Tasmanian Government Information Security Policy *and* Manual

VERSION 1.0 APPROVED APRIL 2011
VERSION 1.1 ABRIDGED PENDING REVIEW JANUARY 2020

Department of Premier and Cabinet

Tasmanian Government

Contents

SECTION 1
Introduction

The Tasmanian Government's Information Security Framework sets out the Tasmanian Government's approach to managing information security. The Framework is based on a risk management approach and requires agencies to implement policies and procedures that are proportionate to the level of risk. The Framework comprises a suite of documents that together provide a comprehensive approach to managing information security risks.

This *Tasmanian Government Information Security Policy and Manual* (Manual) defines the high-level policy and supporting procedures and guidance for implementation by Tasmanian Government agencies and in a whole-of-government context. The Manual also includes information on standards, codes of practice and legislation to assist with Policy implementation. The Policy (refer to section 2) sets out broad level requirements for information security. Agencies are encouraged to manage information security risks in the context of general business risks within their agencies. Procedures (refer to section 3) provide detailed information about minimum requirements for Policy implementation, including mandatory and recommended procedures.

MANDATORY PROCEDURES are highlighted in blue text boxes.

Resources (refer to section 4) reference useful material to support implementation of Procedures in accordance with the Policy. References to standards, codes of practice, handbooks, legislation and other sources referenced in the Procedures are included.

Standards and handbooks published by Standards Australia and referenced in the Manual are available to agencies free-of-charge using the **Standards Select Online** service provided by the Department of Premier and Cabinet's Digital Strategy and Services division and available through: www.dpac.tas.gov.au/divisions/digital_strategy_and_services/services/standards_select_online_service.

1.1 POLICY AUTHORITY

The Policy was endorsed by Cabinet in 2011. Procedures were endorsed by the [former] ICT Policy Board, being the predecessor of the Tasmanian Government's Digital Services Board (DSB).

1.2 TERMINOLOGY

The terminology used in this Manual indicates whether policy and procedure statements are mandatory, conditional or recommended, as follows:

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 or RECOMMENDED	The item is encouraged or suggested.

Agencies deviating from MUST or MUST NOT statements MUST advise the [Deputy Secretaries Digital Services Committee (DSDSC)] of the decision to waive particular requirements.

Agencies deviating from SHOULD or SHOULD NOT statement MUST record:

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

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

1.3 ROLES AND RESPONSIBILITIES

Each Tasmanian Government Head of Agency is responsible for implementation of the Policy and Procedures in their agency. While Procedures reference legislation relevant to information security, this does not reduce the requirement for each agency to be aware of the full extent of legislation that applies to its business or activities.

Agencies that deliver or manage contracts for the delivery of whole-of-government services are responsible for the implementation of the Policy for the whole-of-government components of those services.

The agency that is the original custodian of information is responsible for the security of that information where it is part of a service delivered by another agency.

SECTION 2

Information Security Policy Statement

2.1 PURPOSE

The purpose of this Policy is to provide a consistent approach to managing information security risks across the Tasmanian Government.

2.2 SCOPE

This Policy applies to Tasmanian Government agencies as custodians of information on behalf of the Crown.

2.3 POLICY PRINCIPLES

Agencies MUST apply this Policy in accordance with Policy Principles, which are:

Availability:	information is accessible and useable to authorised entities
Integrity:	the accuracy and completeness of information is protected
Confidentiality:	information is not made available or disclosed to unauthorised individuals, entities or processes
Proportionality:	measures to protect information are relative to the risk of loss or failure of availability, integrity and confidentiality

2.4 POLICY STATEMENT

The Policy is mandatory and is to be applied across the following seven areas:

a) Governance and management

Each Head of 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.

b) Risk management

Each agency MUST conduct regular information security risk assessments and implement appropriate risk management strategies proportionate to the level of identified risk.

c) 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.

d) Identity and access management

Each agency MUST ensure authorised access and prevent unauthorised access to information assets.

Each agency MUST ensure that the identities of employees and others who wish to access agency services are assessed using the Tasmanian Government Identity and Access Management Toolkit [also under review].

e) Personnel and awareness

To minimise the risk of information misuse, each agency MUST ensure staff understand the information security roles and responsibilities assigned to them. Agencies MUST also ensure that these roles and responsibilities are appropriate for level of duties performed by the staff member.

f) Incident management

Each agency MUST have a structured approach to managing information security incidents and events that have potential to breach information security policy or compromise operations.

g) Business continuity management

Each agency MUST have a structured approach, based on an information security risk assessment, to managing business continuity to ensure the uninterrupted availability of all resources that support essential business activities.

2.5 POLICY APPLICATION

The Manual contains Procedures to support application of the Policy, including mandatory and recommended requirements.

SECTION 3
Information Security Procedures

3.1 GOVERNANCE AND MANAGEMENT PROCEDURES

a) Purpose

To assist agencies to implement appropriate information security governance and management procedures in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and Policy sections of this Manual. Each agency is also to consider legislation and policy relevant to its business that could impact on its information security governance.

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

d) Procedures

i. Agency Information Security Committee

Each agency MUST govern application of the Policy with an internal 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.

ii. Information Security Management System (ISMS)

Agencies SHOULD implement an Information Security Management System (ISMS) using *AS/NZS ISO/IEC 27001:2006* [or equivalent]. This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organisation's overall business activities and risks. An overview of the ISMS family of standards and related terminology is available in *ISO/IEC 27000:2009*.

iii. Agency Information Security Officers

Agencies SHOULD appoint designated Agency Information Security Officer/s, whose role is to coordinate:

- implementation of agency information security policies and plans
- delivery of information security communication, education and training, and
- investigation of information security incidents.

