Information Security (IS18)

Purpose

The business of the Queensland Government covers a diverse range of industries and services, with individual agencies having varying technical and operational requirements in terms of information security controls. This Standard enunciates the mandatory requirements for agencies when establishing, implementing and maintaining information security within their organisation.

This standard provides a starting point for the development of individual agency information security management. Agencies must assess specific risks and take reasonable steps to protect information from misuse and loss and from unauthorised access, modification or disclosure.

The requirements of this Standard are based on the three elements of information security:

Confidentiality	Ensuring that information is accessible only to those authorised to have access;
Integrity	Safeguarding the accuracy and completeness of information and processing methods; and
Availability	Ensuring that authorised users have access to information and associated assets when required.

Policy statement

The Queensland Government has responsibility for a significant amount of information. Agencies must develop, document, implement and review appropriate security controls to protect this information from unauthorised use or accidental modification, loss and release by:

- establishing an appropriate information security culture within the agency;
- implementing security measures commensurate with the information's value, business significance and sensitivity; and
- adhering to all legal and legislative requirements.

Issue and review

This Standard was issued by the Director-General of the Department of Public Works in December 2006. Review of this Standard will occur on an annual basis.

Current Version: V3.00 (Reviewed March 2008)

Implementation

The authority for the implementation of the mandatory principles of the Information Standards is primarily derived from the Financial Management Standard 1997. Existing mandatory requirements of the previous version (V2.00) remain unchanged and have been amalgamated into V3.00.

Due to the increasing need for vigilance in the security of information, V3.00 has identified 9 additional requirements:

- Development of Agency Information Security Plan;

- Allocation of security functions, roles and responsibilities;
- Implementation of Queensland Government Information Security Classification Framework (Sections 2 and 5);
- Implementation of Queensland Government Authentication Framework;
- Implementation of clear desk/clear screen policy in areas dealing with security classified information;
- Implementation of wireless communications security;
- Development of Mobile and Teleworking security processes and risk assessments;
- Consideration of security requirements in all systems design and analysis; and
- Development of Disaster Recovery Plan.

These new requirements must be implemented based on the following dates:

High-level risk assessment:	Completion June 2007
High risk principles implementation:	Completion December 2007

Implementation advice and toolboxes

Implementation advice and toolboxes are provided to assist agencies in implementing the mandatory principles of each Information Standard.

IS18 implementation toolbox

Mandatory principles

Principle 1 - Agency security policy and planning

Agency management must recognise the importance of, and demonstrate a commitment to, maintaining a robust agency information security environment. A clear direction must be provided through the development and implementation of an agency information security policy and an agency information security plan. At a minimum, the policy and plan must:

- detail the direction, scope and approach to the management of information security issues and risks within the agency;
- be reviewed and evaluated in line with changes to agency business and information security risks;
- be consistent with the requirements of the agency General Security plan and information security risk assessment findings; and
- be communicated on an on-going basis and be accessible to all appropriate agency employees.

⊟ Implementation advice

⊟ Use of other security standards

Queensland Government Information Standards are developed to provide agencies with the minimum requirements for ICT management. However, some agencies may find that their particular agency requires more stringent information security controls

to be implemented. In these cases it is suggested that agencies refer to the following Standards for guidance:

- **ISO/IEC 17799:2005**
  International Standard ISO/IEC 17799:2005 - Available through Standards Australia.
- **Commonwealth Protective Security Manual**
  The Australian Government's Protective Security Manual :2005 (PSM) is issued by the Attorney-General's Department. This standard is restricted to Government agencies and can be purchased by emailing: psm@ag.gov.au.
- **ACSI 33**
  Australian Government Information and Communications Technology Security Manual is available through the Department of Defence - Defence Signals Directorate website.

Agencies may also consider the application of various methods and industry frameworks for managing their agency information security. Further information on compliance with standards can be found in the Information Standards Compliance - Reference Sheet located in the ICT Planning (IS2) Implementation Toolbox.

⊟ Developing an information security policy

The Agency Information Security Policy serves as the foundation for information security management within the agency. The development of this policy is the first step in establishing management commitment and the responsibilities for information security within the agency and should therefore be concise and clear. Further information outlining suggested steps in the development of agency security policies can be found in the Developing Information Security Policies - Reference Sheet located in the Information Security Implementation Toolbox.

⊟ General agency security plan

Security and counter-terrorism issues throughout Queensland are coordinated by Security Planning and Coordination (SPC), Department of the Premier and Cabinet together with the Counter Terrorism Coordination Unit (CTCU), Queensland Police Service. To enable agencies to effectively integrate terrorism-related risks into existing risk management arrangements SPC and the CTCU developed the Counter-terrorism Risk Framework.

