act 1990, relate to the management of assets:

- TI. 301 – Reporting Procedures in Cases of Illegal Entry and/or Damage to or Loss of Property or Money
- TI. 302 – Recording of Losses
- TI. 304 – Recording of Non-current Assets

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *If physical controls are not possible, agencies need to detail the control methods in place.*
- *How and where is critical equipment to be sited?*
- *What safeguards are to be in place?*
- *What safeguards are in place for power supplies to critical equipment?*
- *How is cabling to be protected?*
- *How is communications equipment to be housed?*
- *How and who is allowed to carry out maintenance on equipment?*
- *What is the policy on security of equipment kept off site (eg. home use equipment, portable equipment)?*
- *What is the process/who authorises the disposal and reuse of equipment?*
- *What is the policy for unattended workstations, unattended facsimiles, etc?*

5. Information and Communications Technology

Information and Communications Technology includes all activities that ensure appropriate resource management procedures, specifically relating to information and communications technology (ICT).

Tasmanian Government Mandatory Clauses

Each agency MUST implement and maintain a comprehensive set of information security controls relating to ICT that meet requirements identified by a risk assessment.

Agencies MUST refer to the 'Tasmanian Government WAN and Internet Services Information Security Policies and Standards' regarding information security controls relating to WAN and internet services.

Agencies MUST implement detection, prevention and recovery controls to protect against malicious software.

Agency Clauses

[*Insert agency specific clauses*].

- *Agencies SHOULD identify and treat risks associated with ICT by referring to AS/NZS ISO/IEC 27002:2006.*

5.1 Operational Procedures and Responsibilities

Operational procedures and responsibilities include all activities that ensure the correct and secure operation of information processing facilities.

Tasmanian Government Mandatory Clauses

Operational procedures and controls must be documented and implemented to ensure that all information assets and ICT assets are managed securely and consistently (in accordance with the level of security required).

Operational change control procedures MUST be implemented to ensure that changes to information processing facilities or systems are appropriately approved and managed.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What processes must be documented and who is responsible?*
- *What is the policy with regard to separating the development/testing environment from the operational environment?*

5.2 Third Party Service Delivery

Third party service delivery includes all activities that implement and maintain information security in line with service delivery agreements.

Tasmanian Government Mandatory Clauses

Third party service delivery agreements MUST comply with the Policy.

Third party service delivery agreements MUST be periodically reviewed and updated to ensure they address any changes in business requirements but remain compliant with the Policy.

Third party service operating agreements MUST specifically address third party governance policies and processes (see TAHO Advice 35 on Information Security Governance).

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Will the service agreements be audited against the policy and how often?*
- *What processes must be documented and who is responsible?*
- *Is there a document style template that must be used?*
- *What is the policy for segregating duties that might involve a conflict of interest?*
- *What are the specific duties that must be segregated?*
- *Do separation agreements with the supplier consider information security arrangements (eg. at the end of a contract or breaking of a contract)?*
- *Have outsourcing/external hosting separation expectations and processes been documented?*
- *Will the agency be notified in the event of the supplier's insolvency? Can the agency terminate the contract?*
- *Have escrow agreements been established to ensure that rights to data, systems, and codes will be transferred to the agency in the case of the supplier's collapse?*

5.3 Capacity Planning and System Acceptance

Capacity planning and system acceptance includes all activities that monitor resources and set criteria for system changes to reduce the risk of system failure.

Tasmanian Government Mandatory Clauses

System acceptance MUST include confirmation of the application of appropriate security controls and of the capacity requirements of the system.

System capacity MUST be regularly monitored to ensure risks of system overload or failure which could lead to a security breach are avoided.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What processes are subject to authorised change control?*
- *Is there a process for implementing changes to information systems?*
- *Who is responsible for information systems capacity planning?*
- *What processes or systems need to be monitored for future planning?*
- *Who is responsible for the migration of new systems or upgrades into the operating environment?*

5.4 Backup Procedures

Backup procedures include all activities that maintain the integrity and availability of information and applications through the use of backup activities.

Tasmanian Government Mandatory Clauses

Comprehensive information and system backup procedures and archiving MUST be implemented.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the policy on backup?*

- *What is the policy for logging system activities?*
- *What is the policy on systems maintenance?*
- *What are the authorisation processes?*

5.5 Network Security

The network security domain includes all activities that ensure the security of information being passed over networks.

