Queensland Government Information Security Policy – Mandatory Clauses

Final

November 2010

v1.0.2

PUBLIC

ICT Policy and Coordination Office
Department of Public Works

Queensland Government

Document details

Security classification	PUBLIC		
Date of review of security classification	November 2010		
Authority	Queensland Government Chief Information Officer		
Author	ICT Policy and Coordination Office (Policy Development)		
Documentation status	Working draft	Consultation release	☑ Final version

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Director, Policy Development
ICT Policy and Coordination Office
ICTPolicy@qld.gov.au

Acknowledgements

This version of the Queensland Government Enterprise Architecture (QGEA) *Queensland Government Information Security Policy – Mandatory Clauses* was developed and updated by the ICT Policy and Coordination Office.

This guideline is based on Annex A Control objectives and controls of the AS/NZS ISO IEC 27001:2006 Information technology – Security techniques – Information security management systems – Requirements. Reproduced with permission from SAI Global under Licence 0911-C028.

Feedback was also received from a number of agencies, including members of the Information Security Reference Group, which was greatly appreciated.

Copyright

Queensland Government Information Security Policy – Mandatory Clauses

Copyright © The State of Queensland (Department of Public Works) 2010

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

Introduction

Purpose

This Queensland Government Information Security Policy – Mandatory Clauses document ('this document') details the mandatory clauses which must be included in agency's Information Security Policy as per the requirements of Information Standard 18: Information Security (IS18). In addition, this document also provides context to the mandatory clauses by structuring them within an example information security policy, with additional guidance provided on other issues which agencies may wish to consider when developing their policies. An agency's information security policy provides a governance for information security management, direction and support within the agency. The development and approval of an agency's information security policy not only establishes management commitment and governance arrangements, but defines the agency's policy in all aspects of information security, including asset management, human resource management and compliance.

Audience

This document is primarily intended for Chief Information Officers, security managers, policy officers and other ICT managers and staff responsible for information security policy, planning and implementation.

Scope

This document relates to the Information Security Policy, Planning and Governance domain within the Information Security slice of the QGEA.

Implementation and mandatory clauses

This document forms part of the mandatory requirements of IS18. Under IS18, Principle 1 – Policy and Governance, agencies are required to develop an Information Security Policy which must contain the mandatory clauses detailed in this document. These mandatory clauses are numbered using red text under each information security domain[1] and must not be altered or deleted.

Following the mandatory clauses are agency clauses which are suggestions for agencies to consider for inclusion within the policy. In addition, agencies are encouraged to add more information and policy statements to ensure all their information security and business requirements are met. Information for agencies to consider is highlighted in blue text within a grey box.

Examples are as follows:

Queensland Government Mandatory Clauses

0.0.1 This is a mandatory clause and cannot be altered or deleted.

0.0.2 This policy was approved on [*blue italic text indicates where agencies can insert free text eg. dates*]

[1] The Queensland Government Information Security Policy Framework defines the various domains and sub-domains of information security. These domains have been used to frame this document and IS18.

Agency Clauses

0.0.2 This is a recommended clause and can be altered or deleted.

0.0.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *xxx*
- *xxx*

In addition, under section 1.1 Information Security Policy – Obligations, there is listed a number of mandatory quality criteria. While these are not mandatory clauses and do not have to be included within the agency's Information Security Policy, they are still activities which agencies must undertake to ensure their Information Security Policy is compliant with IS18. The mandatory quality criteria are highlighted in red text within a grey box, an example of which follows:

Mandatory Quality Criteria:

- xxx

Agencies are strongly recommended to use this document as a basis/template for their Information Security Policy. As can be seen from the above, agency specific policy statements can be added and the blue text/grey box can be deleted.

Information security policy structure

The first section of the agency's information security policy should detail general information about the overall objective of the policy, the scope, who it applies to, legislative obligations, who is responsible for review and approval of the policy. The sections following this introduction detail the policy requirements structured in line with IS18 and the information security domains at two levels. The level 1 and level 2 information security domains are detailed within the Queensland Government Information Security Policy Framework diagram located at Appendix A.

