CCC EXHIBIT

Department of Justice and Attorney-General

Information Technology Services

Information Security Policy

Great state. Great opportunity.

Queensland Government

Document Number: 3711784

Document information

Security classification	**UNCLASSIFIED**		
Date of review of security classification	June 2017		
Authority	Executive Director, Information Technology Services		
Documentation status	Final	Consultation release	☑ Final version
Next review date	June 2019		
Document reference	**eDOCS number:** 3711784		

Version History

Version	Notes	Changed by and date
2	Existing draft	September 2002
3	Changed to IMB Policy template and minor editing amendments that do not change context of document.	Terry McDonald – July 2005
4	Minor amendments to position titles and branch names	Trevor Niblock – July 2005
5	Policy structure changes to comply with IS18 update released November 2006.	Rita Dunning – March 2007
6	Minor amendments to position titles and branch names	Jodie Beale – November 2008
7	Redrafted to align with updates to IS18.	Bridge Point Communications Oct 2013 Chris Ruffin June 2014
8	Minor amendments to align with the new governance body and refresh links.	David Black – January 2017

Policy owner/enquiries

All enquiries regarding this document should be directed in the first instance to the Executive Director, Information Technology Services, Department of Justice and Attorney-General.

This policy is owned by the Executive Director, ITS, who is responsible for the development and ongoing review of the policy.

Policy approval and review

This policy version 8.0 was endorsed by the departmental Information and Technology Innovation Committee (ITIC) on 8 June 2017. This policy version 8.0 was approved by Director-General, Department of Justice and Attorney-General on 13 July 2017. This policy is reviewed every two years. The next scheduled review is June 2019.

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

Security classification

This document has a security classification of UNCLASSIFIED.

License

CCC EXHIBIT

Purpose

The Department of Justice and Attorney-General (DJAG) is responsible for a significant amount of information held in both electronic and paper-based formats, it is critical that this information is protected appropriately.

The purpose of this policy is to state the requirements and necessity for the management of information security to protect the DJAG information assets and any ICT assets which create, process, store, view or transmit information, against unauthorised use or accidental modification, loss or release.

Scope

This Information Security Policy and the supporting DJAG Information Security Policy Framework (See Appendix B) applies to:

- All JAG employees, whether full-time, part-time, casual, temporary or permanent, sub-contractors or consultants, agency employees and any external parties while deployed or engaged within the department; and
- The protection of 'information assets' (an identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business functions) in all forms, including assets owned by the department and entrusted to the department by customers, partners or external third parties.

Policy Statement

The Department of Justice and Attorney-General has a responsibility to develop, document, implement, maintain and review appropriate security controls to protect the information they hold through meeting the following objectives:

- Maintain the confidentiality, integrity and availability of information commensurate with the information's value, business significance, sensitivity and security classification as defined within the Queensland Government Information Security Classification Framework.
- Ensure compliance with Commonwealth and Queensland legislation, all applicable regulatory standards, as well as any contractual obligations that the department enters into with partners and other third parties.
- Satisfy the mandatory requirements set out in the Queensland Government Information Standard 18 (IS18).
- Establish and maintain appropriate security controls to protect all department information assets, commensurate with the risk posed to the assets.
- Establish and maintain effective governance arrangements to ensure personnel are accountable for the protection of information.
- Establish and maintain information security awareness to ensure all departmental employees understand their responsibilities for the protection of information.
- Ensure the department is able to detect and respond to security events and incidents in a timely manner to meet business continuity objectives; and
- Ensure the ongoing utility, efficiency and flexibility of these information security services by regular review of current business requirements and business risks in accord with the general security plans.

Implementation

This policy and the supporting DJAG Information Security Policy Framework (See Appendix B) will be communicated on an ongoing basis and be accessible to all employees.