Tasmanian Government Mandatory Clauses

Network security policy MUST be developed and documented to guide network administrators in achieving the appropriate level of network security.

Processes to periodically review and test firewall rules and associated network architectures MUST be established to ensure the expected level of network perimeter security is maintained.

Processes MUST be established to periodically review and update current network security design, configuration, vulnerability and integrity checking to ensure network level security controls are appropriate and effective.

A policy on scanning MUST be developed to ensure that traffic entering and leaving the agency network is appropriately scanned for malicious or unauthorised content.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Who is responsible for network management?*
- *What are the policies and processes for remote access?*
- *Who authorises external connections?*
- *All external perimeter access should be secured using defence-in-depth security systems, including firewall, intrusion detection and prevention systems*

5.6 Information Technology Media Management

Disposal includes removal of media off-site under warranty or hardware service agreements. Unauthorised use of information can occur through careless disposal.

Tasmanian Government Mandatory Clauses

When disposing of media, agencies MUST ensure all information held on the media is either retained or disposed of in a secure fashion and in accordance with the Archives Act 1983, and;

Hardware (e.g. computers) MUST be disposed of in accordance with the disposal Treasurer's Instructions, issued under the Financial Management and Audit Act 1990 including the following Treasurer's Instructions

- TI. 1301 – Disposal of Goods – Overview; and
- TI. 1305 – Disposal of Personal Computers

Agencies SHOULD address the need for sanitisation or destruction of media prior to reuse in a new environment or disposal. Media sanitisation and disposal guidelines are suggested in the table below. For more information see the Australian Government Information Security Manual.

It is RECOMMENDED that agencies use equipment endorsed by the Australian Government

Security Construction and Equipment Committee for the destruction or sanitisation of electronic media or equipment. See the Australian Government Security Construction and Equipment Committee Security Equipment Catalogue for more details.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the process for reusing media? eg. Hard drives, backup tapes.*
- *What is the process for transporting and storing media?*
- *What is the process and who authorises disposal of all types of information? eg. Paper documents, disks, and system documentation?*
- *What is the process for storage, handling and access to all types of information types? eg. How is media to be labelled, use of distribution lists, filing of emails, facsimiles?*

5.7 Electronic Information Transfer

The information exchange domain includes all activities that maintain the security of information exchanged (internally or externally).

Tasmanian Government Mandatory Clauses

Methods for exchanging information within the agency, between agencies, through online services, and/or with third parties MUST be compliant with legislative requirements and MUST be consistent with the the manual.

The type and level of encryption MUST be authorised and compliant with the requirements of the manual.

All information exchanges over public networks, including all online or publicly available transactions/systems MUST be authorised either directly or through clear policy.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What type of information can be sent over public networks (eg. facsimiles/email)?*
- *What checks are in place to check for transmission receipts?*
- *What is the policy in relation to information and communication devices including answering machines, electronic diaries?*

5.8 eCommerce

The eCommerce domain includes all activities that ensure the security of e-commerce services and their use.

All critical online services MUST have penetration testing performed periodically.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What checks are to be carried out prior to instituting e-commerce services?*
- *Who authorises 'online' or publicly available transactions/systems?*

5.9 Security Audit Logging

Security Audit Logging includes all activities that detect unauthorised information processing activities including the use of audit logging.

Tasmanian Government Mandatory Clauses

Comprehensive operator and audit/fault logs MUST be implemented.

All ICT assets MUST be synchronised to a trusted time source that is visible and common to all.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What system events will be logged, eg. date, IP address, User IDs, unsuccessful logins, alerts from intrusion detection systems (firewall)?*
- *When and who will review and monitor system logs?*
- *Where are they stored?*
- *How long are logs kept for?*
- *Do logs contain confidential information? If so is this information adequately protected?*
- *Have procedures been developed for monitoring use of information processing facilities?*
- *Are these procedures reviewed regularly?*
- *How often should the result of monitoring activities be reviewed?*
- *Is log information and logging facilities protected against tampering and unauthorised access?*
- *Intrusion detection or prevention services should be implemented at critical or essential ingress, egress and end-points within an agency's network domain.*

5.10 Malicious and Mobile Code Control

Malicious and mobile code control includes all activities that protect the integrity of applications and their information from malicious code.

