Checklist: Information Security Policy Implementation

This checklist has been developed to provide agencies with an example of the implementation actions they will be required to put in place in order to implement the Tasmanian Government Information Security Policy Manual. Agencies can use the Agency Status column to rate their own status in terms of information security policy implementation. A rating scale is included at the end of the document.

Note the Tasmanian Government Information Security Policy Manual will be known as 'the manual'.

Policy Area	Implementation Example	Agency Status
Information Security Governance and Management		
Information Security Policy		
An Information security policy has been developed	An information security policy exists	
The Information security policy contains the mandatory clauses detailed in the manual	All mandatory clauses in the manual can be located in the information security policy	
The Information security policy has been prepared on an agency wide basis	There has been consultation across major business areas within the agency	
The Information security policy is aligned with agency business planning	Business requirements have been documented within the policy	
The Information security policy is aligned with the agency's general security plan	General security plan requirements have been documented within the policy	
The Information security policy is aligned with risk assessment findings	A risk assessment has been documented and the results have informed the development of the policy	
The Information security policy is consistent with the requirements of agency	Legislative requirements relevant to the agency have been documented	

relevant legislation	within the policy	
The information security policy is consistent with the requirements of other relevant policies	Agency and W-o-G policies relevant to the agency have been documented within the policy	
The information security policy is communicated to all employees on an ongoing basis	Staff are aware of and trained in the use of the policy with refresher courses available	
The information security policy is accessible to all employees	The policy can be easily accessed by all employees	
Approval for the information security policy has been obtained from the relevant senior executives	Senior Executive signoff/endorsement can be located within the policy or brief	
Endorsement for the information security policy has been obtained from the relevant governance body	Governance body signoff/endorsement can be located within the policy or brief	
The information security policy is reviewed at least on an annual basis	The date of the policy's last review is no more than 12 months old	
The next review for the information security policy has been scheduled	The date for the policy's next review is documented within the policy, and appropriate review mechanisms in place	
The information security policy is reviewed and evaluated in line with changes to business and information security risks, to reflect the current agency risk profile	If changes to business or new risks have occurred within the 12 month review period, has the policy been updated to reflect these changes?	
Information Security Plan		
An Information security plan has been developed	An information security plan exists	
Information security planning is aligned with agency business planning	There has been consultation across major business areas within the agency and business requirements have been documented within the plan	
Information security planning is aligned with the agency's general security plan	General security plan requirements have been documented within the plan	
Information security planning is aligned with risk assessment findings	A risk assessment has been documented and the results have informed the development of the plan	
Endorsement for the information security plan has been obtained from the relevant senior executives	Senior Executive signoff/endorsement can be located within the plan or brief	
Endorsement for the information security plan has been obtained from the relevant governance body	Governance body signoff/endorsement can be located within the plan or brief	
The information security plan is reviewed at least on an annual basis	The date of the plan's last review is no more than 12 months old	
A threat and risk assessment has been conducted for all ICT assets that create,	A threat and risk assessment has been conducted and documented for	

store, process or transmit security classified information at least annually or after any significant change has occurred, such as machinery of Government	all ICT assets that create, store, process or transmit security classified information. The date of the last assessment is no more than 12 months old	
Governance		
Agency management recognizes the importance of, and demonstrates a commitment to, maintaining a robust agency information security environment	Senior executive management group agenda/minutes include information security matters	
Information Security internal governance arrangements have been established	Information security governance body is in operation (e.g. Information security governance body is meeting as documented in minutes)	
Information Security internal governance arrangements have been documented	Information security governance body's terms of reference approved by senior executive management group/CEO	
Information Security Roles and Responsibilities have been documented	Information security roles and responsibilities documented and approved by senior executive management	
Information Security Roles and Responsibilities have been established	Employees with information security roles and responsibilities have signed a document stating that they understand their roles and responsibilities	
Endorsement for the internal governance arrangements has been obtained from the relevant senior executives	Sign off obtained from senior executive management group/CEO for all information security internal governance arrangements	
Endorsement for the internal governance arrangements has been obtained from the relevant governance body	Sign off obtained from relevant governance body (e.g. Information Steering Committee) has been obtained for information security internal governance arrangements	
External Party Governance		
Information Security external governance arrangements have been established	External governance arrangements are in operation	
Information Security external governance arrangements have been documented	External governance arrangements have been documented and approved by the senior executive management group/CEO	
All third party service level agreements, operational level agreements, hosting agreements or similar contracts clearly articulate the level of security required	Standard templates for service level agreement and operational level agreements include clauses dealing with information security requirements	
All third party service level agreements and operational level agreements are regularly monitored	Minutes of Information security governance body meetings include outcomes of routine checks on inclusion of information security requirements in SLAs, and audits to ensure third party adherence to these agreements	