Governing Legislation and Standards

Information Security in the department will be guided by the Queensland Government Information Security Policy Framework, Queensland Government Information Standard 18: Information Security (IS18), Queensland Government Information Security Classification Framework (QGISCF), Queensland Government Network Transmission Security Assurance Framework (NTSAF), Queensland Government Authentication Framework (QGAF), Queensland Government Information Security Controls Standard (QGISCS).

Appendix C provides a summary of the related obligations that apply to Queensland Government departments.

Mandatory Requirements

Under the Financial and Performance Management Standard 2009, the department must implement and maintain internal ICT controls that comply with the mandatory requirements set out in the Queensland Government Information Standard 18: Information Security (IS18).

The Queensland Government Information Standard 18: Information Security (IS18) states that the agency Information Security Policy must contain the mandatory clauses within the following ten mandatory security principles of IS18.

The ten mandatory principles of IS18 are:

Principle 1 – Policy, planning and governance
Principle 2 – Asset management
Principle 3 – Human Resources management
Principle 4 – Physical and environmental management
Principle 5 – Communications and operations management
Principle 6 – Access management
Principle 7 – System acquisition, development and maintenance
Principle 8 – Incident management
Principle 9 – Business continuity planning
Principle 10 – Compliance management

Appendix D states the mandatory clauses which must be contained within an agency's Information Security Policy as defined in the Queensland Government Information Security Policy – Mandatory Clauses document.

The following Mandatory Quality Criteria must be maintained to ensure this policy is effective and are included below for information.

Mandatory Quality Criteria:

- The policy must contain the mandatory clauses detailed in the *Queensland Government Information Security Policy – Mandatory Clauses* document
- The policy must be prepared on an agency wide basis and linked to agency security risks

- The policy is consistent with the requirements of relevant legislation and policies (including the *QGEA*)
- The policy is aligned with agency business planning, the agency's general security plan, and risk assessment findings
- Endorsement for the policy is obtained from the relevant governance body
- Approval for the policy is obtained from the relevant senior executives
- Processes relating to IT change management (including maintenance of network systems) and configuration management processes are established and updated as required
- A policy to control email has been developed, implemented and endorsed
- Policies and controls have been developed to manage all aspects of online and internet activities including anonymity/privacy, data confidentiality, use of cookies, applications/plug-ins, types of language used, practices for downloading executable, web server security configuration, auditing, access controls and encryption.

Information Security Roles and Responsibilities

Every employee, contractor, consultant, vendor, external third party and authorised user of the DJAG ICT computer network has a specific Role and Responsibility that must be adhered to and are defined in the table below:

Role	Responsibility
Director-General	Has ultimate responsibility for information security and risk management within the agency including alignment and compliance to the Queensland Government Information Standard 18: Information Security (IS18). Is accountable for the effective operation, implementation and maintenance of information security measures within DJAG. Responsible for approving departmental information security policies.
Assistant Director-General, Corporate Services	Support the Director-General in establishing and maintaining information security and risk management. Support the ITIC group responsible for ensuring Confidentiality, Integrity and Availability of DJAG Information and ICT Systems. Support the Executive Director, ITS in providing sufficient funding to implement the requirements of DJAG Information Security Policies and Queensland Government Information Standard 18: Information Security (IS18).
Executive Director, Information Technology Services	Ensure that the mandatory requirements defined within the departments Information Security Policy and supporting Information Security Policy Framework (See Appendix B) are implemented including but not limited to: • Monitoring and supporting the performance of the compliance and operational areas of Information Security within ITS. • Ensuring adequate resources are allocated to the compliance and operational areas of Information Security. • Facilitate access to senior management; and provide sufficient backing or authority to effectively review, formulate and implement security improvements. • Support departmental information security awareness.
Executive Director, Financial Services	Provide financial assistance to ITS in order to mitigate DJAG information security risks and harmonize the DJAG information security threat landscape. Consider and represent policy, resource and implementation requirements to the Finance Committee. Work with the Executive Director, ITS to ensure DJAG financial ICT systems are secure, compliant with the requirements of IS18 and that the confidentiality, integrity and availability of the systems is protected.