The structure of the policy is at the agency's discretion. Agencies may wish to develop one single information security policy document. Alternatively, agencies may choose to develop an overarching broad policy that covers strategic intent at a portfolio or agency level with each subordinate agency/functional domain having consistent but tailored specific information security policy statements. For example:

- **High level policy** – A brief document that sets the strategic directions for security and assigns the broad responsibility for security within the agency.
- **Middle level policy** – Document/s that address specific information security issues. Ideally agencies should document policies for each level 1 in the Queensland Government Information Security Policy Framework diagram (Appendix A).
- **Low level policy** – These documents deal with general issues and system specifics. Subject areas may correspond with the level 2 domains.
- **Outputs** – Operational documents that enable compliance with the policies and include the technical details and operational specifications, practices and tasks. For example this could include work instructions, guidelines, templates, reports, checklists, assessments and plans.

Alternatively, each agency within the portfolio may have its own entire set of policies. However, it is recommended that there is then some comparison and harmonisation of policies across the portfolio. A diagram depicting an example policy structure within agencies is shown at Appendix B.

1 Policy, planning and governance

1.1 Information security policy

The information security policy domain includes all aspects of management direction and support for information security in accordance with business, legislation and regulatory requirements. Activities will include policy around compliance, but actual compliance actions should be mapped to compliance management (refer section 10).

The following sections detail the mandatory clauses, mandatory quality criteria, and suggested headings and information for agency consideration when developing the introduction of the agency's information security policy:

Policy statement

[*Insert agency statement here*]

The policy statement should be a concise statement of 'what' the policy is intended to accomplish. It should be two to three sentences long and should clearly reflect the overall government direction, the agency's direction and what the policy is hoping to achieve. The statement should be general enough to provide some flexibility and accommodate periodic changes in agency and whole-of-Government related requirements and standards.

Scope

[*Insert agency scope here*]

The scope details any limitations or constraints on the applicability of the policy to situations or entities within the agency. This policy should be developed in conjunction (or consultation) with relevant business areas such as finance, audit and senior business management. Agencies should also ensure this policy (and associated processes) adequately addresses security considerations relating to off-site work arrangements (eg. home-based, mobile, regional, interstate and overseas).

Objectives

[*Insert agency objectives here*]

This section details the agency's policy objectives, how these policy objectives will be achieved and what resourcing will be supplied to support the implementation of the policy. For example the agency's objectives could be to:

- *protect the agency's information assets through safeguarding its confidentiality, integrity and availability*
- *establish effective governance arrangements including accountability and responsibility for information security within the agency*
- *maintain an appropriate level of employee awareness, knowledge and skill to minimise the occurrence and severity of information security incidents*
- *ensure the agency is able to continue and/or rapidly recover its business operations in the event of a detrimental information security incident.*

Obligations

[*Insert agency obligations here*]

A number of regulatory or legal frameworks, guidelines or policies will impact on the development and implementation of the policy. The following mandatory quality criteria have been provided to ensure the agency's Information Security Policy adheres to the requirements of IS18:

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.

In addition, a suggested list of relevant legislation, standards and policies have been provided, but are a guide only and agencies need to update this list accordingly:

Legislation

- *Financial Accountability Act 2009 (Qld)*
- *Financial and Performance Management Standard 2009 (Qld)*
- *Electronic Transactions Act 2001 (Qld)*
- *Information Privacy Act 2009 (Qld)*
- *Public Records Act 2002 (Qld)*
- *Public Sector Ethics Act 1994 (Qld)*
- *Public Service Act 2008 (Qld)*
- *Right to Information Act 2009 (Qld)*
- *Workplace Health and Safety Act 1995 (Qld)*
- *Workplace Health and Safety Regulation Act 2008 (Qld)*
- *Cybercrime Act 2001 (Cth)*
- *Electronic Transactions Act 1999 (Cth)*
- *Security Legislation Amendment (Terrorism) Act 2002) (Cth)*
- *Spam Act 2003 (Cth)*
- *Telecommunication Act 1997 (Cth)*

Standards/guidelines

- IS18
- *AS/NZS ISO/IEC 27001:2006 Information technology – Security techniques – Information security management systems – Requirements*
- *AS/NZS ISO/IEC 27002:2006 Information technology – Security techniques – Code of practice for information security management*
- *Information Standard 38, Use of ICT Facilities and Devices (IS38)*
- *Queensland Government Counter-Terrorism Strategy 2008-2012 – Department of the Premier and Cabinet (function now residing in Queensland Police)*
- *Queensland Counter Terrorism Plan 2007 – Department of the Premier and Cabinet (function now residing in Queensland Police)*
- *Government Asset Protection Framework – Queensland Treasury*

Agency policy

- *General Security Plan (including strategic security objectives)*
- *Information Security Risk Assessment Findings*
- *Code of Conduct*
- *HR – Personnel Recruitment Policies.*

Implementation

[*Insert agency implementation requirements here*].