Endorsement for the external governance arrangements has been obtained from the relevant senior executives	Sign off obtained from senior executive management group/CEO for all information security external governance arrangements	
Endorsement for the external governance arrangements has been obtained from the information security governance body	Sign off obtained from the information security governance body has been obtained for information security external governance arrangements	
Information Security Risk Management		
Risk Analysis of agencies Information Security Risks has been completed	Risk management plan has been put in place that includes identification, qualification and prioritisation of risks against acceptance criteria and identifies appropriate controls to protect against risks.	
Risk analysis against the agencies information Asset register has been completed	Risk management plan has been put in place for agencies information assets	
Resource Management		
Record Security		
Each agency must have an active Records Management Program	Agency Records Management Program in Place. Agency has an Information Management Policy outlining governance arrangements, roles and responsibilities of all staff for the management of information	
Each agency must have an identified Records Manager	Records Manager appointed with up to date statement of duties	
Each agency must have an information asset register that contains the details of all of the agencies assets regardless of format. This register must identify the information asset owner & custodian and all assets must have a disposal category and information classification assigned.	Information asset register in place, Information Owners and Custodians are identified on the register. Agency has security classified each asset. Agency has worked with TAHO to determine the disposal class appropriate to the information contained in the asset.	
Each agency must have an approved disposal schedule	Agency has up to date schedule in place and an active disposal program	
Information Asset Register		
Procedures for the protective control of information assets (regardless of format) have been implemented	Procedures for the protective control of information assets have been documented and approved by the Information security governance body	
All ICT assets that create, store, process or transmit security classified information are assigned appropriate controls in accordance with the Tasmanian Government Information Security Classification Framework	An ICT asset register exists, that documents the security classification of application and technology assets (in accordance with the policy and the manual or in the case of national security information relevant national arrangements) and the corresponding controls that are applied to that asset (actual controls may be documented elsewhere)	

All ICT assets (including hardware, software and services) have been identified and documented	ICT asset register has been completed and is updated at least annually	
All ICT assets (including hardware, software and services) have been assigned ICT asset custodians	ICT asset register identifies the ICT asset custodian for all assets	
All ICT assets that provide underpinning and ancillary services must be protected from internal and external threats (e.g. Mail gateways, domain name resolution, time, reverse proxies, remote access and web servers)	All ICT assets that provide underpinning and ancillary services have been identified and documented. Adequate controls have been implemented for these services	
Information Security Classification		
Procedures for the classification of information assets (regardless of format) have been implemented	Procedures for the classification of information assets have been documented and approved by the Information security governance body	
All information assets are assigned appropriate classification in accordance with the Tasmania Government Information Security Classification Framework as a minimum	Agency has a complete information asset register, where all information assets are assigned a classification, or in the case of national security information, as per national arrangements	
Classification schemes do not limit the provision of relevant legislation under which the agency operates	The information security classification policy and procedure document state that legislative obligations override the classification scheme. For example, the security classification of an information asset does not prevent it from being considered for release under the Right to Information Act 2010	
Physical Environment Security		
Building controls and security areas		
The requirements of the Tasmania Government Information Security Classification Framework have been implemented	All information assets have been evaluated against the manual	
Building and entry controls for areas used in the processing and storage of security classified information have been established and maintained in line with the manual	Building and entry controls for areas used in the processing and storage of security classified information have been documented approved and are subject to regular updating. Agency records demonstrate that these are subject to routine checks	
Physical security protection controls (commensurate with the security classification information levels) have been implemented for all offices, rooms, storage facilities and cabling infrastructure in line with the manual	Physical security protection controls (commensurate with security classification levels) have been documented, approved and are subject to regular updating. Agency records indicate that these are subject to routine checks	
Control policies (including clear desk/clear screen) has been implemented in	Controls for information processing areas have been documented,	