Role	Responsibility
Information and Technology Innovation Committee	Assuming the responsibilities of an Information Security Governance Body (ISGB) which include: • Supporting the Director-General in establishing and maintaining information security. • Ensuring security measures defined in IS18 are developed, endorsed, instituted and monitored across each member's respective business division. • Reviewing DJAG information security incidents and events of a high or very high severity as defined by the Queensland Government Information Security Incident Category Guideline.
Information Owners	Ensuring that information assets are security classified in accordance with the Queensland Government Information Security Classification Framework. Working with ITS to ensure that ICT controls are implemented commensurate with the security classification of the system and as defined within the requirements of the Queensland Government Information Standard 18: Information Security (IS18). Specify information management requirements for business functions under their control. Define and document current business rules. Specify information requirements. Co-ordinate business rule changes.
Information System Custodian	Develop and manage security procedures for information systems under their control. Procedures must align to the requirements of IS18 and DJAG Information Security Policies. Report to the Information Owner and inform the Assistant Director, ITS of these procedures. Develop, maintain and possibly coordinate the testing of business contingency plans. Determine local access control procedures. Recommend improvements to security procedures to the Assistant Director, ITS. Provide security advice to local managers, system operators and employees. Report security violations promptly to information.security@justice.qld.gov.au. Report information security risks to their Managers and to the Assistant Director, ITS.

Role	Responsibility
Information System Administrators	Implement and monitor security procedures and controls on information systems in their charge. Procedures must align to the requirements of IS18 and DJAG Information Security Policies. Recommend security procedure improvements to the Assistant Director, ITS. Report security violations promptly to information.security@justice.qld.gov.au. Report information security risks and areas of non-compliance to the Assistant Director, ITS. Ensure technical information security controls are addressed, maintained, up-to date, secure, compliant and implemented within the department as per the department's policies and procedures. Ensure network, system architecture and design documentation are developed and maintained for all ICT infrastructure managed by their respective areas.
Information Technology Services	Facilitate compliance of the DJAG Information Security Policy Framework and IS18 across the Department including but not limited to the following: • Develop and maintain the DJAG Information Security Policy Framework • Promote departmental information security awareness. • Provide security advice to management, auditors and to employees. • Maintain the departments ICT security infrastructure. • Coordinate and monitor the implementation, management and improvement of security procedures as well as compliance to IS18 across the Department. • Undertake routine system vulnerability scans where appropriate or deemed necessary by ED ITS and report associated risks to ITS Management and Business Owner. • Report security violations promptly to Management and to the QGCIO. • Report information security risks to the Assistant Director, ITS.
Everyone	All JAG employees, whether full-time, part-time, casual, temporary or permanent, sub-contractors or consultants, agency employees and any external parties while deployed or engaged within the department must comply with the relevant departmental Information Security Policy and supporting Information Security Policy Framework (See Appendix B) for the information and information computer systems they are using; and adhere to the requirements of the Code of Conduct for the Queensland Public Service (for JAG employees).

Role	Responsibility
	Breaches of this policy will be taken very seriously and may result in disciplinary action being taken against the employee responsible, including possible dismissal and civil or criminal liability Information security responsibilities include but are not limited to: • Understand the security procedures for the specific information and information systems used. • Use information and information systems lawfully, respectfully and responsibly. • Take precautions to protect information and information systems against unauthorised access, use, disclosure, modification, duplication or destruction. • Report security violations/issues to management and information.security@justice.qld.gov.au • All employees and Managers must complete the appropriate HR and ITS forms to disable a user's access to the DJAG computer network and all other systems when an employee exits the department or is seconded to another position.