Tasmanian Government Mandatory Clauses

Adequate controls MUST be defined and implemented for the prevention, detection, removal and reporting of attacks by malicious code on all ICT assets.

Vulnerability/integrity scans of core software MUST be defined and conducted regularly to ensure detection of unauthorised changes.

Anti malicious-code software MUST be regularly updated with new definition files and scanning engines.

Employees MUST be educated about malicious and mobile code in general, the risks posed, virus symptoms and warning signs including what processes should be followed in the case of a suspected virus.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the agency method of insuring only authorised software is used?*
- *Are web applications secured against network attacks such as Structured Query Language (SQL) injections?*
- *What is the agency policy on the prohibited use and installation of software not authorised by the agency including user responsibilities with regards to downloading software from Internet and e-*

mail sources?

- *What is the agency policy and method for virus and malicious code protection?*
- *Who is responsible for cleaning and reporting malicious code attacks?*
- *How will users be educated?*

6. Identity and Access Management

6.1 Access Control Policy

The Identity and Access management policy includes all activities that set access and control policies. This applies to a service or information that:

- is provided to agency personnel
- is provided to clients of Government
- is in electronic or non-electronic form
- is new or an improved version

Tasmanian Government Mandatory Clauses

Each agency MUST control the access to information, facilities and business processes on the basis of business need and risk assessment.

Agencies MUST determine appropriate access assurance levels in accordance with the Personal Information Protection Act (2004), particularly:

- Personal Information Protection Principle 1 – specifies that a personal information custodian may only collect personal information where it is necessary for one or more of its functions or activities.

It is RECOMMENDED that risk and access assurance is analysed in the following situations:

- during development of new information systems or services,
- when systems or services require authentication across two or more agencies, and/or
- when systems or services have been identified as high risk.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Have Control mechanisms based on business requirements and assessed/accepted risks for controlling access to all information assets and ICT assets been established?*
- *Are Access control rules consistent with agency business requirements, information classification, and legal/legislative obligations?*
- *Have policies been established for the configuration of remote access support applications and utilities?*
- *Who authorises access to systems and business applications? How is authorisation granted?*

6.2 Authentication

The authentication domain includes all activities and measures that ensure users are the persons they claim to be.

Tasmanian Government Mandatory Clauses

Each agency MUST evaluate the risks associated with providing each service and determine the level of authentication assurance required using the Tasmanian Government Identity and Access Management Toolkit.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Have appropriate authentication mechanisms been applied for users and equipment?*

- *Have appropriate authentication mechanisms been applied for remote users?*
- *Have appropriate authentication controls been implemented to control access to wireless networks?*
- *Do users have a unique identifier (user ID) for their personal use? Has a suitable authentication process been chosen to substantiate the claimed identity of a user?*

6.3 Access Control

Tasmanian Government Mandatory Clauses

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 of their activities are essential.

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

Audit logs are records under the Archives Act 1983 and MUST NOT be disposed of without the written authority of the State Archivist. See Tasmanian Archives and Heritage Office Disposal Schedule for Common Administrative Functions.

It is RECOMMENDED that risk assessments are carefully conducted where a business application:

- has users external to the agency, 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.

6.4 User access

User access includes all activities that ensure authorised access to information and applications.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Access to information systems requires specific authorisation and each user must be assigned an individually unique personal identification code and secure means of authentication.*
- *How is access to information systems to be granted? e.g. passwords.*
- *Who is responsible for monitoring and reviewing access rights?*
- *Who is responsible and what is the process for the removal and notification of, redundant User IDs and accounts?*
- *Who is responsible for granting access to systems utilities and privilege management?*
- *Are those with privileged access required to sign for access to a system before it's granted?*
- *How is access and use of systems utilities monitored?*

6.5 User Responsibilities

User responsibilities include all activities that ensure users understand their responsibilities to prevent compromise of information or systems.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What are users' responsibilities for access and passwords?*
- *Do users follow good security practices in the selection and use of passwords?*
- *Do users ensure that unattended equipment has appropriate protection (eg. computers are locked when left unattended)?*
- *Does the agency adopt clear desk/clear screen policies?*

6.6 Network Access

Network access includes all activities that ensure network access is restricted to authorised users.