Agencies may have several designated Agency Information Security Officers covering different areas. For example, separate officers may be responsible for cybersecurity, 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.

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

ISO/IEC 27000:2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary
AS/NZS ISO/IEC 27001:2006 Information Technology – Security techniques – Information management systems – Requirements
AS/NZS ISO/IEC 27002:2006 Information Technology – Security techniques – Code of Practice for information security management

3.2 RISK MANAGEMENT PROCEDURES

a) Purpose

To assist agencies to implement appropriate information security risk management procedures in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and Policy sections of this Manual. 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 these risks. Information security risk management can be undertaken as part of a broader agency risk management approach.

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

d) Procedures

i. Risk management

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

Agencies use AS/NZS ISO 31000:2009 [or equivalent] to guide risk management.

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

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.

After completing a risk assessment there may be residual information security risks where the agency has:

- elected to accept a risk by doing nothing, or
- adopted a mitigation strategy that does not completely eliminate a risk.

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

AS/NZS ISO 31000:2009 Risk management – Principles and guidelines
Standards Australia HB 231:2004 Information security risk management guidelines
Standards Australia HB 327:2010 Communicating and consulting about risk (Companion to AS/NZS ISO 31000:2009)

3.3 RESOURCE MANAGEMENT PROCEDURES

3.3.1 RECORD SECURITY PROCEDURES

a) Purpose

To assist agencies to implement appropriate resource management procedures, specifically relating to record security, in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and Policy sections of this Manual.

As custodians of Crown records, agencies or statutory bodies have a responsibility to maintain appropriate record security arrangements and enable secure access to records. As custodians of information owned by other entities, agencies have an obligation to identify and respect the information security procedures required by those entities.

These procedures have been developed to be consistent with the *Archives Act 1983* and guidelines and advices issued under that legislation. The State Archivist has endorsed AS ISO 15489 as a model for best practice record-keeping in Tasmanian state and local government organisations.

Record security guidelines apply to all records, whether paper-based or electronic, and include information held in databases. The *Archives Act 1983* describes a record as:

> *…a document or an object that is, or has been, made or kept by reason of any information or matter that it contains or can be obtained from it or by reason of its connection with any event person, circumstance, or thing … [and it]… includes any printed or written material and an object includes a sound recording, coded storage device, magnetic tape or disc, microfilm, photograph, film, map, plan, or model or painting or other pictorial or graphic work.*

Each agency is also to consider legislation and policy relevant to its business or activities that could impact on record security.

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

d) Procedures

i. Records management

The *Archives Act 1983* (section 10) places a responsibility on Heads of Agencies to keep proper records of business activities.

> Section 11 of the *Archives Act 1983* requires that Heads of Agencies, 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.

Agencies SHOULD refer to guidelines and advices issued under the *Archives Act 1983* and relevant sections of AS/NZS ISO/IEC 27002:2006 and AS ISO 15489 [or equivalent] to appropriately protect records.

Also refer to Physical Environment and Information and Communications Technology sections of this Manual for more guidance on records management.

ii. Legislation

> 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.

It is RECOMMENDED that agencies consider the following list of legislation [or equivalent] that applies to all agencies when implementing these guidelines:

Legislation	Provision
Archives Act 1983	To achieve accountability in public administration by prohibiting the unauthorised destruction or manipulation of records. Includes responsibilities for the creation, maintenance, access, retention and disposal of records.
Audit Act 2008	To ensure the Auditor-General can perform the necessary functions including maintaining the confidentiality of information.
Criminal Code Act 1924	Prohibited criminal activity, including fraud.
Electronic Transactions Act 2000	Enables the acceptance of transactions in electronic form, including signatures.
Evidence Act 2001	Enables records kept in electronic format to be admissible as evidence in court proceedings.
Financial Management and Audit Act 1990	Accounting and audit requirements.
Right to Information Act 2009	Gives the public the right to obtain information contained in the records of the Government and its agencies. Information may be exempt from release under the Act if certain criteria are met.
Libraries Act 1984	Legal deposit: copies of published documents are to be provided to the State Library of Tasmania.
Ombudsman Act 1978	Investigation of complaints with respect to administrative actions taken by or on behalf of certain government agencies.

Legislation	Provision
Personal Information Protection Act 2004	Management of personal information collected and stored by agencies. Right to access and amend information by the person to whom the information relates.
Public Account Act 1986	Management of the Public Account of the State.
State Service Act 2000	Code of Conduct, Section 9 (7), states that an employee is to maintain appropriate confidentiality about dealings of, and information acquired by, the employee. Similar requirements may exist in other legislative conditions of employment (eg *Police Service Act 2003*).
Workplace Health & Safety Act 1995	Requirement to maintain records for plant and equipment etc and accident records.

iii. Retention, disposal and transfer

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 Archives Office of Tasmania in accordance with Section 11 of the *Archives Act 1983*. 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 Archives Office of Tasmania Guideline 4 – Agency Determination of Access Restrictions.

Agencies MUST comply with the following Archives Office of Tasmania 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.

It is RECOMMENDED that agencies use appropriate equipment endorsed by the Australian Government Security Construction and Equipment Committee for the destruction of paper records, electronic media or equipment. Also refer to controls in 3.3.4 Information and Communications Technology for disposal of electronic media.