Under this framework the GAP Project was established to improve the ability of Queensland Government agencies to prepare for, prevent, respond to and recover from potential terrorism-related incidents. Under this framework agencies are required to develop a General Security Plan, which addresses agency building security requirements.

⊟ Developing an information security plan

The level of detail contained in the agency's plan should be commensurate with the agency's business functions and the information security risks that it faces. The plan format and style of the plan is at the discretion of the agency and may if required be a sub-plan of the agency ICT Resources Strategic Plan. The plan should document agency activities which will be undertaken to meet its security requirements as identified by this Information Standard.

The priorities and activities of the plan should be guided by the results of agency information security risk assessments. A Reference Sheet - Developing an Information

Security Plan detailing the suggested contents of the Plan is located in the Information Security Implementation Toolbox.

⊟ Assessing risks

The risk assessment process is crucial in implementing effective information security management. Proposed treatments should be subject to a cost-benefit analysis. Where agencies have no formal process for risk management in place it is strongly recommended that the Australian Standards AS/NZS 4360: 2004 - Risk Management is used. For further information agencies should refer to Queensland Government Information Risk Management Guidelines.

⊟ Reviewing information security

To ensure that security controls in the agency continue to remain relevant to the agency goals, objectives and operational and business environments, the agency's security plan should be monitored and reviewed on an ongoing basis.

It is suggested that agencies review their security plan at least annually to identify changes to the business and technology risk environments and to assess the effectiveness of existing controls.

Further to this, the agency should ensure that security planning becomes an integral component of all agency management, projects and activities rather than an isolated and once a year planning activity.

An Information Security Assessment Toolkit for Queensland Government agencies has been developed to assist agencies in assessing their information security requirements and maturity. This Toolkit is available to agencies by emailing qgcio@publicworks.qld.gov.au. Agencies should also refer to Principle 10 Compliance for further requirements relating to review and compliance.

⊟ Queensland Government information security strategy

A draft of the Queensland Government Information Security Strategy can be accessed by agencies via the Queensland Government GovNet. Once endorsed the strategy will be available on the Queensland Government Chief Information Office website.

This strategy takes account of the current information security and related ICT environment, explores emerging trends, provides guidance in terms of whole-of-Government directions and requirements, and establishes an action plan. The actions of the strategy will:

- ensure that a consistent level of protection for information assets is maintained in any inter-agency transactions;
- assist Queensland Government agencies to meet statutory and legal requirements associated with information security; and
- improve value for money spent on information security.

Over time much of the work undertaken as a consequence of the strategy will be mandated under this Information Standard.

⊟ Government Enterprise Architecture - Security position papers

The Smart Directions Statement requires that agencies demonstrate alignment with the Government Enterprise Architecture (GEA). Alignment with the GEA means having achieved or having the intention to achieve consistency with the directions stated in

priority domains by the specified deadlines. Endorsed GEA Position Paper's define which parts of the Government this applies to, the Queensland Government's position and what the timeframes are for achieving the targets specified.

Endorsed Position Papers which currently impact on agency Information Security include:

- Network Security (Restricted access to Government employees only);
- Network Management (Restricted access to Government employees only);
- Identity Management, Authentication and Authorisation Services (Restricted access to Government employees only); and
- Directory Services (Restricted access to Government employees only).

⊟ Communicating security issues

Communicating security policies to employees is critical to the successful implementation of security across the agency. The processes for regularly communicating all relevant security policies may take the form of notifying staff via email, newsletter distributed to all employees, briefing sessions, network log-on notices or on-line or face-to-face training.

The contents of security incident reports will provide a good source of information as to what areas the agency Security and awareness programs should take into consideration. Refer Principle 4 - Human Resource Security.

Principle 2 - Security framework and third party access

A framework must be established within each agency to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risks to the agency information environment. At a minimum, agencies must:

- allocate and document security functions, roles and responsibilities to implement, maintain and control operational information security within the agency and/or with third party or outsourced service providers;
- document agency requirements for information security when entering into outsourcing contracts and arrangements with contractors and consultants; and
- ensure that prior to providing third parties access to Government information and systems, security controls commensurate with the security classification of the information or system, are in place or clearly defined in appropriate agreements or contracts.

⊟ Implementation advice

⊟ Roles and responsibilities

To ensure a consistent approach to managing security, agencies should establish functions, roles and responsibilities to coordinate, instruct and manage the information security requirements of the agency.

The security functions, roles and responsibilities established by the agency should be appropriate to the nature of the information assets, business requirements and the level of associated risk for information in the agency's care. Functions, roles and responsibilities and required infrastructure will vary across agencies. Further

information can be found in the Security Roles and Responsibilities - Reference Sheet located in the Information Security Implementation Toolbox.