Tasmanian Government Mandatory Clauses

Control measures MUST be implemented to detect and regularly log, monitor and review information systems and network access and use, including all significant security relevant events.

Authorisation MUST be obtained and documented for access (including new connections) to agency networks.

All wireless communications MUST have appropriate configured product security features and afford at least the equivalent level of security of wired communications.

Security risks associated with the use of ICT facilities and devices (including non-government equipment) such as mobile telephony, personal storage devices and internet and email MUST be assessed prior to connection and appropriate controls implemented.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Who is responsible for authorising network access (both internal and external connections)?*
- *What is the process for enforced network paths and user authentication for external connection, Node authentication, use of remote diagnostic ports?*
- *How will network domains and groups be segregated?*
- *What network connection controls will be in place? – eg. time, type and size of file transfers to external source.*
- *The number of external gateways allowed access to extranets, internal networks and other security zones should be minimised.*

6.7 Operating System Access

Operating system access includes all activities that ensure access to operating systems is restricted to authorised users.

Tasmanian Government Mandatory Clauses

Policies and/or procedures for user registration, authentication management, access rights and privileges, MUST be defined, documented and implemented for all ICT assets.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *How is automatic terminal identification used to authenticate connections to specific locations and portable equipment?*
- *What is the secure logon and logoff process for access?*
- *Are there restrictions on connection times in place?*
- *How will passwords be issued and managed – what are the rules for passwords?*
- *How will systems utilities' use be controlled?*

6.8 Application and Information Access

Application and information access includes all activities that ensure access to information and applications are restricted to authorised users.

Tasmanian Government Mandatory Clauses

Restricted access and authorised use only warnings MUST be displayed upon access to all systems.

Access to all confidential/sensitive systems MUST only be allowed after authorised approval.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Who authorises application access? eg. read, write*
- *Is a record kept of authorised user access to confidential/sensitive systems?*
- *Is this list reviewed and revalidated periodically?*
- *What is the process for authorising access to information when systems share resources? eg. two separate systems are integrated to form a third application or system.*

6.9 Mobile Computing and Telework Access

Mobile computing and telework access includes all activities that ensure information security is maintained when using mobile computing and telework facilities.

Tasmanian Government Mandatory Clauses

Risk assessments MUST be conducted and processes MUST be established for mobile technologies and teleworking facilities.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *the development of information security policies and procedures for devices (eg. laptop and notebook computers; palm tops; smart cards; mobile phones; portable storage devices)*

These policies and procedures should be based on the results of risk assessments and provide the policy (direction?) and instructions for such issues as:

- *physical storage and protection of equipment, for example use in public places and transporting equipment*
- *personal usage*
- *protection of the information held on the device (eg backups, virus protection)*
- *access mechanisms (eg, password, authentication methods).*

Policies and procedures should be clearly documented to authorise and control teleworking activities, and cover issues including:

- *physical security of the site*
- *authorisation processes and system access*
- *security of the telecommunications link*
- *lack of control of information, (for example, access by family, friends)*
- *increased risk of disclosure or unauthorised use of information*
- *increased risk of unauthorised access to agency network and systems*
- *support and maintenance of hardware and software updates*
- *backup procedures*
- *access security aspects (writing down of instructions for login including passwords).*
- *policy on connection of privately owned devices to agency networks. (eg. authentication measures, access controls, virus and malicious codes and physical/personnel security).*

7.7. Information System Acquisition Development and Maintenance

7.1 System Security Requirements

System security requirements include all activities that ensure security requirements are articulated during the development of new systems, or when planning enhancements to existing systems.

Tasmanian Government Mandatory Clauses

Agencies purchasing information technology goods and services MUST do so in accordance with the procurement Treasurers Instructions, issued under the Financial Management and Audit Act 1990. In particular:

- TI. 1112 – Common use / Whole-of-government contracts: goods and services requires agencies to use the C150 contract for the provision of computer hardware and related services via a manufacturer/reseller network; and
- TI. 1123 – Government Information Technology Conditions requires agencies to use the Government Information Technology Conditions for all IT purchases.