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

AS/NZS ISO/IEC 27002:2006 Information Technology – Security techniques – Code of Practice for information security management
AS ISO 15489.1:2002 Records Management – Part 1. General
AS ISO 15489.2: 2002 Records Management – Part 2. Guidelines
Archives Office of Tasmania guidelines and advices

Tasmanian legislation

3.3.2 INFORMATION SECURITY CLASSIFICATION PROCEDURES

a) Purpose

To assist agencies to implement appropriate resource management procedures, specifically relating to information security classification, in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and Policy sections of this Manual.

Procedures include a standard set of classification definitions, markings and procedures for providing appropriate access to information assets. Security classification is useful to reduce the risk associated with transfer of information between Tasmanian Government agencies or to external organisations.

This classification does not displace other business or security classifications and can operate in parallel with other classifications, for example the National Security Classification. It is independent and separate from assessments that may be required under legislation, for example the *Right to Information Act 2009*.

Each agency is to also consider legislation and policy relevant to its business or activities that could impact on information security classification.

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

d) Procedures

i. Applying information security classification markings

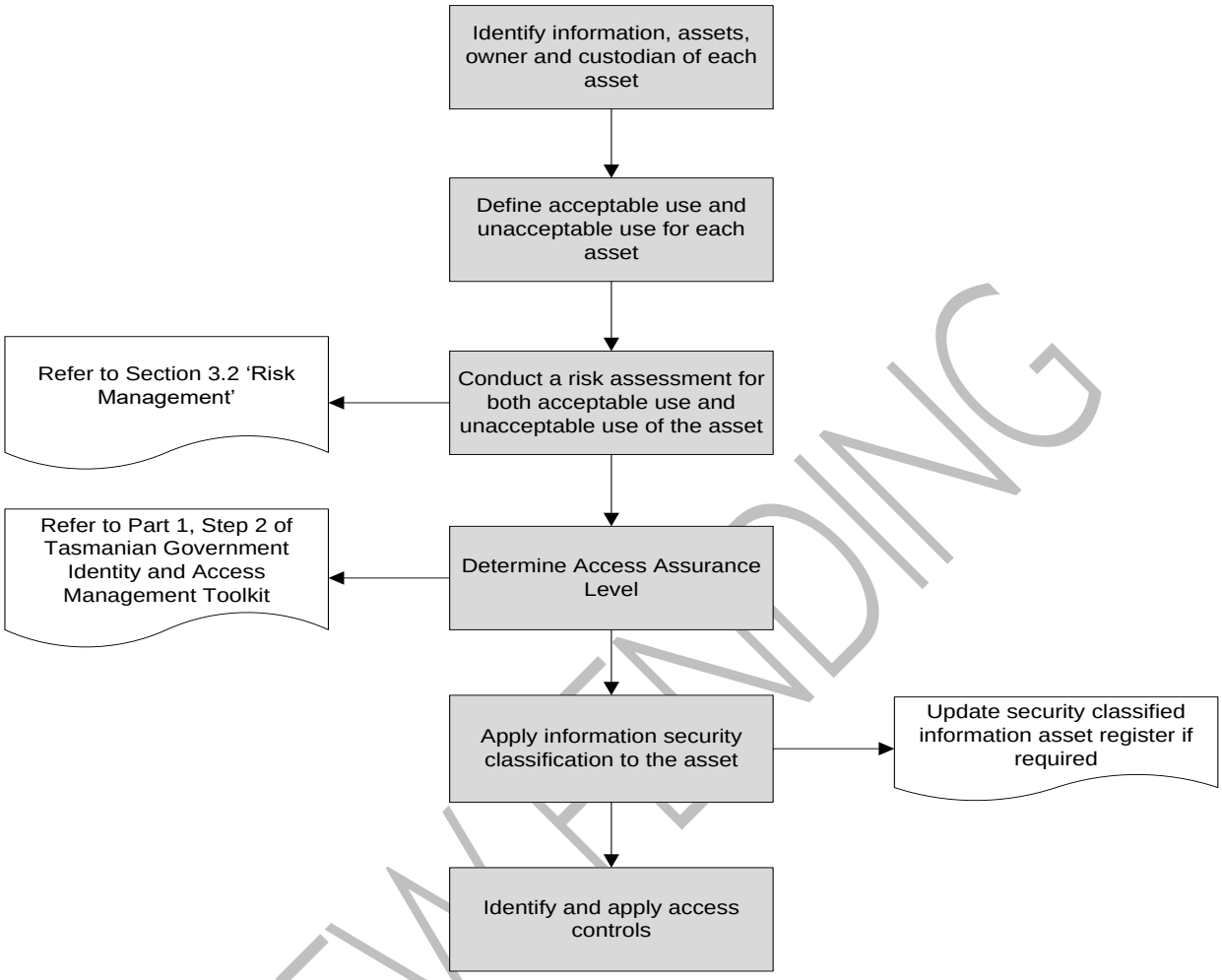
If an agency is not obliged to use other information security classification marking and handling, then it MUST conduct a risk assessment to determine the appropriate marking and handling in accordance with this *Tasmanian Government Information Security Policy and Manual*.

Information security classification markings are appropriate when the consequences of improper use of the information warrant the cost of increased protection. Inappropriate over-classification has the following consequences:

- unnecessary restrictions on public access to government information
- unnecessary restrictions on agency operations
- unnecessary cost to administer information, and
- classification and security procedures being devalued or ignored.