⊟ Security and third parties

When outsourcing a service, agencies remain accountable for the secure performance of that service. Agencies should ensure that appropriate information security and confidentiality requirements are incorporated into contracts and service agreements. To maintain security in regard to third party access and/or outsourcing arrangements the following should be considered by agencies:

- identification of risks from, and associated with privacy and third party access to information, systems, networks or infrastructure;
- determine business needs for third party access; and
- level and type (physical and logical) of access required by the third party.

Agencies also should ensure that requirements under Information Standard, Privacy (IS42) are also taken into consideration when dealing with these issues and that local agency contract and legal guidelines are followed when dealing with these issues.

When engaging ICT contractors or third parties who are external to Government, agencies should refer to the Government Information Technology Contracting Version 5 - Clause 5.4 Confidentiality, Clause 5.5 Privacy and Disclosure of Personal Information and Clause 5.6 Secrecy and Security for security related contract conditions. Further information on establishing ICT contracts can be sourced through the Government Information Technology Contracting (GITC) website.

Principle 3 - Information asset classification and control

Agencies must implement policies and procedures for the classification and protective control of information assets (in electronic and paper-based formats) which are commensurate with their value, importance and sensitivity. When addressing classification and control policies and procedures, the agency must at a minimum ensure:

- all major information assets including hardware, software and services used in agency operations (including physical information assets used to process, store or transmit information) are identified, documented and assigned owners for the maintenance of security controls;
- the classification of all information is in accordance with Queensland Government Information Security Classification Framework - Section 2 ;
- the control of all security classified information (including handling, storage, transmission, transportation and disposal) is in accordance with Queensland Government Information Security Classification Framework - Section 5;
- classification schemes do not limit the provision of relevant legislative requirements under which the agency operates; and
- disposal of public records is in accordance with legislative and regulatory requirements and with the agency's Retention and Disposal Schedules, as approved by the State Archivist or in accordance with the Public Records Act 2002.

⊟ Implementation advice

⊟ Identification of information assets

To ensure that agency information assets are provided with the appropriate level of protection, the agency first needs to identify its assets and assign owners. Suggested information asset classes include:

- employee related information;
- corporate documentation;
- client information;
- hardware and software; and
- infrastructure components.

Agencies should refer to the Queensland Government Information Security Classification Framework for further details on the processes involved in identifying, classifying and protecting information assets.

⊟ Classification and handling of information

Agencies should refer to the Queensland Government Information Security Classification Framework for all information relating to the classification and handling of information assets.

⊟ Disposal of public records

There are a number of legislative and regulatory obligations that have specific requirements concerning the retention and disposal of records that agencies should be aware of. The disposal (including the destruction, sale or transfer) of records can only be performed with the written authorisation of the State Archivist. For further information regarding the disposal of records agencies should refer to Information Standard, Retention and Disposal of Public Records (IS31).

Principle 4 - Human resource security

Agencies must minimise the risk of loss or misuse of information assets by ensuring that security controls are incorporated into agency human resource management. At a minimum, agencies must:

- implement induction and ongoing training and security awareness programs, to ensure that employees are aware of and acknowledge their security responsibilities and that employees are provided with the appropriate skills for the correct use of agency information, systems, facilities and devices;
- document security roles and responsibilities where employees have access to security classified information or perform specific security related roles, and ensure that security requirements are addressed, in recruitment and selection and in job descriptions;
- develop and implement procedures for the separation of employees from, or movement within, the agency;
- communicate responsibilities and procedures to all employees including contractors and third parties for the timely reporting of security incidents including breaches, threats and security weaknesses; and

- ensure that security violations or breaches are investigated and where it is found that a deliberate violation or breach has occurred, that formal disciplinary processes are applied.

⊟ Implementation advice

⊟ Security training and awareness

Agencies should ensure that ongoing security awareness programs are in place to communicate the agency security policy and to actively promote an understanding of the importance of security within the agency.

Refer to the Human Resource Security - Reference Sheet located in the Information Security Implementation Toolbox for issues to consider when addressing information security training and awareness.

⊟ Security in job descriptions

It is critical that all employees are aware of their responsibilities with respect to information security. Whilst many general issues relating to security and employee behaviour will be outlined in the agency Code of Conduct, and in many cases this may be sufficient, it is suggested that agencies consider the implementation of employee agreements or acknowledgement processes to clarify and reinforce both general and specific security responsibilities. The agency may also consider adding specific security clauses in its Code of Conduct.

Depending on the nature of the agency business, consideration should be given as to whether security responsibilities should be outlined in all job descriptions.

Acknowledgment of responsibilities by the employee in writing should always be considered when a position involves the handling of security classified information.

Further information can be found in the Human Resource Security - Reference Sheet which is located in the Information Security Implementation Toolbox.