information processing areas that deal with security classified information	approved and are subject to regular updating. Agency records indicate that these are subject to routine checks	
Asset Management		
All Information assets that store or process information are located in secure areas with access control mechanisms in place to restrict use to authorised personnel only	Agency equipment is located in secure areas. Records of routine checks confirm that these areas are accessible only to authorised personnel	
Policies are implemented to monitor and protect the use and/or maintenance of information assets and ICT assets away from premises as required by the manual	Agency information security policies address the protection and monitoring of ICT assets that are offsite. The relevant policy has been approved by the agency senior executive management group/CEO	
Processes are implemented to monitor and protect the use and/or maintenance of information assets and ICT assets away from premises as required by the manual	Procedures for the protection and monitoring of offsite equipment have been documented and approved	
Policies are implemented for the secure disposal or reuse of ICT assets which are commensurate with the information asset's security classification level (as required by the manual)	Agency information security policies address the disposal and reuse of ICT assets commensurate with the information asset's security classification level. These policies have been approved by the agency senior executive management group/CEO. Agency records demonstrate that this policy is being complied with	
Processes are implemented for the secure disposal or reuse of ICT assets which are commensurate with the information asset's security classification level as required by the manual	Procedures for the disposal and reuse of equipment, storage devices and media commensurate with the security classification of the information stored on the asset have been approved. Agency records demonstrate that these procedures are being followed	
Information and Communications Technology		
Operational procedures and responsibilities		
Operational procedures and controls have been documented to ensure that all information assets and ICT assets, are managed securely and consistently, in accordance with the level of required security	Operational procedures ensuring information assets and ICT assets, including information systems and network tasks, are managed consistently in accordance with the required level of security, have been documented and approved	
Operational procedures and controls have been implemented to ensure that all information, assets and ICT assets, are managed securely and consistently, in accordance with the level of required security	Agency records indicate that these procedures are being implemented. e.g. Errors and exceptional conditions are captured and handled in accordance with the procedures; backups occur in accordance with procedures	
Operational change control procedures have been implemented to ensure that	Capacity planning and system acceptance procedures have been	

changes to information processing facilities or systems are appropriately approved and managed	documented and approved. Agency records demonstrate that these are being implemented, e.g. new system business requirements document capacity requirements; system acceptance criteria is documented and tests are taken out during development and prior to acceptance	
Third Party Service Delivery		
Third party service delivery agreements comply fully with Policy	All the requirements within policy relating to third party service delivery have been documented within agreements	
Third party service delivery agreements are periodically reviewed and updated to ensure they address any changes in business requirements whilst remaining compliant with Policy	Agreements are reviewed regularly and documented	
Third party service operating agreements must specifically address third party governance policies and processes	Agreements clearly articulate the level of security required, are regularly monitored and endorsed by the relevant senior executives and governance body	
Capacity planning and system acceptance		
System acceptance must include confirmation of the application of appropriate security controls and of the capacity requirements of the system	Appropriate system acceptance and change criteria and processes have been established and documented	
System capacity must be regularly monitored to ensure risks of system overload or failure, which could lead to a security breach, are avoided	Processes for reviewing and updating system capacity have been documented	
Malicious and Mobile Code Control		
Adequate controls have been defined and implemented for the prevention, detection, removal and reporting of attacks of malicious code on all ICT assets	Controls for the prevention, detection, removal and reporting of the introduction of malicious and mobile code are documented and approved	
Vulnerability / integrity scans of core software must be defined and conducted regularly to ensure detection of unauthorised changes	Details of vulnerability/integrity scans have been documented, including what core software has been scanned, when it has been scanned, when the next scan is due, and the scan results	
Anti malicious-code software has been regularly updated with new definition files and scanning engines	Details of anti-malicious-code software updates have been documented, including details of definition files and scanning engines	
Employees have been educated about malicious and mobile code in general, the risks posed, virus symptoms and warning signs including what processes should be followed in the case of a suspected virus	Employee education about malicious code and associated processes have been conducted, for example through induction programs, training programs/plans and awareness campaigns (eg. emails, posters, factsheets, intranet contents etc)	
Backup procedures		

