TAHO
Tasmanian Archive + Heritage Office

Checklist for Your Agency's Current Information Security Practices

This checklist is intended to help your agency consider how well it is managing the fundamentals of good information security. It provides a means for Agency executives to discuss the current approach of their agency with the Chief Information Officer/Information Technology Manager. It is not intended to be a comprehensive evaluation, but rather an initial exploration to stimulate further discussion on the effective management of information systems, and provide impetus for review of your agency's information security practices.

Please indicate the status of your agencies implementation; not started, Initiated, partially complete, completed, not relevant.

Information Security (IS) Milestones	***Agency Status***	***Comments***
Internal Governance		
Agency Information Security Committee has been formed		
Agency Internal governance arrangements have been documented		
Agency information Security Roles and Responsibilities have been established		
Endorsement for Internal Governance Arrangements has been obtained from senior executives/governance body		
Information Security Policy		
An information security policy has been developed		
The Policy has been endorsed by Agency executive		
The policy is regularly communicated to staff		
Information Security Plan		
An IS Plan has been developed		
IS planning is aligned with risk assessment findings		
IS plan has been endorsed by agency executives		
IS Plan has been endorsed by the IS Governance Body		
Management of risks - risks are identified, assessed, and treated within appropriate timeframes and that these practices become a core part of business activities.		
Risks are identified, assessed and treated within appropriate timeframes		

Measures to address risks are built into business activities and processes		
Asset Management		
An information Asset Register has been developed		
Information Security Classification		
Procedures for the classification of information assets have been implemented		
All information assets are assigned an appropriate classification		
Resource Management – Physical and Environmental Management - Physical security – **Physical and environmental control mechanisms are in place to prevent unauthorised access or accidental damage to computing infrastructure and systems.**		
Building and entry controls have been established		
Physical security protection controls have been implemented for all sites		
Control policies (including clear desk /clear screen) have been implemented in information processing areas that deal with security classified information		
Resource Management - Information and Communications Technology – **Good security practices are implemented, up-to-date, and regularly tested and enforced for key computer systems.**		
User access to systems is regularly reviewed to ensure they are appropriate at all times		
Network, applications and database security controls are in place, up-to-date, regularly tested and enforced		
Security software is kept up-to-date with the latest recommended updates		
Systems are patched for known vulnerabilities without delay		
Systems are configured and monitored to ensure there is no unauthorised access to or loss of information, and any fraudulent activity or inappropriate access can be readily detected		
Laptops and Portable Storage Devices (PSDs). PSDs include such devices as mobile phones, Personal Digital Assistants and flash drives. Comprehensive management, technical and physical controls over these devices is in place to minimise the risk of them being lost or stolen and of sensitive information being accessed.		
Adequate and up-to-date information about laptops and PSDs is maintained		
Basic access controls are activated as standard on laptops and PSDs		
Threats and vulnerabilities to laptops and PSDs have been assessed and policies, procedures and practices have been implemented to mitigate those risks. This will likely include deciding about:		

• Accessing external networks • Different rules for different types of information and devices • The business need for laptops and Portable Storage Devices		
Media Sanitisation – Secure removal of data from computer equipment takes place prior to disposal.		
Policies and procedures are in place, communicated to all relevant staff and third parties and consistently applied for media sanitisation.		
An assurance process in place to ensure that no sensitive data is disclosed through inappropriate disposal of computer equipment		
Wireless networks – Significant risks associated with deploying wireless networks are appropriately managed		
A wireless policy is in place whether or not a wireless network has been deployed		
Unauthorised wireless installation and access to the network is monitored whether or not a wireless network has been deployed		
Audit Capability – Security software, devices and mechanisms and key applications within agencies have adequate audit trails enabled to ensure audit capability and assist in incident detection and management.		
Change control – Change control processes are in place and consistently followed for all changes to computer systems		
All changes are subject to thorough planning and impact assessment to minimise the likelihood of problems		
Change control documentation is current, and approved changes are formally tracked		
Identity and Access Management		
Access control policy has been developed		
Agencies have developed control policies and procedures in the areas of: Authentication User access Network access Operating system access Application and information access Mobile computing and telework access		
Personal and sensitive information – An endorsed IT security policy is in place that reflects the sensitivity of the information held and the risks to that information.		
All instances of personal and sensitive information held have been identified and, based on risk assessments, there is an appropriate level of security controls over the information		
All users who will be given access to, or who have access to personal and sensitive information are appropriately authorised. Where appropriate, screening is undertaken including identity, background		

and criminal checks		
Personnel and Awareness		
Security requirements have been addressed within recruitment and selection and in SOD		
Induction program has been implemented to ensure employees agencies IS policies and procedures		
Awareness raising programs have been implemented to ensure employees are aware of and acknowledge security responsibility's		
Security obligations – All users must be made aware of their obligations under your agency's Code of Conduct regarding reasonable and appropriate use of information systems and equipment.		
All users have ready access to agency Code of Conduct and information security policies, procedures and guidelines		
All users understand and have signed appropriate confidentiality and acceptable use of information systems agreements		
Mechanisms are in place to remind users of their security responsibilities		
Incident Management – Preparation has taken place to ensure the agency can respond quickly and effectively to information security and cyber related incidents.		
Incident Response Plan is in place		
Business continuity – Preparation has taken place to ensure the agency can continue to undertake essential core services in the event of a significant incident or disaster.		
Business Continuity and Disaster Recovery Plans are in place		
Plans are tested on a periodic basis		

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

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	July 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: July 2013

Ross Latham
State Archivist