⊟ Separation of employees

Agencies should ensure that security processes are in place for the exit or movement of employees, contractors or other third parties from or within the agency. These processes may include:

- exit interviews;
- revoking of access rights and disabling of all User-IDs; and
- at the time of leaving, ensure that all keys, access devices, credit cards, etc, are collected from the employee.

Further information can be found in the Human Resource Security - Reference Sheet located in the Information Security Implementation Toolbox.

⊟ Reporting of security incidents

Agencies should ensure that all users of information and information facilities are educated in reporting any observed or suspected security threats through appropriate management channels. Agencies should refer to the Incident Management - Reference Sheet in the Information Security Implementation Toolbox for issues to consider when developing the agency security reporting processes.

⊟ Disciplinary processes

The disciplinary actions and processes should be determined under the Public Service Act 1996 and/or other relevant legislation that the agency operates under. Agencies should refer to Incident Management - Reference Sheet in the Information Security Implementation Toolbox for issues to consider when developing agency disciplinary processes.

Principle 5 - Physical and environmental security

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. At a minimum, agencies must ensure that:

- building and entry controls are in place for areas used in the processing and storage of security classified information;
- physical security protection (commensurate with the security classification the level of the information) is in place for all government offices, rooms, storage facilities and cabling infrastructure;
- computer and communications equipment, where practical, are located in secure areas with access control mechanisms in place to restrict use to authorised personnel only, and that where physical controls are not possible, other control methods are in place;
- policies and processes are implemented to monitor and protect the use and/or maintenance of information, equipment, storage devices and media away from agency premises, and in situations where a risk assessment determines, additional control mechanisms are in place;
- policies and processes are implemented for the secure disposal and/or reuse of equipment, storage devices and media (including, delegation, approval, supervision, removal methods and training of employees) which are commensurate with the security classification level of the information stored on the asset; and
- general control policies including a clear desk and clear screen policy are implemented in information processing areas that deal with security classified information.

⊟ Implementation advice

⊟ Physical security controls

At a minimum a secure area would be a locked office. However the level of physical controls to be implemented would depend on risk and the sensitivity or importance of the information to be protected. When securing information processing or storage areas, agencies should address and establish practices for monitoring and review of access mechanisms.

Physical perimeters and physical entry controls could include the issuing of access tokens or cards for access to computer processing facilities or areas where information is stored or processed in particular those where security classified information or valuable equipment is in use.

Agencies should refer to the Queensland Government Information Security Classification Framework for further details on securing areas which are used for the storage and processing of security classified information and systems.

⊟ Computer equipment

All computer equipment including personal computers, servers and terminals should, where practical, be located in an area with access restricted to Government personnel, external contractors and other authorised third parties. Where access to computing equipment (eg. system consoles) will allow access to security classified information, access to that equipment should be restricted to authorised users.

Agencies should address environmental and building factors when siting computer rooms and information processing facilities. Where possible, agencies should implement physical computer room controls to meet minimum Australian Standards requirements such as Computer Accommodation AS 2834.

Equipment should be protected from power failures or other electrical anomalies. An un-interruptible power supply (UPS) and backup generators should be considered for equipment supporting business operations. Agencies should refer to the Queensland Government Information Security Classification Framework for further details.

⊟ Communications equipment

To prevent unauthorised disclosure of information, or tampering, communications equipment should be located in a secure area with access restricted to authorised personnel, contractors or consultants.

To protect critical communications equipment agencies should consider locked cabinets, etc, with restricted access, and where possible, communications equipment should be hidden from view. Agencies should refer to the Queensland Government Information Security Classification Framework for further details.

⊟ Information and assets outside the agency

Security risks should be assessed before locating information and information facilities off-site from Government office space. Agencies should ensure that policies concerning the security of both paper based records and mobile equipment taken off site are developed and implemented.

When removing information assets employees should be made aware of their responsibilities including the following:

- equipment and media shouldn't be left unattended in public places;
- laptop computers should be taken as hand luggage when travelling; and
- appropriate security controls are in place and observed when telecommuting.

Further details on movement of information assets outside the agency can be found in the Queensland Government Information Security Classification Framework and the Mobile and Tele-working Security - Reference Sheet located in the Information Security Implementation Toolbox.

⊟ Maintenance and disposal

To ensure availability and integrity of information, equipment should always be maintained according to manufacturers' maintenance guidelines. Maintenance processes cover a wide range of activities including preventative, repair and upgrade maintenance, which may be the result of scheduled or non-scheduled activities. Agencies need to ensure that adequate policies and processes are in place to protect agency information, during any maintenance process.

Further information concerning processes for maintenance and disposal of equipment and media can be found in, Australian Government Information and Communications Technology Security Manual (ACSI 33), or in the Equipment and Media Disposal - Reference Sheet located in the Information Security Implementation Toolbox.