Comprehensive systems maintenance processes and procedures (including operator and audit/fault logs), information backup procedures and archiving have been implemented	Agency backup policies and procedures (including archiving) have been documented and approved. Agency records that may indicate implementation of this requirement include records of backup copies and test results	
Network security		
A network security policy has been developed and documented to guide network administrators in achieving the appropriate level of security	Network security policy and guidelines have been documented and approved. Network administrators are aware of and follow these documents	
Processes to periodically review and test firewall rules and associated network architectures have been developed and implemented to ensure the expected level of network perimeter security is maintained	Firewall rule and associated network architecture testing processes are documented. Agency records document tests, their results and any corrective action taken	
Processes must be established to periodically review and update current network security design, configuration, vulnerability and integrity checking to ensure network level security controls are appropriate and effective	Processes for reviewing and updating network security design, configuration, vulnerability and integrity are documented. Agency records demonstrate that periodic network security checks, reviews and updates are occurring	
A policy on scanning has been developed to ensure that traffic entering and leaving the agency network is appropriately scanned for malicious or unauthorised content	A policy on scanning has been documented and approved. Supporting processes to ensure adherence to the manual have also been developed	
Processes relating to IT change management (including maintenance of network systems) and configuration management processes are established and updated as required	Approved IT change management processes address network security and configuration management. Agency records indicate that network security configuration is updated regularly	
Information Technology Media Management		
Media handling procedures must be in line with the requirements of the manual	Media handling procedures have been documented and implemented. All the requirements of the manual have been documented within these procedures	
Electronic Information Transfer		
A Network policy has been implemented to ensure the security of data during transportation over communication networks	Network security policy and guidelines have been documented and approved. Network administrators are aware of and follow these documents	
Methods for exchanging information within the agency, between agencies, through online services, and/or third parties are compliant with legislative requirements	Approved agency information security policy documents relevant legislative requirements to be complied with	
Methods for exchanging information within the agency, between agencies, through online services, and/or third parties are consistent with the Tasmania	Agency information exchange controls are consistent with those specified in the manual and in the case of national security information,	

Government Information Security Classification Framework	national arrangements	
Methods for exchanging information within the agency, between agencies, through online services, and/or third parties are consistent with the manual	Agency information exchange controls are consistent with those specified in the manual	
The type and level of encryption must be authorised and compliant with the requirements of the manual	Appropriate authorisation has been obtained and documented for the type and level of encryption used within the agency. The type and level of encryption is consistent with those specified in the manual	
All information exchanges over public networks, including all online or publicly available transactions/systems must be authorised either directly or through clear policy	Appropriate authorisation for information exchanges can be documented (either within existing policies or separate documentation)	
A policy to control email has been developed, implemented and endorsed	A policy to control email, has been approved by the relevant senior executive/governance body and has been implemented within the agency	
e-commerce		
All critical online services must have penetration testing performed periodically	Details of penetration testing have been documented, including what critical online services have been tested, when the testing has occurred, when the next test is due and test results	
Policies and controls have been developed to manage all aspects of on-line and internet activities including anonymity/privacy, data confidentiality, use of cookies, applications/plug-ins, types of language used, practices for downloading executables, web server security configuration, auditing, access controls and encryption	Policies and controls exist to manage all aspects of online and internet activities, and have been endorsed by the relevant senior executive/governance body. The policies and controls have also been implemented within the agency	
Security Audit Logging		
Comprehensive operator and audit/fault logs must be implemented	Details of operator and audit/fault logs have been documented including what events are logged, when and who will review and monitor logs, where and for how long the logs are stored, are logs adequately protected	
All ICT assets must be synchronised to a trusted time source that is visible and common to all	All assets have a synchronised time source which is visible	
Identity and Access Management		
Access Control Policy		
Control mechanisms based on business owner requirements and	Access control policy	