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

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

Agency information security 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. Information can be disclosed during exchange of media conducted under a warranty and/or maintenance agreement.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Security controls must be commensurate with the security classifications of the information contained within/- passing across information systems, network infrastructures and applications.*
- *Security requirements should be addressed in the specifications, analysis and/or design phases. Internal and/or external audit must be consulted when implementing new or significant changes to financial or critical business information systems.*
- *Security controls should be established during all stages of system development, as well as when new systems are implemented and maintained in the operational environment.*
- *Appropriate change control, acceptance and system testing, planning and migration control measures must be carried out when upgrading or installing software in the operational environment.*
- *Accurate records should be maintained to show traceability from original business requirements to actual configuration and implementation, including appropriate justification and authorisation.*
- *Have access controls been identified and implemented including access restrictions and segregation/isolation of systems into all infrastructures, business and user developed applications?*
- *What are the security controls that should be addressed in new systems or upgrades? eg. input data validation, internal processing, message authentication, output data validation?*

7.2 Correct Processing

Correct processing includes all activities that prevent errors, loss, unauthorised modification or misuse of information in systems.

Tasmanian Government Non Mandatory Clauses

Access controls SHOULD be identified and implemented including access restrictions and segregation/isolation of systems into all infrastructures, business and user developed applications.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Do access controls include the validation of input data, internal processing and output data?*
- *Are additional controls in place for sensitive, valuable or critical information?*
- *Has data input to applications been validated? Are validation checks incorporated into applications?*
- *Has data output from applications been validated?*

7.3 Cryptographic Protocols

Cryptographic Protocols include- all activities that protect the integrity, confidentiality and authenticity of information by using cryptographic controls.

Tasmanian Government Non Mandatory Clauses

Agencies SHOULD only use Defence Signals Directorate approved cryptographic protocols for protection of data in transit. Refer to the Australian Government Information Security Manual for details on the approved protocols.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Has a cryptographic control policy been established and implemented?*
- *Has a risk assessment been used to determine whether a cryptographic control is appropriate?*
- *Are all cryptographic keys protected against modification, loss, disclosure and destruction?*
- *Is equipment used to generate, store and archive keys physically protected?*
- *Has activation and deactivation dates for cryptographic keys been defined?*

7.4 System Files

Considerations relating to System Files include all activities that ensure system files are adequately protected.

Tasmanian Government Non - Mandatory Clauses

Access to system files should be controlled to ensure integrity of the business systems, applications and data.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *How is access to system files granted?*
- *Who is responsible for monitoring and recording changes to systems?*
- *What is the policy on keeping previous versions of software?*
- *What checks are in place for assessing impact of new systems or changes on existing systems?*
- *Who is responsible for authorisation of new systems or other changes?*
- *Where will system test data originate? How will operational data be monitored & authorised?*
- *How will program source code be monitored and maintained?*

7.5 Secure Development and Support Processes

Secure development and support processes include all activities that ensure the ongoing security of applications.

Tasmanian Government Clauses

Processes (including data validity checks, audit trails and activity logging) MUST be established in applications to ensure development and support processes do not compromise the security of applications, systems or infrastructure.

Audit logs are maintained.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the change request process for systems?*
- *Who can authorise changes to systems (eg timing in relation to business activities)? Who carries these out?*
- *What is the process for upgrading software changes – who assesses changes and impacts on current systems, business activities and costs?*
- *What checks are in place for ensuring that outsourced software development addresses agency information security requirements?*
- *What is the process for testing and evaluating software?*

7.6 Technical Vulnerability Management

Technical vulnerability management includes all activities that reduce risks arising from the exploitation of technical vulnerabilities.

Tasmanian Government Mandatory Clauses

Processes to manage software vulnerability risk for all IT security infrastructures MUST be developed and implemented.

A patch management program for operating systems, firmware and applications of all ICT assets MUST be implemented to maintain vendor support, increase stability and reduce the likelihood of threats being exploited.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Does the agency have a current and complete inventory of assets?*
- *Is timely information obtained about technical vulnerabilities of information systems?*
- *Has the agency's exposure to technical vulnerabilities been evaluated?*

- *Are vulnerability monitoring, risk assessment, patching and asset tracking undertaken?*
- *Has a timeline been defined to react to notification of potential vulnerabilities?*
- *When vulnerabilities are identified, how are actions managed?*
- *Are risks associated with the action assessed?*
- *Are patches tested and evaluated before they are installed?*

8. Personnel and Awareness

8.1 Personnel Procedures

Tasmanian Government Mandatory Clauses

Each agency MUST implement and maintain a comprehensive set of information security controls concerning personnel that meet requirements identified by a risk assessment.