Queensland Government Mandatory Clauses

1.1.1 This policy will be communicated on an ongoing basis and be accessible to all employees.

Agency Clauses

1.1.2 [*Insert agency specific clauses*].

The implementation and review section details how the policy will be implemented including how the policy will be communicated and be accessible to all appropriate agency employees.

Details the performance measures or review mechanisms established to ensure the policy is being implemented effectively.

Policy owner/enquiries

[*Insert agency text here*].

Agencies should identify the owner of the Information Security Policy and who is responsible for the development and ongoing review of the policy. Contact details for enquiries should be listed in this section.

Policy approval

[*Insert agency policy approval here*]

Queensland Government Mandatory Clauses

1.1.3 This policy [insert version number] was endorsed by [*insert name of governance body*] on [*insert date*].

1.1.4 This policy [*insert version number*] was approved by [*insert name and role title*] on [*insert date*].

Agency Clauses

1.1.5 [*Insert agency specific clauses*].

This section details the specific delegations for approval of security policies.

Agencies should obtain appropriate approval/endorsement/signoff from the agency Chief Executive Officer and their Information Steering Committee or similar agency governance body.

Policy review

[*Insert agency review details here*]

Queensland Government Mandatory Clauses

1.1.6 This policy is reviewed [*annually/biannually*]. The next scheduled review is [*insert date*].

1.1.7 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.

Agency Clauses

1.1.8 [*Insert agency specific clauses*].

The agency should review their policy periodically (at least annually) and as a result of significant changes to the agency business or structure, machinery-of-Government changes, information security risk analysis, information security compliance assessment and reports of security incidents.

1.2 Information security plan

The information security plan domain includes all activities relating to developing and maintaining information security plans, and ensuring that plans are communicated and accessible to employees as necessary.

Queensland Government Mandatory Clauses

1.2.1 An Information Security Plan must be developed and must align with agency business planning, general security plan and risk assessment findings.

1.2.2 Endorsement for the Information Security Plan must be obtained annually from the relevant senior executives and governance body.

1.2.3 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.

Agency Clauses

1.2.4 [*Insert agency specific clauses*].

Agencies should provide a brief summary of their Information Security Plan including a link to where the plan is located. See principle 1 of IS18 for details relating to the mandatory requirements.

1.3 Internal governance

The internal governance domain includes all activities related to the governance, authorisation and auditing of information security arrangements within the organisation. Roles and responsibilities relating to information security within the agency should also be defined.

Queensland Government Mandatory Clauses

1.3.1 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.

1.3.2 Endorsement for the information security internal governance arrangements must be obtained from the relevant senior executives and governance body.

Agency Clauses

1.3.3 [*Insert agency specific clauses*].

See principle 1 of IS18 for details relating to the mandatory requirements. Agencies should also consider the following:

- *detail the agency's internal governance arrangements – eg. an information security committee (ISC) or existing committee exists within the agency*
- *information security controls should address all relevant business requirements and considerations*
- *information security controls should be integrated with all agency processes to create a coherent approach to agency business*
- *the accountability and responsibilities for information security should be clearly outlined including the implications of breaches of security policy.*

Further information on information security roles and responsibilities is detailed in the Information Security Internal Governance Guideline located in the Information Security Implementation Toolbox. In addition, information relating to Use of ICT planning in ICT governance is detailed within Principle 3 of Information Standard 2, ICT Resources Strategic Planning.

1.4 External party governance

The external party governance domain includes all activities related to the governance, authorisation and auditing of information security arrangements for external parties that handle organisational information.

Queensland Government Mandatory Clauses

1.4.1 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.