⊟ General security controls

To minimise the threat of information misuse or theft, the implementation of a 'clear desk and clear screen' policy should be considered for all areas used for the storage, printing and processing of non-classified information. General operation controls for computer and other office equipment including practices for unattended computer equipment should also be considered.

The security of offices, rooms and facilities can be improved by establishing secure working practices, such as the escorting of visitors and service contractors by authorised employees in areas containing sensitive information and equipment. Restricting out-of-hours access, or the installation of access monitoring controls, should also be considered.

Agencies should refer to the Queensland Government Information Security Classification Framework for further details on general control policies.

Principle 6 - Operational security management

Operational procedures and controls must be documented and implemented to ensure that information, information systems and network tasks are managed securely and consistently, in accordance with the level of required security. Agencies must at a minimum ensure:

- incident management procedures and mechanisms to review violations are in place to ensure appropriate responses in the event of security incidents, breaches or failures;

- adequate controls are in place for the prevention, detection, removal and reporting of attacks of malicious and mobile code on information systems and networks;

- comprehensive systems maintenance processes and procedures including operator and audit/fault logs and information backup procedures are in place;
- operational change control procedures are implemented to ensure that changes to information processing facilities or systems are appropriately approved and managed;
- methods for exchanging information in all forms, between agencies and/or third parties are compliant with legal and legislative requirements and consistent with the classification schemes and controls defined in the Queensland Government Information Security Classification Framework; and
- on-line transactions and services are assessed against and consistent with the requirements of the Queensland Government Authentication Framework.

⊟ Implementation advice

⊟ Operational procedures and responsibilities

When documenting operational procedures agencies should at a minimum ensure that detailed operating instructions are in place for all processes outlined in the mandatory principles of this Information Standard.

In terms of assigning operational responsibilities agencies should consider the separation of operational functions and duties where procedures involve activities, which could be susceptible to unauthorised activity, misuse of information or pose a conflict of interest, such as security audits.

⊟ Network management procedures

Network security management is critical to the overall security of the agency information environment. Agencies should ensure that appropriate management practices are in place for network security, and that these are automated where possible in order to address scalability requirements and to reduce costs. Processes in place for secure network management include but are not limited to:

- maintaining current documentation for firewall and security device configurations;
- security configuration management and software updates;
- monitoring and analysis of logs from firewalls for security breaches;
- alerts for detected breaches and intrusion attempts, and a documented response process; and
- regular testing of network security.

Agencies should refer to the Government Enterprise Architecture (GEA) Network Security Position Paper and Network Management Position Paper for targets.

⊟ Security incident management

All information security incidents should be investigated promptly. Procedures for investigations should attempt to identify the cause, minimise any adverse consequences and recommend actions that will ensure similar incidents do not happen again. Suggested incident management procedures are located in the Incident Management - Reference Sheet located in the Information Security Implementation Toolbox.

⊟ Controls for malicious and mobile code

Malicious software is one of the major threats to agency information security. There are many types of malicious and mobile code that can severely impact information networks, systems and data and undermine the integrity, confidentiality and availability of information.

As new types of virus and code are being introduced on an ongoing basis, anti-virus scanners are only as effective as the regularity of their update. The method and frequency of updates should be considered when selecting anti-virus and malicious code prevention and protection software.

Refer to the Operational Management - Reference Sheet located in the Information Security Implementation Toolbox when addressing the key aspects which should be considered when implementing and maintaining virus and malicious code programs.

⊟ Logging processes

Agencies should ensure that logging of user activities, exceptions and security events are recorded. When conducting the monitoring of systems or user activities agencies should ensure that their monitoring activities are in line with all legislative obligations and the risk the system or activities pose to the security of the environment. Agencies should refer to Information Standard, Use of ICT Facilities and Devices (IS38) for further information regarding the monitoring of Internet and email and Information Standard, Privacy (IS42 and IS42A) for obligations regarding the protection of personal information.

Audit, fault, administrator and operator logs should be maintained, monitored and reviewed on a regular basis to assist in maintaining the security of the agency information environment. Further information on suggested data to capture in logs can be found in the Operational Management - Reference Sheet located in the Information Security Implementation Toolbox.

⊟ Backup procedures

Backup cycles should be related to the business risk, frequency with which data and software is changed and the criticality of the system to business operations. The cycle should include, as a minimum:

- incremental daily backups of data and full weekly backups of all data, operating system and applications. Backups of data on a cycle deemed appropriate by the IT Manager, but as a minimum, on a weekly basis; and
- backups of the complete operating system, and applications on a cycle deemed appropriate by the IT Manager, but as a minimum, on a monthly basis.

Further details on implementing can be found in the Operational Management - Reference Sheet which is located in the Information Security Implementation Toolbox.