Appendix A - Definitions and Acronyms

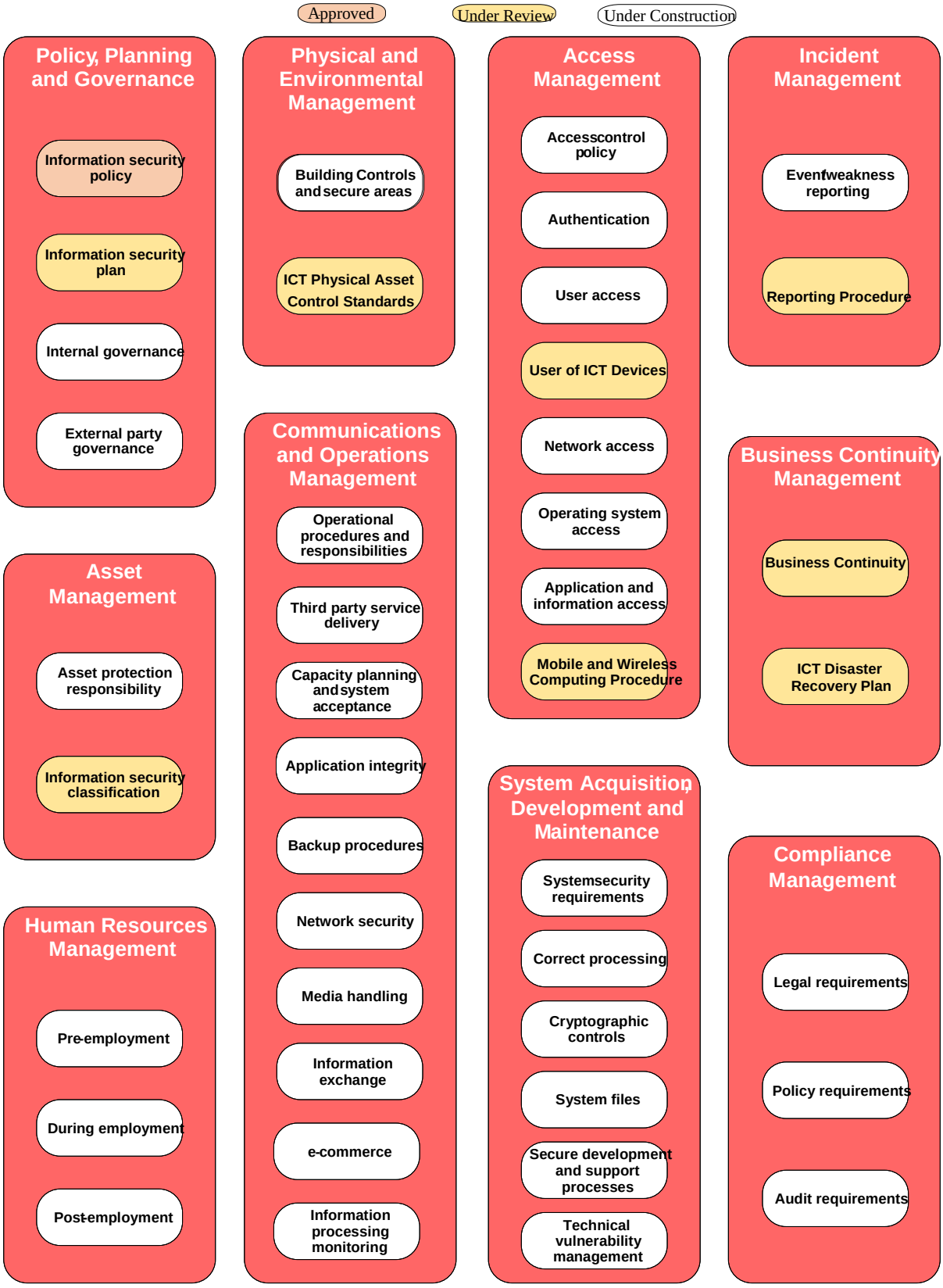
Term/Acronym	Definition
Authorised	Use by individuals who have: • Received the appropriate authorisation (which must be signed and documented as stipulated in local business procedures) before operating the relevant device or service; • Agreed to abide by the policies, guidelines and local practice arrangements for use of the relevant device or service, and who have appropriately acknowledged this agreement where required.
Classification	The systematic arrangement of information into logical categories.
Department	This refers to the Department of Justice and Attorney-General, Queensland and statutory authorities within the portfolio of the Attorney-General. This Policy is also applicable to employees of PartnerOne.
Employee	Those engaged on a permanent, temporary, seconded or contract basis including contractors engaged to work for or on behalf of the Department. This also includes students, volunteers, work experience or other external persons and/or organisations.
Information and Technology Innovation Committee (ITIC)	Leads the Department's strategy in respect of Information Management/ Information Communications Technology (IM/ICT) and to provide expert advice to the Director-General.
Information	A collection of data in any form which is maintained by an Agency or person, and which may be transmitted, manipulated, and stored by the information system.
Information Asset	An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business functions.
Information Owner(s)	The recognised officer(s) who is identified as having the authority and accountability under legislation, regulation or policy, for the collection and management of information assets on behalf of the State of Queensland, usually the Chief Executive Officer (CEO).
Information System Custodian	The recognised officer who is identified as owning hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information.
Information System Administrators	The recognised officer who is identified as managing and maintaining the configuration and reliable operation of an information system.
Information Standard 18 (IS18)	Sets out the mandatory requirements for Agencies when establishing, implementing and maintaining information security within their organisation.
Information Technology Services (ITS)	The Information Technology Services group is within the Corporate Services Division of the Department of Justice and Attorney-General.
Internet	Worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange.
JAG	This refers specifically to the Department of Justice and Attorney-General, Queensland.