Agencies SHOULD use relevant sections of AS/NZS ISO/IEC 27002:2006 to identify possible information security risks and procedures to treat identified risks associated with personnel.

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

Agency Clauses

[*Insert agency specific clauses*].

Acts that may be applicable to agencies in the implementation of personnel information security policies include:

- *Industrial Relations Act 1984*
- *Anti-Discrimination Act 1998*
- *State Service Act 2000*
- *Police Service Act 2003*
- *Education Act 1994*

The Tasmanian Government Information Identity and Access Management Toolkit provides definitions and detailed guidance on how to evaluate the risk associated with providing personnel with access to information services.

8.2 Prior to Engagement

Pre-employment checks may be considered for personnel that are likely to be handling sensitive material. There are a number of legislative restrictions to consider. In general, pre-employment security checks SHOULD NOT be used unless there is a legislative requirement or clearly identified risk that can be reduced by such checks.

The pre-employment domain includes all pre-employment activities that ensure employees, contractors and third party users will not compromise information security arrangements. Activities also include information security roles and responsibility definition, screening and employment terms and conditions.

Tasmanian Government Mandatory Clauses

Where applicable, agencies MUST refer to the State Service Commissioner Direction No. 10:2001 regarding pre-employment checks.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Security requirements must be addressed within recruitment and selection and in Statements of Duties.*
- *Who is responsible for assessing the level of security and ensuring that it is addressed in job descriptions?*
- *Will there be specific security clauses in contracts where third parties are involved?*

- *What security verification checks (eg. criminal reference checks) will be made on job applicants, contractors, and consultants, especially those who deal with sensitive information?*
- *Who authorises this? Who is authorised to carry out these checks?*
- *Will confidentiality agreements be signed?*
- *Do terms and conditions of employment outline security responsibilities and disciplinary processes?*

8.3 Assigning Personnel Responsibilities for Information Security – During Employment

Assignment of Personnel responsibilities during employment includes all activities that ensure employees, contractors and third party users

- are aware of information security threats and concerns,
- are aware of their information security responsibilities and liabilities,
- are equipped to support organisational information security policy and reduce the risk of human error.

All personnel are responsible for disclosing information 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*.

The 'need-to-know' principle requires that information is only available to those who need to access information for their assigned duties. It is the personal responsibility of all who access agency information to apply this principle. Implementing the need-to-know principle requires careful balancing of the risk to an agency of restricting the availability of information, against the risk of breaching confidentiality. For example, reduced availability may diminish an agency's ability to deliver services; alternatively, unrestricted access may cause avoidable harm to others.

Where appropriate, agencies SHOULD assign individual personnel or positions with 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 a high level of confidentiality to be maintained); or
- the role of monitoring and reporting on information security policies, procedures and risks to specified personnel or positions.

Tasmanian Government Mandatory Clauses

Agencies MUST implement and maintain communication and awareness processes that meet requirements identified by a risk assessment.

Induction, ongoing security training and security awareness programs MUST be implemented to ensure that all employees are aware of and acknowledge the agency's information security policy, their security responsibilities, and associated security processes.

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.

Where employees have access to HIGHLY PROTECTED information or perform specific security related roles, these responsibilities MUST be fully documented with signed acknowledgement, and communicated.

Agency Clauses

[*Insert agency specific clauses*].

- *Activities include information security awareness and training, disciplinary processes and setting of management responsibilities. Agencies should also consider the following:*
- *What security responsibilities will be included in induction and ongoing staff training?*
- *How will security responsibilities be communicated to staff and when?*
- *What is the disciplinary process for security violations?*
- *How is it communicated to staff, how often? Does the agency distribute copies to all employees?*
- *Who is authorised to deal with security violations?*

8.4 Post-employment

Considerations post-employment include all activities that seek to ensure that during changes or termination of employment, information security is not compromised.