Five information security classification levels are defined in these procedures: PUBLIC, UNCLASSIFIED, X-IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED.

The following steps are RECOMMENDED when conducting information security classification. Agencies SHOULD refer to the *Tasmanian Government Identity and Access Management Toolkit* [also under review] for more information regarding identity Access Assurance Levels (AALs).



Part I of the *Tasmanian Government Identity and Access Management Toolkit* identifies the link between information security classification levels and AALs as follows:

Record security classification and corresponding minimum AALs)				
PUBLIC	UNCLASSIFIED	IN CONFIDENCE	PROTECTED	HIGHLY PROTECTED
AAL-0 No Assurance	AAL-1 Minimal Assurance	AAL-2 Low Assurance	AAL-3 Moderate Assurance	AAL-4 High Assurance

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.

Agencies SHOULD conduct an audit of highly protected assets at irregular intervals to ensure they are being managed in accordance with these guidelines. A regular review of all assets with lower levels of protection may not be required; assessing the classification of these on a case-by-case basis may be sufficient.

Information received from an external organisation SHOULD be handled in accordance with the security classification applied by the external party (where known).

Information SHOULD NOT be reclassified without the consent of the information owner/custodian.

The sender of security-classified information has an obligation to inform the recipient of their responsibilities in regard to handling procedures associated with a marking; therefore, agencies SHOULD include definitions or instructions on where to locate definitions of markings when transferring security classified information.

ii. Security classified record registers

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.

The RECOMMENDED specification for a security classified information asset register is tabled below:

Register Item	Description of item	PROTECTED	HIGHLY PROTECTED
Identifier	Name or identifier of the information asset	✓	✓
Description	Description of information asset	✓	✓
Owner/custodian	The owner/custodian of the asset	✓	✓
Location	Current location of the asset	✓	✓
Security classification	Security classification of the asset	✓	✓
Classification commences	Date that the security classification commenced	✓	✓
Classification review	Date that the classification of the asset is to be reviewed	✓	✓
Copies	Number of copies of the asset		✓
Copy distribution	Names of persons and copy number distributed to that person		✓
Disposed	Date at which the asset was disposed		✓

iii. Tasmanian Government Information Security Classification

The following pages provide definitions of and handling procedures for PUBLIC, UNCLASSIFIED, X-IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED markings.

PUBLIC

Information that has been authorised by the owner/custodian for public access and circulation.

It is important that agencies maintain the integrity and availability of PUBLIC information. Until public access is authorised, it is common for information to have some access restrictions applied by using a non-public security classification. No assurance regarding the identity of individuals accessing PUBLIC information is required (Access Assurance Level 0).

Compromise could cause loss of confidence in the Government and limited damage to commercial entities or members of the public.

PUBLIC does not mean that information will be supplied to the general public free-of-charge in all cases.

Examples of PUBLIC information include: publications and public registers.

Preparation and processing

- Markings: distinct markings on document or asset if required, eg centre bottom of each page, in capitals, 5 mm (20 point), bold if possible.
- Page numbering: optional, but generally helpful.
- Date and time of last update: optional, but generally helpful.
- Electronic preparation: in disk drive, web content management system or document and records management system with restricted access is desirable.
- Printing: no specific requirements.
- Copying: no specific requirements.
- Electronic publication: web content management system, electronic register or equivalent with access restricted to authorised personnel is essential.
- Filing: in accord with normal records management practices.
- Security classified record register: not required.
- Audit logging: logging access to electronic publication systems is essential, ie login, logout, failed login attempt, modify, create and delete.
- Removal from workplace: as required.

Storage

- Physical storage: no specific requirements.
- Electronic storage: as for preparation and processing.

Archive

- In accordance with retention and disposal schedule authorised by the State Archivist.
- The Libraries Act 1984 requires agencies to deposit copies of publication documents with the State Library of Tasmania.

Disposal

- Paper waste: no specific requirements.
- Electronic media and equipment: may contain information of other classifications, therefore as per Information and Communications Technology section of this Manual.

Manual transmission

- Within the Tasmanian Government: no specific requirements.
- Outside the Tasmanian Government: no specific requirements.
- Receipting: no specific requirements.
- Electronic transmission
- Data transmission: may be passed unencrypted over Tasmanian Government or public networks.
- Portable media/devices: no specific requirements.
- Email, instant message: no specific requirements.
- Fax: no specific requirements.
- Receipting: optional.

Discussion

- Meetings, telephone, video conference: no specific requirements.

UNCLASSIFIED

UNCLASSIFIED information may need to be protected and controlled and is not to be considered PUBLIC information. Official information needs to be specifically classified as PUBLIC before it is released into the public domain.

As a minimum, UNCLASSIFIED information requires only minimal confidence in the identity of the individual accessing the information (Access Assurance Level 1).

The unauthorised disclosure or compromise of UNCLASSIFIED information may undermine public confidence in government operations.

Preparation and processing

- Markings: if required, distinct markings on document or asset, eg centre bottom of each page, in capitals, 5 mm (20 point), bold if possible.
- Page numbering: optional, but generally helpful.
- Date and time of last update: optional, but generally helpful.
- Electronic preparation: in disk drive or electronic document and records management system with restricted access.
- Printing: no specific requirements.
- Copying: to be kept to a minimum in accord with operational requirements.
- Filing: in accord with normal records management practices.
- Security classified record register: not required.
- Audit logging: checking of access control logs as required, ie login, logout, failed login attempt.
- Removal from workplace: only on a basis of need.