⊟ Change control procedures

To minimise threats to the operational environment agencies should consider but not limit activities to ensuring:

- adequate testing and change control mechanisms are in place for the migration of new or modified systems into the operational environment; and
- that the information environment is managed in a way that will easily accommodate changes or future expansions so as to not adversely impact the operational environment.

Agencies should refer to Principle 8 - Systems Development and Maintenance for further details on controls relating to change control.

⊟ Secure handling and exchange of information

To ensure the security of information exchanged within the agency and with external parties, including on-line information systems, the agency should ensure information handling and exchange procedures are established in line with the Queensland Government Information Security Classification Framework and the Queensland Government Authentication Framework.

Principle 7 - Access controls

Control mechanisms based on business owner requirements and assessed/accepted risks must be in place for controlling access to all information, information systems, networks (including remote access), infrastructures and applications. Access control rules must be consistent with agency business requirements and information classification as well as legal and legislative obligations. At a minimum, agencies must ensure that:

- access requirements are assessed against the Queensland Government Authentication Framework;
- access to agency information systems requires specific authorisation and that each user is assigned an individually unique personal identification code and secure means of authentication;
- policies and procedures are defined, documented and implemented for the management of operating systems security, including user registration, authentication management, access rights and privileges to systems or application utilities;
- restricted access and authorised use only warnings are displayed upon access to all agency systems;
- where wireless communications are used, that the security features of the product are appropriately configured and afford at least the equivalent level of security of wired communications;
- control measures are implemented to detect and regularly log, monitor and review information systems and network access and use, including all significant security relevant events;
- risk assessments are conducted and policies and processes are defined for mobile technologies and teleworking facilities; and

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

⊟ Implementation advice

⊟ Access management policy

Access control policies should address and detail access control rules and rights for each group of users. Generally these should be based on "what must be generally forbidden unless expressly permitted" ensuring that business requirements are followed. The overall framework for access rights should be reviewed on a regular basis to determine that they remain appropriate.

⊟ User access management

User access rights should be in accordance with the requirements of the information owner and should be authorised by the user's manager before the user is granted access to the information or system. All changes to employees' user duties should be reflected in access control rights, with all changes being carried out on a timely basis.

Agencies should ensure that there are documented procedures which take Service desk staff through a strict set of client identification steps so that the bona fides of a caller requesting a password reset can be established. Procedures may include an email back to the account holder and/or manager of account holder which operates as detective control providing an 'alert' that a password has been requested and changed or password reset requests having to be in writing (usually per email).

Agencies should ensure that access privileges are disabled or modified when users change jobs, or leave the agency for a prolonged period of time or permanently. Further information can be found in the Access Controls - Reference Sheet located in the Information Security Implementation Toolbox, or in Government Enterprise Architecture (GEA) Identity Management Position Paper.

⊟ Remote access

To minimise risks from external connections, agency remote access processes should at a minimum register all persons with remote access privileges and log all remote access attempts and activity and ensure all users are authenticated before access to the network is granted. Agencies should refer to the Government Enterprise Architecture (GEA), Network Security Position Paper for targets concerning remote access management.

⊟ Application and utilities management

Access to systems utilities that may be used to alter data or program code should be kept to a minimum with all systems master passwords restricted to, and maintained by, the information and system security Administrator or applicable position. Further information can be found in the Access Controls - Reference Sheet located in the Information Security Implementation Toolbox.

⊟ Authentication management

The Queensland Government Authentication Framework (QGAF) provides a process and a set of definitions which will allow agencies, as service providers, to evaluate the risk associated with their services and determine the appropriate level of authentication assurance required. Agencies should refer to the QGAF series of documents for detailed information regarding authentication management.

Agencies should also refer to the Government Enterprise Architecture (GEA), Identity Management, Authentication and Authorisation Position Paper for targets concerning authentication management.

⊟ Network controls and services

Policies should be documented outlining methods for security and consistency of data, computers and communications infrastructure in agency networks. To prevent and reduce the risk of users selecting routes to network services outside authorised access paths, agency access control processes and policies should implement enforced network paths.

Agency network access policies should also document how they intend to manage and protect information integrity and availability on agency networks from authorised and unauthorised connections.

Agencies should also refer to the Government Enterprise Architecture (GEA) Network Security Position Paper for targets related networks.

⊟ Wireless communications

Agencies should refer to the Government Enterprise Architecture (GEA) Network Security Position Paper for further information regarding wireless security requirements.

⊟ Monitoring system access and use

In access control policies, agencies need to consider, what events and which systems need to be logged and monitored in order to detect deviation from normal access in the event of security incidents, and the risk these pose to agency information and systems. These logs should include recording exceptions and access logs along with access activities such as:

- user IDs, successful and failed logon and logoff dates and times and files accessed;
- use of systems utilities and operator privileges;
- systems failures and alerts including failed access attempts through firewalls and gateways; and
- significant security relevant events (for example time of logins, modification to critical business application).