Tasmanian Government Mandatory Clauses

Procedures for ensuring the security of the agency during the separation of employees from, or movement within the [agency/department/entity] should be developed and implemented.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What are the security processes for the exit or movement of employees, contractors or other third parties from or within the agency (eg. exit interviews; revoking of access rights and disabling of all User-IDs); and at the time of leaving, ensure all keys, access devices, credit cards are collected from employees?*
- *Is the employee aware of their continuing responsibilities in relation to the protection of the confidentiality and privacy of information they may have had access to in their duties?*
- *Are employees aware of the legal implications of non-compliance? i.e. the penalties involved?*
- *Are there procedures in place for employees who are terminated on an 'unfriendly' basis?*

9. Incident Management

The Australian Standard defines an information security event as an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be information security relevant.

An information security incident is indicated by a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations or threatening information security.

9.1 Incident Management Controls

Incident Management Controls include all activities that ensure a consistent and effective approach is applied to the management of information security incidents.

Tasmanian Government Mandatory Clauses

Each Agency MUST implement and maintain incident management controls that meet requirements identified by a risk assessment.

Information security incident management procedures MUST be established to ensure appropriate responses in the event of information security incidents, breaches or system failures.

Establish and maintain an information security incident register and record all incidents.

All information security incidents MUST be reported and escalated (where applicable) through appropriate management channels and/or authorities.

Where a deliberate violation or breach of this agency information security policy or subordinate processes has occurred, this MUST be investigated and formal disciplinary processes MUST be applied.

Responsibilities and procedures for the timely reporting of security events and incidents including breaches, threats and security weaknesses, MUST be communicated to all employees including contractors and third parties.

When criminal activity affecting information security is identified, agencies MUST liaise with Tasmania Police at the earliest opportunity. In these cases, the agency investigator and any other relevant agency representative should take care not to prejudice further police investigations and possible prosecution.

A decision to 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.

It is RECOMMENDED that agencies implement procedures to determine if and when legal action is to be pursued including:

- internal processes to approve referral to the Tasmania Police;
- rules to assist in determining when incidents will be referred to the Tasmania Police; and
- procedures and rules to ensure that evidence is retained in a form suitable for investigation and prosecution.

Agencies SHOULD use the relevant sections of AS/NZS ISO/IEC 27002:2006 for guidance on managing information security incidents.

Agencies SHOULD refer to AS/NZS ISO/IEC 18044:2006 for detailed guidance on information security incident management.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the process and policy for Agency security incident reporting?*
- *What type of security incidents must be reported?*
- *How is the information to be collected?*
- *Who is the information to be reported to?*
- *Who is responsible for following up security incident reports?*
- *What are reportable software malfunctions?*
- *Who is responsible for following up and resolving malfunctions?*
- *What is the reporting structure for reporting these?*
- *How are procedures to be communicated to staff?*
- *What are the procedures to be carried out for each type of incident?*
- *What are the escalation processes for criminal information security violations?*

9.2 Planning for Information Security Incidents

Tasmanian Government Non Mandatory Clauses

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. RECOMMENDED priorities are:

- protection of human life and people's safety
- protection of sensitive information
- protection of other information
- decision to pursue legal action
- prevention of irreparable damage to systems
- internal and external communication of the incident
- minimising disruption to services

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

- agency staff responsible for each site;
- external property managers (for leased sites);
- agency business owners of systems and sites;
- ICT system managers, including appropriate contracted suppliers;
- agency/government media liaison staff;
- agency senior managers; and
- Tasmania Police contacts to be used if legal action is to be pursued.

If an information security incident or event occurs, it is RECOMMENDED that agencies liaise with media units to establish appropriate public communication procedures. In doing so they may consider:

- the visibility and impact of such an incident on staff,
- the visibility and impact of such incidents on services with other agencies and the public,
- potential media interest in the incident, and
- potential political impact of the incident.

10. Business Continuity Management

10.1 Business Continuity

Business Continuity includes all activities that counteract interruptions to business activities and to protect critical business processes from the effect of interruptions or failures of ICT systems or disasters, and to ensure their timely resumption.

Business continuity also includes business continuity risk assessment, developing and implementing plans to address continuity management, and testing and maintenance of business continuity plans.

Tasmanian Government Mandatory Clauses

Each Agency MUST implement and maintain business continuity management controls that meet requirements identified by a risk assessment.