assessed/accepted risks for controlling access to all information assets and ICT assets have been established		
Access control rules are consistent with business requirements	Approved access control policy refers to the agency's specific business requirements	
Access control rules are consistent with information classification	Approved access controls as documented in the agency policy are consistent with the manual and where applicable national arrangements	
Access control rules are consistent with legislative obligations	Approved access control policy documents legal obligations	
Authentication		
Authentication requirements, including on-line transactions and services, have been assessed against the manual	Agency records indicate that all authentication requirements have been assessed against the manual. Business requirements for all online transactions and services include consistency with the manual. Agency records indicate that online transactions and services have been assessed against the manual	
All authentication of users external to the agency must be implemented in compliance with the manual	Agency records indicate that all authentication of users external to the agency have been assessed against the manual	
User access		
Access to information systems requires specific authorisation	Agency information systems cannot be accessed without specific authorisation. Agency records that may indicate evidence of compliance include completed system access request forms for all users	
Each user has been assigned an individually unique personal identification code and secure means of authentication	Agency records indicate that each user is issued a unique personal identification code and secure means of authentication	
User responsibilities		
NO MANDATORY CLAUSES		
Network access		
Control measures have been implemented to detect and regularly log, monitor and review information systems and network access and use, including all significant security relevant events	Agency records indicate that system and network access and use is logged, monitored and reviewed. Events are recorded	
Authorisation must be obtained and documented for access (including new connections) to agency networks	Agency records indicate that authorisation has been obtained and documented for new and existing access to networks	
All wireless communications have appropriate configured product security features and afford at least the equivalent level of security of wired communications	Agency records (e.g. configuration documentation, tests) indicate that wireless communications are secured as per any agency wired communication	

Security risks associated with use of ICT facilities and devices (including non-government equipment) such as mobile telephony, personal storage devices and internet and email have been assessed prior to connection and appropriate controls implemented	Agency records indicate that a risk assessment has been performed for all ICT facilities and devices (including non-government equipment) prior to connection. Records all indicate that appropriate controls have been implemented based on this risk assessment	
Operating system access		
Policies and/or procedures for user registration, authentication management, access rights and privileges, are defined, documented and implemented for all ICT assets	Agency has documented and approved access controls for operating systems that cover user registration, authentication, user responsibilities. Access to operating systems is conducted in compliance with these controls	
Application and information access		
Restricted access and authorised use only warnings are displayed upon access to all systems	Agency systems cannot be accessed until restricted access and authorised use only warning are displayed on the screen and accepted by the user	
Access to all confidential/sensitive systems must only be allowed after authorised approval	Confidential/sensitive systems cannot be access unless appropriate approval has been given by those authorised within the agency to do so	
Mobile computing and telework access		
Risk assessments have been conducted for mobile technologies and teleworking facilities	Agency records indicate that mobile technologies and teleworking facilities are not introduced unless a risk assessment has been performed	
Processes have been established for mobile technologies and teleworking facilities	Agency has documented and approved processes for mobile technologies and teleworking facilities	
Information Systems Acquisition Development and Maintenance		
Security Systems Requirements		
Security controls are commensurate with the security classifications of the information contained within, or passing across information systems, network infrastructures and applications	Agency system security controls are commensurate with the highest level of security classification of the information stored and passing through the system	
Security requirements are addressed in the specifications, analysis and/or design phases	Business requirements for all systems include information security requirements	
Internal and/or external audit have been consulted when implementing new or significant changes to financial or critical business information systems	Records of audit results are documented for new or significant changes to financial or critical business information systems	
Security controls have been established during all stages of system development, as well as when new systems are implemented and maintained in the operational environment	Documented system security controls address acquisition, development and maintenance stages	