Storage

- Physical storage: may be stored in unsecured cabinet in a room for authorised personnel.
- Electronic storage: access by authorised personnel only.

Archive

- In accordance with retention and disposal schedule authorised by the State Archivist.

Disposal

- Paper waste: destruction by shredding is optional.
- Electronic media and equipment: as per Information and Communications Technology section of this Manual.

Manual transmission

- Within the Tasmanian Government: uncovered by hand or by internal mail in a use-again envelope.
- Outside the Tasmanian Government: Passed by external mail in an opaque envelope.
- Receipting: no specific requirements.

Electronic transmission

- Data transmission: may be passed unencrypted over Tasmanian Government or public networks.
- Portable media/devices: password-protected, eg USB drive, CD ROM, smart phone.
- Email, instant message: no specific requirements.
- Fax: no specific requirements.
- Receipting: optional.

Discussion

- Meetings, telephone, video conference: on the basis of need-to-know.

X-IN-CONFIDENCE

Information that if compromised could cause limited damage to the State, the Government, commercial entities or members of the public. As a minimum, requires a low level of confidence in the identity of the individual accessing the information (Access Assurance Level 2). Compromise could: cause distress to individuals or private entities; cause financial loss or loss of earning potential, or facilitate improper gain or advantage; prejudice the investigation or facilitate the commission of crime; breach undertakings to maintain the confidentiality of information provided by third parties; impede the effective development or operation of government policies; breach statutory restrictions on the management and disclosure of information; disadvantage the Government in commercial or policy negotiations with others; and/or undermine the proper management of the public sector and its operations.

This protective marking includes a notification of the subject matter (X), which alludes to its audience and the need-to-know principle (this does not include CABINET-IN-CONFIDENCE, see PROTECTED). Examples include:

STAFF-IN-CONFIDENCE: includes all official staff records where access would be restricted to HR personnel and nominated authorised staff. For example, personnel files, recruitment information, grievance or disciplinary records.

EXECUTIVE-IN-CONFIDENCE: information associated with executive management of the entity that would normally be restricted to the executive and nominated authorised staff. For example, sensitive financial reports, strategic plans, government matters, staff matters etc.

COMMERCIAL-IN-CONFIDENCE: procurement or other commercial information such as sensitive intellectual property. For example, draft requests for offer information, tender responses, tender evaluation records, designs and government research.

Preparation and processing

- Markings: distinct markings on document or asset, eg centre bottom of each page, in capitals, 5 mm (20 point), bold if possible.
- Page numbering: desirable.
- Date and time of last update: optional, but generally helpful.
- Electronic preparation: in disk drive or electronic document and records management system with restricted access.
- Printing: printer not to be left unattended while documents are being printed and avoid over-viewing.
- Copying: may be prohibited by information owner/custodian. To be kept to a minimum in accord with operational requirements.
- Filing: in accord with normal records management practices.
- Security classified record register: not required.
- Audit logging: checking of access control logs as required, ie login, logout, failed login attempt, create and delete.
- Removal of file or document: on basis of need. To be kept in personal custody. Ensure adequate storage arrangements are available.

Storage

- Physical Storage: in a lockable cabinet or room when unattended. See Physical Environment section of this Manual.
- Electronic Information Storage: restrict logical access based on need to know.

Archive

- In accordance with retention and disposal schedule authorised by the State Archivist.

Disposal

- Paper waste: destruction by cross-cut shredding.
- Electronic media and equipment: as per the Information and Communications Technology section of this Manual.

Manual transmission

- Within the Tasmanian Government: single opaque envelope indicating classification. Uncovered by hand in discrete office environment.
- Outside the Tasmanian Government: single opaque envelope that does not indicate classification.
- Receipting: at discretion of information owner/custodian.

Electronic transmission

- Data transmission: may be passed unencrypted over Tasmanian Government or public networks.
- Portable media/devices: password-protected eg USB drive, CD ROM, smart phone.
- Email, instant message: no specific requirements.
- Fax: someone to attend the receiving facsimile to receive the material. Encryption desirable.
- Receipting: at discretion of data owner/custodian

Discussion

- Meetings, telephone video conference: ensure that people without a need to know are not able to overhear discussions or overview equipment and materials. Clear equipment prior to vacating room.

PROTECTED

Information that if compromised could cause damage to the State, the Government, commercial entities or members of the public. As a minimum, requires a moderate level of confidence in the identity of the individual accessing the information (Access Assurance Level 3). For instance, compromise could: endanger individuals and private entities; work substantially against government finances or economic and commercial interests; substantially undermine the financial viability of major organisations; impede the investigation or facilitate the commission of serious crime; and/or seriously impede the development or operation of major government policies.

Generally, most non-national security information would be adequately protected by the procedures given to information marked X-IN-CONFIDENCE or PROTECTED. Includes Cabinet submissions and decisions to be marked CABINET-IN-CONFIDENCE.