Methods MUST be developed to reduce known risks to information and ICT assets including undertaking a business impact analysis.

Business continuity plans MUST be maintained and tested to ensure information and ICT assets are available and consistent with agency business and service level requirements.

All critical business processes and associated information and ICT assets have been identified and prioritised.

Agencies SHOULD use the relevant sections of AS/NZS ISO/IEC 27002:2006 for guidance on managing business continuity.

Agencies SHOULD use the Handbooks HB 221:2004, HB 292:2006 and HB 293:2006 for detailed guidance on business continuity management.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Is there an understanding of the impact interruptions will have on the agency?*
- *Has appropriate insurance been purchased?*
- *Have all possible events been identified?*
- *Are all business continuity plans within the agency consistent?*

10. 2 ICT Disaster Recovery

ICT disaster recovery includes all activities related to ensuring the availability of ICT systems and services, including the restoration of ICT systems and services following an event which disrupts their delivery, or the continued operation of ICT systems and services despite the loss of operational ICT equipment.

ICT disaster recovery supports business continuity activities, but is distinct in focussing on the restoration of ICT services rather than on the restoration of business services themselves (which even if heavily dependent on ICT can often be maintained for short periods using manual systems).

Tasmanian Government Mandatory Clauses

An ICT disaster recovery register MUST be established to assess and classify ICT assets to determine their criticality.The register MUST include details of suppliers of critical systems.

Plans and processes MUST be established to assess the risk and impact of the loss of information and ICT assets in the event of a security failure or disaster, to enable information and ICT assets to be restored or recovered.

ICT disaster recovery plans MUST have clearly defined maximum acceptable downtimes.

ICT disaster recovery plans MUST be maintained and tested to ensure information and ICT assets are available and consistent with agency business and service level requirements.

Maximum acceptable downtimes for ICT services MUST also be defined in service and operational level agreements with external parties.

Copies of ICT disaster recovery plans MUST be stored in multiple locations including at least one location offsite.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *What impact will a disaster have on the agency?*
- *Has the agency identified and prioritised critical ICT processes and systems?*
- *Have additional preventative and mitigating controls been identified?*
- *Have all possible events been identified?*
- *Has the probability of a disaster occurring been calculated (eg. time, damage scale and recovery period)?*

11. Monitoring for Compliance

11.1 Legal Requirements

Legal requirements include all information security activities relating to compliance with legal requirements.

Tasmanian Government Mandatory Clauses

All legislative obligations relating to information security MUST be complied with and managed appropriately.

Each agency is to consider legislation and policy relevant to its business that could impact on how it manages information security risks. Information security risk management can be undertaken as part of a broader agency risk management approach.

All information security policies, processes and requirements including contracts with third parties, MUST be reviewed for legislative compliance on a regular basis and the review results reported to appropriate agency management.

Processes to ensure legislative compliance across all agency activities MUST be developed and implemented.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Are information security controls compatible with all legal and legislative needs?*
- *Are approaches to Right to Information and information privacy clearly stated?*

11.2 Policy Requirements

The policy requirements domain includes all information security compliance activities relating to information security policies and standards.

Tasmanian Government Non-Mandatory Clauses

All reporting obligations relating to information security MUST be complied with and managed appropriately.

The Checklist for Your Agencies Current Information Security Practices MUST be submitted annually to DPAC.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Is the security of information systems regularly reviewed?*
- *Are these reviews performed against the agencies security policies?*
- *Are all security processes and procedures carried out correctly? Is this regularly reviewed?*
- *Are results of reviews recorded, maintained and reported?*
- *Are independent reviews carried out? What action is taken for non-compliance?*

11.3 Audit Requirements

The audit requirements domain includes all audit activities relating to information security activities.

Tasmanian Government Mandatory Clause

All reasonable steps are taken to monitor, review and audit agency information security compliance, including the assignment of appropriate security roles and engagement of internal and/or external auditors and specialist organisations where required.

Agency Clauses

[*Insert agency specific clauses*].

Agencies should also consider the following:

- *Are controls established to safeguard operational systems and audit tools during audits?*
- *Are controls established to safeguard the integrity and prevent misuse of audit tools?*
- *Are audits planned to minimise the risk of disruptions to business processes?*