Appropriate change control, acceptance and system testing, planning and migration control measures have been carried out when upgrading or installing software in the operational environment	Agency records document change control, acceptance and system testing, planning and migration control measures have been taken when upgrading or installing software	
Accurate records must be maintained to show traceability from original business requirements to actual configuration and implementation, including appropriate justification and authorisation	Records of traceability from original business requirements to actual configuration and implementation are documented (including authorisation)	
Correct processing		
Access controls have been identified and implemented including access restrictions and segregation/isolation of systems into all infrastructures, business and user developed applications	Records of the identified access controls and their implementation are documented	
Cryptography Protocols		
Authentication processes are consistent with the manual requirements	Authentication processes are consistent with the manual	
Cryptographic controls are consistent with the manual	Agency records document cryptographic controls in place	
System files		
Access to system files is controlled to ensure integrity of business systems, applications and data	Access controls for system files are documented	
Secure development and support processes		
Processes (including data validity checks, audit trails and activity logging) have been established in applications to ensure development and support processes do not compromise the security of applications, systems or infrastructure	Records of the processes for secure development have been documented	
Audit logs are maintained in accordance with the manual	Audit logs for UNCLASSIFIED and security classified information log activity as specified by the manual.	
Administrator rights to audit logs follow the specifications set out in the 'Tasmania Government Information Security Controls Standard'"		
Technical Vulnerability Management		
Processes to manage software vulnerability risks for all IT security infrastructure has been developed and implemented	Existence of an audit log for all technical vulnerability procedures undertaken	
A patch management program for operating systems, firmware and applications of all ICT assets must be implemented to maintain vendor support, increase stability and reduce the likelihood of threats being exploited	Patch management program is implemented and documented including any tests that are carried out	

Personnel and Awareness		
Pre-employment		
Security requirements have been addressed within recruitment and selection and in job descriptions	Job descriptions include information security requirements	
During Employment		
Policies have been developed to address information security issues within human resources	Agency policies addressing information security issues within human resources have been approved by the senior executive management group/CEO	
Processes have been developed to address information security issues within human resources	Procedures for addressing information security within human resource management have been document and approved	
Induction programs have been implemented to ensure that employees are aware of and acknowledge their security responsibilities	Induction program documentation includes information security	
Ongoing security training has been implemented to ensure that employees are aware of and acknowledge their security responsibilities	An information security training plan has been approved by the CEO (note that this may be part of the agency's general information security plan). Attendance records for information security training	
Security awareness programs have been implemented to ensure that employees are aware of and acknowledge their security responsibilities	Example evidence of compliance might include emails, posters, fact sheets, intranet content etc that communicate information security responsibilities	
Induction programs have been implemented to ensure that employees are aware of and acknowledge the agency's information security policies and processes	Induction program documentation includes an overview of the agency's information security policies and processes and details of where employees can go to get further information	
Ongoing training has been implemented to ensure that employees are aware of and acknowledge the agency's information security policies and processes	The information security training plan includes targeted training in the agency's information security policies and processes	
Security awareness programs have been implemented to ensure that employees are aware of and acknowledge the agency's information security policies and processes	Training attendance records or documents signed by all employees that document that they have been shown and understand agency information security policies and processes including how to use agency ICT assets	
All information security roles and responsibilities have been fully documented where employees have access to security classified information (X-IN-CONFIDENCE or above) or perform security related roles	Information security roles and responsibilities documented and approved by senior executive management	
All information security roles and responsibilities have been assigned to employees who have access to security classified information or perform security related roles	Roles and responsibilities have been physically assigned to employees (with appropriate records retained)	