Term/Acronym	Definition
Risk Assessment	An evaluation of system assets and their vulnerabilities to threats, including potential losses that may result from threats.
Standards	A published document, which sets out technical or other specifications necessary to ensure that a material or method will consistently do the job it is intended to do, i.e. 'what' must occur to achieve the desired result.
Third Party	An individual or an organisation outside of JAG who provides labour or services
Unauthorised use	Access which has not been appropriately authorised. (See *Authorised*) contrary to or in-breach of the requirements for authorised use.

CCC EXHIBIT

Appendix B - DJAG Information Security Policy Framework

Information Security Policy Framework



For further details refer to the Queensland Government Information Security Policy Framework.

Appendix C - Related legislation and other requirements

This appendix provides a summary of some of the related obligations that apply to Queensland Government departments. The contents of this appendix do not constitute legal advice and should not be relied on as a comprehensive statement of legislative and statutory obligations.

Queensland legislation

- Financial Accountability Act 2009 (Qld)
- Financial and Performance Management Standard 2009 (Qld)
- Information Privacy Act 2009 (Qld)
- Public Records Act 2002 (Qld)
- Right to Information Act 2009 (Qld)
- Public Service Act 2008 (Qld) - sections 187 – 192
- Public Sector Ethics Act 1994 (Qld) - sections 4(2), 7-11

Commonwealth legislation

- Cybercrime Act 2001 (Cth)
- Electronic Transactions Act 1999 (Cth) - part 2, s.8
- Electronic Transactions Act 2001 (Qld)
- Security Legislation Amendment (Terrorism) Act 2002 (Cth) - s.2 (e)
- Spam Act 2003 (Cth) - Schedule 1, Clauses 3,4
- Telecommunication Act 1997 (Cth)

Queensland Government Enterprise Architecture requirements

- QGEA Information Standard 18: Information Security (IS18)
- Queensland Government Information Security Policy – Mandatory Clauses
- Queensland Government Information Security Incident Category Guideline
- QGEA Information Standard 31: Retention and disposal of public records (IS31)
- QGEA policy: Information access and use policy (IS33)
- QGEA policy: Use of ICT facilities and devices (IS38)
- QGEA Information Standard 40: Recordkeeping (IS40)
- QGEA Information Standard 44: Information asset custodianship (IS44)

JAG supporting documents

- JAG Information Security Standards
- JAG Information Security Plan (including strategic security objectives)
- JAG Use of Information and Communication Technology (ICT) Devices Policy