⊟ Mobile equipment and teleworking

Agencies should ensure that policies and procedures are in place for the use and access of mobile computing devices to agency infrastructure and networks including mobile devices such as laptops, phones and other hand held devices palm pilot devices.

Clear policies and procedures should also be in place to manage the security of equipment information and access to agency networks for employees engaged in teleworking arrangements.

Further information can be found in the Mobile and Teleworking Security - Reference Sheet located in the Information Security Implementation Toolbox or the Government Enterprise Architecture (GEA) Network Security Position Paper.

⊟ Internet and email security

When addressing policies and procedures for the security of Internet and email use within the agency, the following points provide a starting point for agencies to consider:

- the implementation of passwords for access to internet and email systems;
- the implementation of software for blocking access to unauthorised or potentially inappropriate Internet sites and for scanning email for unauthorised content and malicious and mobile codes; and
- the implementation of clear and unambiguous Internet and email use protocols, policies and procedures.

Further details can be found in the Information Standard, Use of ICT Facilities and Devices (IS38) and in the Operational Management - Reference Sheet located in the Information Security Implementation Toolbox.

⊟ Secure use of ICT facilities and devices

Agencies should establish policies and procedures to assess the risks posed by new and existing ICT facilities and devices technologies based on the security risks to agency information, information systems and network, including palm and handheld devices; telephones (including mobiles); removable media; radios or other high frequency communication devices; television sets; digital or analogue recorders (including DVD and video); cameras; photocopiers; facsimile machines; printers (and other imaging equipment). Agencies should refer to Information Standard, Use of ICT Facilities and Devices (IS38) and the Government Enterprise Architecture (GEA) Network Security Position Paper for further details.

⊟ Related information standards

- Use of ICT Facilities and Devices (IS38)

Principle 8 - System development and maintenance

Security controls must be in place during all stages of system development, as well as when new systems are implemented into the operational environment. Such controls must be commensurate with the security classification of the information contained within, or passing across, information systems, networks infrastructures and applications. When establishing new systems or implementing improvements to current information systems including off-the-shelf or outsourced software development, agencies must at a minimum ensure:

- security requirements are addressed in the specifications, analysis and/or design phases and that internal and/or external audit are consulted when implementing new or significant changes to financial and critical business information systems;

- processes including data validity checks, audit trails and activity logging are included in applications to ensure the accuracy and integrity of data captured or held in applications;
- authentication techniques and policies are consistent with those of the Queensland Government Authentication Framework requirements;
- appropriate change control, acceptance and system testing, planning and migration control measures are carried out when upgrading or installing software in the operational environment;
- that access to system files is controlled to ensure integrity of the business systems, applications and data; and
- access controls including access restrictions and segregation/isolation of systems are identified and implemented into all infrastructures, business and user developed applications.

⊟ Implementation advice

⊟ System security requirements

The security requirements and specifications should be addressed and agreed with the business owners of any new or improved system in the initial stages of development, or acquisition. These requirements should identify and address any potential risks, vulnerabilities and/or conflicts with existing systems or business processes. Where possible, authentication should be managed through a separate enterprise directory product. Where appropriate agencies may should also consider seeking independent evaluation or security certification of systems.

Agencies should ensure that applications which are to be implemented into the web environment undergo a stringent risk assessment process in the development phase and during the life of the application to ensure appropriate security controls are in place.

Agencies should also ensure that patch management issues are assessed and considered prior to the implementation of systems and in the case of developed applications that periodic code reviews are incorporated into security maintenance.

Further information can be found in the Government Enterprise Architecture (GEA) Directories Position Paper.

⊟ Validation checks

Agencies should ensure that implementation policies and processes outlining the practices for input validation, internal processing checks and controls, message authentication techniques and output data validation are in place to ensure appropriate security of all application and systems development. These processes should be in accordance with the risks associated with the system data. Audit trails and activity logs should also be written into applications for the validation of data and internal processing.

⊟ Cryptographic controls

Agencies should refer to the Queensland Government Authentication Framework for further information regarding cryptography and authentication methods.

⊟ System development and support

Policies and processes should be in place for control of changes to operational applications including version control for software upgrades. To minimise threats to the operational environment agencies should consider but not limit activities to ensuring:

- adequate testing and change control mechanisms are in place for the migration of new or modified systems into the operational environment; and
- that the information environment is managed so that future expansions or changes can be accommodated and do not adversely impact the operational environment.

⊟ Access and system file security

Operational software should be maintained at a level supported by the supplier. Appropriate testing, planning and migration control measures should be carried out when upgrading patches or new software versions to ensure the overall security of the agency operational environment is not adversely impacted. The testing of systems and data should be controlled and monitored especially where operational data sets are used.