1.4.2 Endorsement for the information security external governance arrangements must be obtained from the relevant senior executives and governance body.

Agency Clauses

1.4.3 [*Insert agency specific clauses*].

See principle 1 of IS18 for details relating to the mandatory requirements. Agencies should also consider the following:

- *detail agency participation in external/whole-of-Government information security committees*
- *detail the external organisations that handle the organisation's information*
- *are there policies and processes in place at these external organisations?*

Further information on information security roles and responsibilities is detailed in the Information Security Internal Governance Guideline located in the Information Security Implementation Toolbox. In addition, information relating to the QGEA is located on the website.

2 Asset management

2.1 Asset protection responsibility

The asset protection responsibility domain includes all activities that implement and maintain appropriate protection of organisational assets.

Queensland Government Mandatory Clauses

2.1.1 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).

2.1.2 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.

2.1.3 All ICT assets that provide underpinning and ancillary services must be protected from internal and external threats (eg. mail gateways, domain name resolution, time, reverse proxies, remote access and web servers).

Agency Clauses

2.1.4 [*Insert agency specific clauses*].

Information should be provided about the agency's information asset register (or similar registers for security classified information), including what information assets are identified, documented, the owners/custodians etc. Further information on the requirements of information asset registers can be located in Information Standard 44, Information Asset Custodianship (IS44).

2.2 Information security classification

The information security classification domain includes all activities that ensure information is appropriately classified.

Queensland Government Mandatory Clauses

2.2.1 All information assets must be assigned appropriate security classification and control in accordance with the QGISCF.

2.2.2 Classification schemes do not limit the provision of relevant legislation under which the *[agency/department/entity]* operates.

Agency Clauses

2.2.3 [*Insert agency specific clauses*].

The level of security controls should be commensurate to the classification level, value and degree of reliance on the information and systems. Agencies should provide information about how the agency's information assets are classified, eg. Are they recorded in the agency's information asset register?

Further information on the requirements of information asset registers can be located in IS44. Further information on information security classification and control can be located in the QGISCF and the Queensland Government Network Transmission Security Assurance Framework (NTSAF).

3 Human resources management

3.1 Pre-employment

The pre-employment domain includes all pre-employment activities that ensure employees, contractors and third party users will not compromise information security arrangements. Activities also include information security roles and responsibility definition, screening and employment terms and conditions.

Queensland Government Mandatory Clauses

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

Agency Clauses

3.1.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Who is responsible for assessing the level of security and ensuring that it is addressed in job descriptions?*
- *Will there be specific security clauses in contracts where third parties are involved?*
- *What security verification checks (eg. criminal reference checks) will be made on job applicants, contractors, and consultants, especially those who deal with sensitive information?*
- *Who authorises this? Who is authorised to carry out these checks?*
- *Will confidentiality agreements be signed?*
- *Do terms and conditions of employment outline security responsibilities and disciplinary processes?*

3.2 During employment

The during employment domain includes all activities that ensure employees, contractors and third party users are aware of information security threats and concerns, their information security responsibilities and liabilities, are equipped to support organisational information security policy and reduce the risk of human error.

Queensland Government Mandatory Clauses

3.2.1 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.

3.2.2 Where employees have access to HIGHLY PROTECTED information or perform specific security related roles, these responsibilities must be fully documented with signed acknowledgement and communicated.

Agency Clauses

3.2.3 [*Insert agency specific clauses*].

Activities include information security awareness and training, disciplinary processes and setting of management responsibilities. Agencies should also consider the following:

- *What security responsibilities will be included in induction and ongoing staff training?*
- *How will security responsibilities be communicated to staff and when?*
- *What is the disciplinary process for security violations?*
- *How is it communicated to staff? Does the agency distribute copies to all employees?*
- *Who is authorised to deal with security violations?*

3.3 Post-employment

The post-employment domain includes all activities that seek to ensure that during changes or termination of employment, information security is not compromised.

Queensland Government Mandatory Clauses

3.3.1 Procedures for ensuring the security of the agency during the separation of employees from, or movement within the *[agency/department/entity]* must be developed and implemented.