Related procedures

- Australian Government Information Security Manual (ISM)
- Australian Government Protective Security Policy Framework (PSPF)
- ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security management
- AS/NZS ISO 31000:2009 – Risk Management – Principles and Guidelines
- Queensland Government Counter-Terrorism Strategy 2013-2018

- Queensland Counter Terrorism Plan 2007 – Department of the Premier and Cabinet (function now residing in Queensland Police)
- *Queensland Infrastructure Protection and Resilience Framework*

Forms

- Information Security Compliance Checklist

Guidelines

- Information Standard 18: Information Security - Implementation Guideline

Appendix D – IS18 Principles - Mandatory Clauses

This appendix provides the mandatory clauses contained within the Queensland Government Information Security Policy – Mandatory Clauses document. The document stipulates that the mandatory clauses must not be altered or deleted, and so must be used as specified in the Queensland Government Information Security Policy – Mandatory Clauses document.

Principle 1 – Policy, planning and governance

Agency management must recognise the importance of, and demonstrate a commitment to, maintaining a robust agency information security environment.

Information Security Plan

- An Information Security Plan must be developed and must align with agency business planning, general security plan and risk assessment findings.
- Endorsement for the Information Security Plan must be obtained annually from the relevant senior executives and governance body.
- A threat and risk assessment must be conducted for all ICT assets that create, store, process or transmit security classified information at least annually or after any significant change has occurred, such as machinery-of-Government.

Internal governance

- Information security internal governance arrangements must be established and documented (including roles and responsibilities) to implement, maintain and control operational information security within the agency.
- Endorsement for the information security internal governance arrangements must be obtained from the relevant senior executives and governance body.

External governance

- Information security external governance arrangements must be established and documented to ensure that third party service level agreements, operational level agreements, hosting agreements or similar contracts clearly articulate the level of security required and are regularly monitored.
- Endorsement for the information security external governance arrangements must be obtained from the relevant senior executives and governance body.

Principle 2 – Asset management

Agencies must implement procedures for the classification and protective control of information assets (regardless of format). Agencies may wish to extend existing information asset and technology registers to incorporate security classification and control requirements.

Asset protection responsibility

- All ICT assets that create, store, process or transmit security classified information must be assigned appropriate controls in accordance with the Queensland Government Information Security Classification Framework (QGISCF).
- All ICT assets (including hardware, software and services) and information assets must be identified, documented and assigned ICT asset custodians for the maintenance of security controls.
- All ICT assets that provide underpinning and ancillary services must be protected from internal and external threats (e.g. mail gateways, domain name resolution, time, reverse proxies, remote access and web servers).

Information security classification

- All information assets must be assigned appropriate security classification and control in accordance with the QGISCF.
- Classification schemes do not limit the provision of relevant legislation under which JAG operates.

Principle 3 – Human Resources management

Agencies must minimise the risk of loss or misuse of information assets by ensuring that security controls are incorporated into agency human resource management, including the development of supporting policies and processes.

Pre-employment

- Security requirements must be addressed within recruitment and selection and in job descriptions.

During employment

- Induction, ongoing security training and security awareness programs must be implemented to ensure that all employees are aware of and acknowledge the agency's information security policy, their security responsibilities, and associated security processes.
- Where employees have access to PROTECTED or higher information or perform specific security related roles, these responsibilities must be fully documented with signed acknowledgement and communicated.

Post-employment

- Procedures for ensuring the security of the agency during the separation of employees from, or movement within JAG must be developed and implemented.

Principle 4 – Physical and environmental management

The level of physical controls implemented must minimise or remove the risk of equipment or information being rendered inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

Building controls and secure areas

- Building and entry controls for areas used in the processing and storage of security classified information must be established and maintained in line with the QGISCF.
- Physical security protection (commensurate with the security classification information levels) must be implemented for all offices, rooms, storage facilities and cabling infrastructure in line with the QGISCF.
- Control policies (including clear desk/clear screen) must be implemented in information processing areas that deal with security classified information.