Preparation and handling

- Markings: distinct markings on document or asset eg centre bottom of each page, in capitals, 5 mm (20 point), bold if possible.
- Page numbering: desirable.
- Date and time of last update: desirable.
- Electronic preparation: in disk drive or electronic document and records management system with restricted access.
- Printing: printer not to be left unattended while documents are printed and avoid over-viewing.
- Copying: may be prohibited by information owner/custodian. To be kept to a minimum in accordance with operational requirements. Copies to be numbered and registered.
- Filing: in accord with normal records management practices. To be placed in appropriate file without delay.
- Security classified record register: registration essential.
- Audit logging: regular checks of the Security Classified Information Register are desirable. Regular checks of access control logs are desirable, ie user login, logout, failed login attempt, read, write, create, modify and delete.
- Removal from workplace: basis of need, but not recommended. Authorisation of information owner/custodian required. To be kept in personal custody. Ensure adequate storage arrangements are available.

Storage

- Physical storage: in a lockable container in a secure or partially secure environment when unattended. See Physical Environment section of this Manual.
- Electronic information storage: restrict logical access based on need to know.

Archive

- In accordance with retention and disposal schedule authorised by the State Archivist.

Disposal

- Paper waste: secure destruction using a Class B shredder rated by the Australian Government Security Construction and Equipment Committee.
- Electronic media and equipment: as per the Information and Communications Technology section of this Manual.

Manual transmission

- Within the Tasmanian Government: single opaque envelope indicating classification. Uncovered by hand directly between authorised members of staff in discrete office environment. To remain in personal custody during transmission.
- Outside the Tasmanian Government: double enveloping (ie sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); inner envelope is to be sealed with an Australian Government Security Construction and Equipment Committee-endorsed tamper-proof seal. To remain in personal custody during transmission.
- Receipting: required.

Electronic transmission

- Data transmission: to be encrypted over public networks. Encryption is desirable over Tasmanian Government networks. End-to-end encryption is desirable, eg PC to PC.
- Portable media/devices: to be encrypted, eg USB drive, CD ROM, smart phone.
- Email, instant message: information to be a separate and encrypted attachment.
- Fax: someone to attend the receiving facsimile to receive the material. Encryption required.
- Receipting: required
- Refer to the Information and Communications Technology section of this Manual.

Discussion

- Meetings, telephone, video conference: to occur behind closed doors in fully enclosed rooms. Ensure people without a need to know are not able to overhear discussions or over-view equipment and materials. Notify audience of the classification and that recording is not permitted. Materials to include classification markings. Clear equipment and whiteboards prior to vacating room. See Physical Environment section of this Manual.

HIGHLY PROTECTED

Information that requires a substantial degree of protection as compromise of the information could cause serious damage to the State, the Government, commercial entities or members of the public. As a minimum, requires a high level of confidence in the identity of the individual accessing the information (Access Assurance Level 4). For instance, compromise could: threaten life directly; seriously prejudice public order; and/or substantially damage government finances or economic and commercial interests.

Generally, very little information belongs in the HIGHLY PROTECTED category.

Preparation and handling

- Markings: distinct markings on document or asset eg centre bottom of each page, in capitals, 5 mm (20 point), bold if possible.
- Page numbering: essential in the form of 'Page n of x' where x is the total number of pages.
- Date and time of last update: essential.
- Electronic preparation: in disk drive or electronic document and records management system with restricted access or on standalone equipment.
- Printing: printer not to be left unattended while documents are being printed and avoid over-viewing.
- Copying: may be prohibited by information owner/custodian. To be kept to a minimum in accord with operational requirements. Copies to be numbered and registered.
- Filing: in accord with appropriate records management practices. To be placed in appropriate file without delay.
- Security classified record register: registration is essential for all copies.
- Audit logging: regular checks of the Security Classified Information Register are essential. Regular checks of access control logs essential, ie user login, logout, failed login attempt, read, write, create, modify and delete.
- Removal from workplace: basis of need, but not recommended. Authorisation of information owner/custodian required. To be kept in personal custody at all times. Ensure adequate storage arrangements are available. Maintain a record of removal in the Security Classified Information Register.

Storage

- Physical storage: in a lockable container in a secure area when unattended. See Physical Environment section of this Manual.
- Electronic information storage: restrict logical access based on need to know.

Archive

- In accordance with retention and disposal schedule authorised by the State Archivist.
- Electronic media and equipment: as per Information and Communications Technology section of this Manual.

Manual transmission

- Within the Tasmanian Government: single opaque envelope indicating classification. Uncovered by hand directly between authorised members of staff in discrete office environment. To remain in personal custody during transmission.
- Outside the Tasmanian Government: double enveloping (ie sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); inner envelope is to be sealed with an Australian Government Security Construction and Equipment Committee endorsed tamper-proof seal. To remain in personal custody during transmission.
- Receipting: required

Electronic transmission

- Data transmission: to be encrypted over public and Tasmanian Government networks. End-to-end encryption is desirable, eg PC to PC.
- Portable media/devices: to be encrypted eg USB drive, CD ROM, smart phone.
- Email, instant message: the last resort for distribution unless the information is a separate and encrypted attachment.
- Fax: someone to attend the receiving facsimile to receive the material. Encryption required.
- Receipting: required
- See Information and Communications Technology section of this Manual.

Discussion

- Meetings, telephone, video conference: to occur behind closed doors in fully enclosed rooms. Ensure that people without a need to know are not able to overhear the discussions or over-view equipment or materials. Notify audience of the classification and that recording is not permitted. Materials to include classification markings. Clear equipment and whiteboards prior to vacating room. See Physical Environment section of this Manual.