All information security roles and responsibilities that have been assigned to employees have been communicated to these employees and signed acknowledgements obtained	Employees with information security roles and responsibilities have signed a document stating that they understand their roles and responsibilities	
Post-Employment		
Procedures for the separation of employees within the agency have been developed	Procedures for the separation of employees within the agency have been approved	
Procedures for the separation of employees within the agency have been implemented	Agency records demonstrate that all employee separations follow the approved procedure	
Procedures for employee movement within the agency have been developed	Procedures for the movement of employees within the agency have been approved	
Procedures for employee movement within the agency have been implemented	Agency records demonstrate that all employee movements within the agency follow the approved procedure	
Incident Management		
Incident Management Controls		
All information security incidents have been reported and escalated through appropriate management channels	Copies of information security incident reports. Receipt of incident reports by relevant management channels	
All information security incidents have been reported through appropriate authorities if applicable	Agency records indicate that information security incidents are reported to appropriate authorities (e.g. police) where applicable	
Responsibilities and procedures have been communicated to all employees including contractors and third parties for the timely reporting of information security events and incidents including breaches, threats and security weaknesses	Training attendance records or documents signed by all employees, contractors and third parties that document that they understand their responsibilities to report events/weaknesses and incidents	
Incident procedures		
Information security incident management procedures have been established to ensure appropriate responses in the event of information security incidents, breaches or system failures	Agency information security incident management procedures have been documented and covers the review of and response to incidents	
All Information security incidents caused by employees have been investigated	Records of information security incident reports and corresponding investigations.	
Where a deliberate information security violation or breach has occurred, formal disciplinary processes have been applied	Disciplinary processes for deliberate violations or breaches of information security policy have been approved by the senior executive management group/CEO. Where these incidents have occurred, agency	

	records demonstrate that these processes have been applied	
An information security incident and response register has been established and maintained. All incidents have been recorded within this register	Existence of a current agency information security incident and response register	
Business Continuity Management		
Business continuity		
Business continuity plans have been established to enable information and ICT assets to be restored or recovered in the event of a major security failure	Approved agency business continuity plan	
Business continuity processes have been established to enable information and ICT assets to be restored or recovered in the event of a major security failure	Processes that enable the information environment to be restored or recovered in the event of a major information security failure have been approved	
Business continuity processes have been established to assess the risk and impact of the loss of information and ICT assets in the event of a security failure	Business continuity risk and impact assessment processes have been approved. Agency records indicate that these assessments are made, and inform the development of the agency's business continuity plan	
Methods have been developed to reduce known risks to information and ICT assets	Existence of a risk register that documents how known risks will be managed	
Business continuity plans have been maintained and tested to ensure information and ICT assets are available and consistent with agency business and service level requirements	Business continuity plan is regularly updated. Business continuity tests are conducted and any weaknesses identified as a result are addressed	
A business impact analysis has been undertaken	Records show that a business impact analysis has been undertaken, and the results have been used to reduce risks	
All critical business processes and associated information and ICT assets have been identified and prioritised	Records show that all critical business processes and associated assets have been identified, prioritised and documented	
ICT Disaster Recovery		
An information and ICT asset disaster recovery register has been established to assess and classify systems to determine their criticality	Existence of disaster recovery register	
An ICT disaster recovery plan has been established to enable information and ICT assets to be restored or recovered in the event of a disaster	Approved disaster recovery plan	
ICT disaster recovery processes have been established to enable information and ICT assets to be restored or recovered in the event of a disaster	Processes that enable the information environment to be restored or recovered in the event of a disaster have been approved	
ICT disaster recovery processes have been established to assess the risk and	Disaster recovery risk and impact assessment processes have been	