Equipment security

- All ICT assets that store or process information must be located in secure areas with access control mechanisms in place to restrict use to authorised personnel only, as required by the QGISCF.
- Policies and processes must be implemented to monitor and protect the use and/or maintenance of information assets and ICT assets away from premises, as required by the QGISCF.

- Policies and processes must be implemented to securely dispose and/or reuse ICT assets, commensurate with the information asset's security classification level, as required by the QGISCF.

Principle 5 – Communications and operations management

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

Operational procedures and responsibilities

- Operational procedures and controls must be documented and implemented to ensure that all information assets and ICT assets are managed securely and consistently (in accordance with the level of security required).
- Operational change control procedures must be implemented to ensure that changes to information processing facilities or systems are appropriately approved and managed.

Third party service delivery

- Third party service delivery agreements must comply fully with IS18.
- Third party service delivery agreements must be periodically reviewed and updated to ensure they address any changes in business requirements but remain compliant with IS18.
- Third party service operating agreements must specifically address third party governance policies and processes (see External governance, above).

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

Application integrity

- Adequate controls must be defined and implemented for the prevention, detection, removal and reporting of attacks by malicious code on all ICT assets.
- Vulnerability/integrity scans of core software must be defined and conducted regularly to ensure detection of unauthorised changes.
- Anti-malicious code software must be regularly updated with new definition files and scanning engines.
- Employees must be educated about malicious and mobile code in general, the risks posed, virus symptoms and warning signs including what processes should be followed in the case of a suspected virus.

Backup procedures

- Comprehensive information and system backup procedures and archiving must be implemented.

Network security

- Network security policy must be developed and documented in line with the NTSAF to guide network administrators in achieving the appropriate level of network security.
- Processes to periodically review and test firewall rules and associated network architectures must be established to ensure the expected level of network perimeter security is maintained.

- Processes must be established to periodically review and update current network security design, configuration, vulnerability and integrity checking to ensure network level security controls are appropriate and effective.
- A policy on scanning must be developed to ensure that traffic entering and leaving the agency network is appropriately scanned for malicious or unauthorised content.

Media handling

- Media handling procedures must be in line with the requirements of the QGISCF.

Information exchange

- Methods for exchanging information within the agency, between agencies, through online services, and/or with third parties must be compliant with legislative requirements and must be consistent with the QGISCF and the NTSAF.
- The type and level of encryption must be authorised and compliant with the requirements of the QGISCF and the NTSAF.
- All information exchanges over public networks, including all online or publicly available transactions/systems must be authorised either directly or through clear policy.

E-commerce

- All critical online services must have penetration testing performed periodically.

Information processing monitoring

- Comprehensive operator and audit/fault logs must be implemented.
- All ICT assets must be synchronised to a trusted time source that is visible and common to all.

Principle 6 – Access management

Control mechanisms based on business requirements, assessed/accepted risks, information classification and legislative obligations must be in place for controlling access to all information assets and ICT assets.

Access control policy

- Control mechanisms based on business requirements and assessed/accepted risks for controlling access to all information assets and ICT assets must be established.
- Access control rules must be consistent with agency business requirements, information classification, and legal/legislative obligations.

Authentication

- Authentication requirements including on-line transactions and services must be assessed against QGAF.
- All authentication of users external to the agency must be implemented in compliance with QGAF.

User access

- Access to information systems requires specific authorisation and each user must be assigned an individually unique personal identification code and secure means of authentication.

Network access

- Control measures must be implemented to detect and regularly log, monitor and review information systems and network access and use, including all significant security relevant events
- Authorisation must be obtained and documented for access (including new connections) to agency networks.
- All wireless communications must have appropriate configured product security features and afford at least the equivalent level of security of wired communications.
- Security risks associated with the use of ICT facilities and devices (including non-government equipment) such as mobile telephony, personal storage devices and internet and email must be assessed prior to connection and appropriate controls implemented.