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

Tasmanian Government Identity Access Management Toolkit
Australian Government Security Construction and Equipment Committee Security Equipment Catalogue
Example transition plan for new information security classification and record security procedures
Tasmanian legislation

3.3.3 PHYSICAL ENVIRONMENT PROCEDURES

a) Purpose

To assist agencies to implement appropriate resource management procedures, specifically relating to the physical environment, in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and the Policy provided in this manual.

Protecting physical assets from unauthorised access includes issues such as:

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

Each agency is to also consider legislation and policy relevant to its business or activities that could impact on the physical environment.

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

d) Procedures

i. Physical environment controls

To prevent unauthorised physical access to Tasmanian Government information assets requires protection of facilities, information and people from damage or interference.

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

Agencies SHOULD use AS/NZS ISO/IEC 27002: 2006 [or equivalent] for general guidance on physical and environmental security controls. Note that while this standard recommends a 'clear desk' or 'clear screen' policy, it is RECOMMENDED that this is only applied by agencies in appropriate situations. For example, it may be inappropriate in hospitals where continuous access to information is required.

ii. Entry control and visitor control

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.

Entry control by personal recognition

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

- alert and responsible doorkeepers are regularly employed on the same duty and they are 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.

Entry control by identity pass

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, and
- 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.

Visitor control in high-risk areas

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.

iii. Identification of personnel keeping unusual hours

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.

iv. Buildings and secure areas

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

v) Planning accommodation

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.

vi) Secure zones within buildings

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

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

vii) Managing the risk of overhearing

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.

Telephone/video call or conference

Videoconferencing presents the same risks of overhearing. It is recommended 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 office design and what may be visible/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.

viii) Managing the risk of over-viewing from outside

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.

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.

ix) Ancillary staff

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

x) Room security

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, and
– 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.

xi) Room checks by occupants at close of work

Occupants SHOULD check all rooms at the close of work to ensure that sensitive documents, including sensitive waste, have been properly locked away in security containers and security keys mustered. 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.

xii) Conferences and meetings

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

- prior to commencing the meeting, ensure that unauthorised people are not present
- ensure that no sensitive information or waste remains in the room at the close of the meeting
- when representatives of outside organisations are present, preclude the possibility of official documents being 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.

xiii) Home-based work environments

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.

xiv) Mail and other delivery areas

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.

xv) Asset management

Treasurer's Instructions issued under the *Financial Management and Audit Act 1990* relating to the management of assets should be followed [updated references to be included].

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

AS/NZS ISO/IEC 27002:2006 Information Technology – Security techniques – Code of Practice for information security management
Treasurer's Instructions
Tasmanian legislation

3.3.4 INFORMATION AND COMMUNICATIONS TECHNOLOGY PROCEDURES

a) Purpose

To assist agencies to implement appropriate resource management procedures, specifically relating to information and communications technology (ICT), in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and the Policy provided in this manual.

Each agency is to consider legislation and policy relevant to its business or activities that could impact on ICT.

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

d) Procedures

i. ICT controls

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.

Agencies SHOULD identify and treat risks associated with ICT by referring to AS/NZS ISO/IEC 27002:2006 [or equivalent].

ii. Access control

Agencies SHOULD ensure that controls applied to privileged users and associated audit logs are more comprehensive than for other users. Privileged users have the potential to impersonate other users; therefore, secure audit trails 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 The Archives Office of Tasmania *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.

iii. Acquisition development and maintenance

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 [updated references to be included] Instructions for Common use and/or whole-of-government contracts: goods and Government Information Technology Conditions [or equivalent].

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.

iv. Cryptographic protocols

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

v. Disposal

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

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 (eg. computers) MUST be disposed of in accordance with [the relevant] Treasurer's Instructions, issued under the *Financial Management and Audit Act 1990.*

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* [or equivalent].

It is RECOMMENDED that agencies use equipment endorsed by the Australian Government Security Construction and Equipment Committee [or equivalent] for the destruction or sanitisation of electronic media or equipment. See the *Australian Government Security Construction and Equipment Committee Security Equipment Catalogue* [or equivalent] for more details.

Media Type	Media reuse or disposal method	
	PUBLIC, UNCLASSIFIED or IN-CONFIDENCE	PROTECTED or HIGHLY PROTECTED
Optical disks eg CD or DVD Microfilm Microfiche	Physical destruction	One, or a combination of: • Physical destruction (shredding) • Incineration
Electrostatic devices eg laser printer or copier drums	Reuse or disposal without destruction or sanitisation	One, or a combination of: • Sanitised by printing a quantity of non-sensitive information prior to disposal (or recycling) • Physical destruction
Magnetic media eg hard disk drives, floppy disks, tapes, photo copies or multifunction copier/printer devices	Low-level formatting or similar activity (do not use 'quick' format methods)	One, or a combination of: • Low-level formatting or similar activity (do not use 'quick' format methods) • Demagnetisation to render useless • Physical destruction
Personal electronic devices or flash ROM eg mobile phones, SIM cards, USB flash drives, memory stick, camera cards	Low-level formatting or similar activity (do not use 'quick' format methods)	One, or a combination of: • Low-level formatting or similar activity (do not use 'quick' format methods) • Physical destruction

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

AS/NZS ISO/IEC 27002:2006 Information Technology – Security techniques – Code of Practice for information security management
Standards Australia HB 171:2003 Guidelines for the management of IT evidence
State Service Act 2000 Ministerial Direction No. 10:2003 Internet and email use by State Service officers and employees
Tasmanian Government WAN and Internet Services Information Security Policies and Standards
Treasurer's Instructions
Tasmanian legislation
Australian Government Information Security Manual [or equivalent]
Archives Office of Tasmania Disposal Schedule for Common Administrative Functions
Australian Government Security Construction and Equipment Committee Security Equipment Catalogue [or equivalent]

3.4 IDENTITY AND ACCESS MANAGEMENT PROCEDURES

a) Purpose

To assist agencies to implement appropriate identity and access management procedures in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and Policy sections of this Manual

Each agency is also to consider legislation and policy relevant to its business or activities that could impact on identity and access management procedures.