impact of the loss of information and ICT assets in the event of a disaster	approved. Agency records indicate that these are made, and inform the development of the agency's disaster recovery plan	
Methods have been developed to reduce known risks to information and ICT assets	Existence of a risk register that documents how known risks will be managed	
An ICT disaster recovery plan has been maintained and tested to ensure information and ICT assets are available and consistent with agency business and service level requirements	Disaster recovery plan is regularly updated. Disaster recovery tests are conducted and any weaknesses identified as a result are addressed	
ICT disaster recovery plans must have clearly defined maximum acceptable downtimes	Clearly defined maximum acceptable downtimes are documented within ICT disaster recovery plans	
Maximum acceptable downtimes for ICT services must also be defined in service and operational level agreements with external parties	Maximum acceptable downtimes for ICT services are documented in all service and operational level agreements with external parties	
Copies of ICT disaster recovery plans must be stored in multiple locations including at least one location offsite	Copies of ICT disaster recovery plans are located in multiple locations including at least one offsite location	
Monitoring for Compliance		
Legal requirements		
All legislative obligations relating to information security have been complied with and managed appropriately	Agency has identified and documented all its legal obligations relating to information security and its response to these.	
All information security policies and processes have been reviewed for legislative compliance on a regular basis	A list of legislation compliance has been developed and is cross referenced against all information security policies and processes on a regular basis (including when changes to legislation occur)	
The results of compliance reviews against information security policies and processes have been reported to appropriate agency management	Agency management has signed off on the compliance review	
All information security requirements (including contracts with third parties) have been reviewed for legislative compliance on a regular basis	A list of legislative compliance has been developed and is cross referenced against all information security requirements (including contracts with third parties) on a regular basis (including when changes to legislation occur)	
The results of compliance reviews against all information security requirements (including contracts with third parties) have been reported to appropriate agency management	Agency management has signed off on the compliance review	
Processes to ensure legislative compliance across all agency activities have been developed and implemented	Agency has identified and documented processes for assessing compliance against its information security related legal obligations.	

Checklist: Information Security Policy Implementation

	Agency records indicate that these processes are being conducted	
Policy Requirements		
All reporting obligations relating to information security have been complied with and managed appropriately	Agency has identified all reporting obligations and have documented compliance and management	
Audit Requirements		
All reasonable steps have been taken to monitor, review and audit agency information security compliance	Examples include: completed internal and external audit against legal and policy requirements; accreditation with appropriate standards or industry bodies	
All reasonable steps have been taken to ensure the assignment of appropriate security roles	Employees with information security roles and responsibilities have signed a document stating that they are understand their roles and responsibilities	
All reasonable steps have been taken to ensure the engagement of internal and/or external auditors and specialist organisations where required	Examples include: completed internal and external audit against legal and policy requirements; accreditation with appropriate standard	

Rating Scale

Mandatory Principles	
Fully Compliant	➢ Meets all aspects of the mandatory principle or policy requirement. ➢ Implementation has occurred throughout the entire agency.
Substantially Compliant	➢ Most aspects of the mandatory principle or policy requirement have been met. ➢ Significant implementation has occurred for all business critical elements (systems/services/assets/domains/risks etc.) and throughout the majority of business units in the agency.
Partially Compliant	➢ Many aspects of the mandatory principle or policy requirement have been met. ➢ Implementation has occurred across many business units of the agency.
Not Compliant	➢ Limited or no aspects of the mandatory principle or policy requirement have been met. ➢ Implementation has not occurred or is ad-hoc.
Exception Granted	➢ An official exception to the mandatory principle or policy requirement has been approved through the agency Information Security Committee and request submitted to DPAC ➢ Where departments self-assess as an 'exception granted' without formal approval, the department will be deemed 'not compliant'.

Not Applicable	➢ A 'not applicable' should only be used when the manual excludes the agency. ➢ A 'not applicable' cannot be used where the agency is engaging a third party service, as the agency is responsible for the compliance of the service provider. ➢ All uses of 'not applicable' need to be justified. ➢ Where agency incorrectly self-assess as 'not applicable', the agency will be deemed as 'not compliant'.

Further Advice

For more detailed advice, please contact:

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

Acknowledgements

- Queensland Government Information Security Compliance Checklist
- Tasmanian Government Information Security Policy Manual

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	December 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: December 2013

Ross Latham
State Archivist