Operating system access

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

Application and information access

- Restricted access and authorised use only warnings must be displayed upon access to all systems.
- Access to all confidential/sensitive systems must only be allowed after authorised approval.

Mobile computing and telework access

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

Principle 7 – System acquisition, development and maintenance

During system acquisition, development and maintenance, security controls must be established and must be commensurate with the security classifications of the information contained within, or passing across, information systems, network infrastructure and applications.

System security requirements

- Security controls must be commensurate with the security classifications of the information contained within, or passing across information systems, network infrastructures and applications.
- Security requirements must be addressed in the specifications, analysis and/or design phases and internal and/or external audit must be consulted when implementing new or significant changes to financial or critical business information systems.
- Security controls must be established during all stages of system development, as well as when new systems are implemented and maintained in the operational environment.
- Appropriate change control, acceptance and system testing, planning and migration control measures must be carried out when upgrading or installing software in the operational environment.
- Accurate records must be maintained to show traceability from original business requirements to actual configuration and implementation, including appropriate justification and authorisation.

Correct processing

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

Cryptographic controls

- Cryptographic control must be consistent with those of the NTSAF.

System files

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

Secure development and support processes

- Processes (including data validity checks, audit trails and activity logging) must be established in applications to ensure development and support processes do not compromise the security of applications, systems or infrastructure.
- Audit logs are maintained in accordance with the Queensland Government Information Security Controls Standard (QGISCS).

Technical vulnerability management

- Processes to manage software vulnerability risk for all IT security infrastructures must be developed and implemented.
- A patch management program for operating systems, firmware and applications of all ICT assets must be implemented to maintain vendor support, increase stability and reduce the likelihood of threats being exploited.

Principle 8 – Incident management

Effective management and response to information security incidents is critical to maintaining secure operations within the Queensland Government.

Event/weakness reporting

- Establish and maintain an information security incident register and record all incidents.
- All information security incidents must be reported and escalated (where applicable) through appropriate management channels and/or authorities.
- Where a deliberate violation or breach of this agency information security policy or subordinate processes has occurred, this must be investigated and formal disciplinary processes must be applied.
- Responsibilities and procedures for the timely reporting of security events and incidents including breaches, threats and security weaknesses, must be communicated to all employees including contractors and third parties.

Incident procedures

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

Principle 9 – Business continuity management

A managed process including documented plans must be in place to enable information and ICT assets to be restored or recovered in the event of a disaster or major security failure

Business continuity

- Methods must be developed to reduce known risks to information and ICT assets including undertaking a business impact analysis.
- Business continuity plans must be maintained and tested to ensure information and ICT assets are available and consistent with agency business and service level requirements.

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

ICT disaster recovery

- An ICT disaster recovery register must be established to assess and classify ICT assets to determine their criticality. The register must include details of suppliers of critical systems.
- Plans and processes must be established to assess the risk and impact of the loss of information and ICT assets in the event of a security failure or disaster to enable information and ICT assets to be restored or recovered.
- ICT disaster recovery plans must have clearly defined maximum acceptable downtimes.
- ICT disaster recovery plans must be maintained and tested to ensure information and ICT assets are available and consistent with agency business and service level requirements.
- Maximum acceptable downtimes for ICT services must also be defined in service and operational level agreements with external parties.
- Copies of ICT disaster recovery plans must be stored in multiple locations including at least one location offsite.

Principle 10 – Compliance management

Agencies must ensure compliance with, and appropriate management of, all legislative and reporting obligations relating to information security.

Legal requirements

- All legislative obligations relating to information security must be complied with and managed appropriately.
- All information security policies, processes and requirements including contracts with third parties, must be reviewed for legislative compliance on a regular basis and the review results reported to appropriate agency management.
- Processes to ensure legislative compliance across all agency activities must be developed and implemented.

Policy requirements

- All reporting obligations relating to information security must be complied with and managed appropriately.
- The Information security compliance checklist must be submitted annually to the ICT Policy and Coordination Office in line with the IS18 reporting requirements.

Audit requirements

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