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

This procedure applies to a service or information that is:

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

d) Procedures

i. Identity and access management

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

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.*

Agencies MUST determine appropriate access assurance levels in accordance with the *Personal Information Protection Act 2004* particularly Personal Information Protection Principle 1, which specifies that a personal information custodian may only collect personal information where it is necessary for one or more of its functions or activities.

See the Information and Communications Technology section of this Manual for more procedures regarding access control.

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.

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

Tasmanian Government Identity and Access Management Toolkit
Tasmanian legislation

3.5 PERSONNEL AND AWARENESS PROCEDURES

a) Purpose

To assist agencies to implement appropriate personnel, communication and awareness procedures in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and Policy sections of this Manual

Each agency is also to consider legislation and policy relevant to its business or activities that could impact on personnel, communication and awareness procedures.

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

Agency personnel security controls apply to employees, contractors, volunteers, students and others who have authorised access to agency information assets.

d) Procedures

i. Personnel

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

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.

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

Legislation that may be applicable to agencies in the implementation of personnel information security policies include the following [or equivalent/s]:

- *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.

ii. 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.

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

iii. Assigning personnel responsibilities for information security

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.

iv. Compliance and monitoring

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

v. Communication and awareness

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

Agencies SHOULD use relevant sections of AS/NZS ISO/IEC 27002:2006 [or equivalent] for communication and awareness procedures.

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

- using the Agency Information Security Officer to facilitate communications where appropriate
- highlighting to personnel relevant parts of their Statement of Duties or contract
- providing personnel with a copy of the State Service Code of Conduct. and
- providing regular reminders to personnel of their information security responsibilities. These may include: newsletters to personnel on their responsibilities highlighting current issues and risks; and displaying prominent messages, eg. on computer login screens, on file covers or on filing cabinets.

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

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

AS/NZS ISO/IEC 27002:2006 Information Technology – Security techniques – Code of Practice for information security management
Tasmanian legislation
State Service Code of Conduct
State Service Commissioner's Directions
Ministerial Directions and Determinations
Tasmanian Government Identity Access Management Toolkit

3.6 INCIDENT MANAGEMENT PROCEDURES

a) Purpose

To assist agencies to implement appropriate information security incident management procedures in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and Policy sections of this Manual

An information security event is 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.

Each agency is to also consider legislation and policy relevant to its business that could impact on incident management.

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

d) Procedures

i. Incident management controls

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

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.

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

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

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.

ii. Treasurer's Instructions

When developing information security incident reporting procedures, where applicable agencies MUST consider the [relevant] Treasurer's Instructions issued under the *Financial Management and Audit Act 1990*, including those relevant to: reporting cases of illegal entry and/or damage or loss of property or money; and recording of losses.

iii. Planning for information security incidents

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.

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

AS/NZS ISO/IEC 27002:2006 Information Technology – Security techniques – Code of Practice for information security management
AS/NZS ISO/IEC 18044:2006 Information technology – Security techniques – Information security management
Standards Australia HB 171:2003 Guidelines for the management of IT evidence
Treasurer's Instructions
Tasmanian Government WAN and Internet Services Information Security Policies and Standards

3.7 BUSINESS CONTINUITY MANAGEMENT PROCEDURES

a) Purpose

To assist agencies to implement appropriate business continuity management procedures in accordance with the Policy.

b) Context

Procedures are to be read in the context of the Introduction and Policy sections of this Manual

Business continuity is the uninterrupted availability of all key resources supporting essential business functions. This includes testing plans processes and facilities that are put in place.

Each agency is to also consider legislation and policy relevant to its business that could impact on incident and business continuity management

c) Scope

Procedures apply to all Tasmanian Government agencies as defined in Schedule 1, Part 1 of the *State Service Act 2000*.

d) Procedures

i. Business continuity management controls

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

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

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

e) Resources

Relevant standards and handbooks published by Standards Australia are available to agencies free-of-charge using the Standards Select Online service (refer to section 1). Pending review:

AS/NZS ISO/IEC 27002:2006 Information Technology – Security techniques – Code of Practice for information security management
Standards Australia HB 221:2004 Business Continuity Management
Standards Australia HB 292:2006 A practitioners guide to business continuity management
Standards Australia HB 293:2006 Executive guide to business continuity management
Tasmanian Government WAN and Internet Services Information Security Policies and Standards

DOCUMENT HISTORY

Version	Date	Comments
1.1	20200120	Abridged version pending review
1.0	20110421	Authorised version – please email digital@dpac.tas.gov.au for a copy

POLICY AUTHORISATION
Tasmanian Government Cabinet

MONITORING PROGRESS OF POLICY IMPLEMENTATION
Monitoring occurs through the Tasmanian Government's digital services governance framework

POLICY MAINTENANCE
Digital Strategy and Services, Department of Premier and Cabinet

POLICY ISSUED
Version 1.0 issued 7 November 2011

REVIEW DATE
TBA

CREATIVE COMMONS STATEMENT