Access controls should be implemented to ensure restricted access to all systems and applications including system source code.

Principle 9 - Business continuity and disaster recovery management

A managed process including documented plans must be in place to enable the information environment to be restored or recovered in the event of a disaster or major security failure. At a minimum, agencies must:

- establish processes to assess the risk and impact of the loss of information or systems on agency business in the event of a disaster or security failure;
- develop methods for reducing known risks to agency information or systems; and
- ensure business continuity and disaster recovery plans are maintained and tested to ensure systems and information are available and consistent with agency business and service level requirements.

⊟ Implementation advice

⊟ Assessing and reducing risks

When developing information risk management strategies to assess the vulnerability of information assets and the impact on these assets as a result of a security failure or a disaster, agencies should consider adapting the Australian Standards AS/NZS 4360:2004 Risk Management. Further information can also be found in the

Information Risk Management Best Practice Guide located on the Information Standards website.

⊟ Business continuity and disaster recovery planning

The Queensland Government Chief Information Office is currently developing Business Continuity and Disaster Recovery Frameworks. These frameworks will be available for consultation in early 2007.

In the interim, when developing business continuity management plans, agencies should consider adapting the Australian Standards HB:221:2004 Business Continuity Management available through the Australian Standards website. Further detailed information on both Business Continuity and Disaster Recovery Plans can be found in the Information Risk Management Best Practice Guide located on the Information Standards website.

⊟ Review and testing of plans

Agency business continuity plan's should be reviewed and tested on a regular basis to ensure that all current business and ICT systems and infrastructure are accounted for. When developing the agency testing strategy, the importance of each system to the business operations and the ability to recover it within the time frames required by users should determine the extent of the testing.

Agencies should also undertake a review of their plans and strategies after any significant disruption to information services or failure to ascertain the cause, assess the remedy and ensure procedures are adjusted to reduce the likelihood of any repeat occurrence.

Principle 10 - Compliance

Agency information security controls for all information processes, systems and infrastructure must adhere to any legislative or regulatory obligations under which the agency operates. To ensure all legal, statutory, regulatory, contract or privacy obligations relating to information security are managed appropriately agencies must at a minimum:

- ensure that all reasonable steps are taken to monitor, review and audit agency information security effectiveness, including the assignment of appropriate security roles and engagement of internal and/or external auditors and specialist organisations where required; and
- all agency information security policies, processes and requirements including contracts with third parties, are reviewed for compliance on a regular basis and reported to appropriate agency management.

⊟ Implementation advice

⊟ Compliance with policies and standards

As outlined previously this Information Standard provides only the minimum security requirements for agencies, in agencies that manage a large amount of security classified information it is suggested that agencies refer to the following Standards for guidance:

- International Standard ISO/IEC 17799:2005 - Available through Standards Australia;
- The Australian Government's Protective Security Manual (PSM) is issued by the Attorney-General's Department. This standard is restricted to Government agencies and can be purchased by emailing: psm@ag.gov.au; and
- ACSI 33 - Australian Government Information and Communications Technology Security Manual is available through the Department of Defence - Defence Signals Directorate website.

Information security policies, procedures and compliance should be reviewed and reported on to appropriate management at least annually to ensure the reliability and overall effectiveness of the security controls for all information systems, networks infrastructures and applications.

Agencies should ensure that appropriately qualified personnel are assigned to audit the compliance of the information environment against agency policies, processes and industry technical standards to ensure appropriate security levels are maintained. These personnel should, where practical, not be involved in the operational information or systems environment of the agency.

⊟ Legal and legislative compliance obligations

Agencies should develop processes and where appropriate seek advice on legal compliance to ensure that all legal and legislative obligations under which they operate are observed when using and managing information.

Agencies should include in their agency security education and awareness programs, the responsibilities for compliance with legal and legislative issues, in particular copyright, intellectual property, licensing and terms and conditions of use infringements of information and software systems.

Agencies are required under Information Standard, Privacy (IS42) and IS42A, to ensure that records of personal information are protected by such security safeguards as it is reasonable in the circumstances to take. This includes protection against loss, against unauthorised access, use, modification or disclosure and other misuse. A Privacy and security statement should be placed on the agency's website. A model privacy and security statement can be found in the Information Privacy Guidelines located on the Information Standards website.

Agencies should ensure that security controls provide the agency with the necessary safeguards to ensure records are protected in accordance with the Public Records Act 2002, Freedom of Information Act 1992 and the Information Standards Recordkeeping (IS40) and Managing Technology-Dependent Records (IS41).

⊟ Related information standards

- Information Standard, Privacy (IS42)
- Information Standard, Privacy (IS42A) (for Queensland Health)
- Information Standard, Recordkeeping (IS40)
- Information Standard, Managing Technology-Dependent Records (IS41)