Agency Clauses

3.3.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What are the security processes for the exit or movement of employees, contractors or other third parties from or within the agency (eg. exit interviews; revoking of access rights and disabling of all User-IDs); and at the time of leaving, ensure all keys, access devices, credit cards are collected from employees?*
- *Is the employee aware of their continuing responsibilities in relation to the protection of the confidentiality and privacy of information they may have had access to in their duties?*
- *Are employees aware of the legal implications of non-compliance? ie. the penalties involved?*
- *Are there procedures in place for employees who are terminated on an 'unfriendly' basis?*

4 Physical and environmental management

4.1 Building controls and secure areas

The building controls and secure areas domain includes all activities that ensure information security is not compromised by unauthorised physical access, damage or interference to premises or information.

Queensland Government Mandatory Clauses

4.1.1 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.

4.1.2 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.

4.1.3 Control policies (including clear desk/clear screen) must be implemented in information processing areas that deal with security classified information.

Agency Clauses

4.1.4 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What are the agency's control policies?*
- *What areas need physical entry and perimeter controls (eg. computer rooms, document storage)?*
- *How are all other areas (eg. offices, workstations, delivery facilities, third party access) to be secured?*
- *What type of access mechanisms should be used (eg. beyond just a locked door)?*

4.2 Equipment security

The equipment security domain includes all activities that ensure information security is not compromised by loss, damage, theft or other compromise of the organisation's physical equipment assets.

Queensland Government Mandatory Clauses

4.2.1 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.

4.2.2 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.

4.2.3 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.

Agency Clauses

4.2.4 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *If physical controls are not possible, agencies need to detail the control methods in place.*
- *How and where is critical equipment to be sited?*
- *What safeguards are to be in place?*
- *What safeguards are in place for power supplies to critical equipment?*
- *How is cabling to be protected?*
- *How is communications equipment to be housed?*
- *How and who is allowed to carry out maintenance on equipment?*
- *What is the policy on security of equipment kept off site (eg. home use equipment, portable equipment)?*
- *What is the process/who authorises the disposal and reuse of equipment?*
- *What is the policy for unattended workstations, unattended facsimiles, etc?*

5 Communications and operations management

5.1 Operational procedures and responsibilities

The operational procedures and responsibilities domain includes all activities that ensure the correct and secure operation of information processing facilities.

Queensland Government Mandatory Clauses

5.1.1 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).

5.1.2 Operational change control procedures must be implemented to ensure that changes to information processing facilities or systems are appropriately approved and managed.

Agency Clauses

5.1.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What processes must be documented and who is responsible?*
- *What is the policy with regard to separating the development/testing environment from the operational environment?*

For further information agencies should refer to the IS18 Implementation Guideline located in the IS18 toolbox.

5.2 Third party service delivery

The third party service delivery domain includes all activities that implement and maintain information security in line with service delivery agreements.

Queensland Government Mandatory Clauses

5.2.1 Third party service delivery agreements must comply fully with IS18.

5.2.2 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.

5.2.3 Third party service operating agreements must specifically address third party governance policies and processes (see section 1.4).

Agency Clauses

5.2.4 Third party service delivery agreements should require service providers to complete annual compliance audits against IS18.

5.2.5 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What processes must be documented and who is responsible?*
- *Is there a document style template that must be used?*
- *What is the policy for segregating duties that might involve a conflict of interest?*
- *What are the specific duties that must be segregated?*
- *Do separation agreements with the supplier consider information security arrangements (eg. at the end of a contract or breaking of a contract)?*

- *Have outsourcing/external hosting separation expectations and processes been documented?*
- *Will the agency be notified in the event of the supplier's insolvency? Can the agency terminate the contract?*
- *Have escrow agreements been established to ensure that rights to data, systems, codes will be transferred to the agency in the case of the supplier's collapse?*

5.3 Capacity planning and system acceptance

The capacity planning and system acceptance domain includes all activities that monitor resources and set criteria for system changes to reduce the risk of system failure.

Queensland Government Mandatory Clauses

5.3.1 System acceptance must include confirmation of the application of appropriate security controls and of the capacity requirements of the system.

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

Agency Clauses

5.3.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What processes are subject to authorised change control?*
- *Is there a process for implementing changes to information systems?*
- *Who is responsible for information systems capacity planning?*
- *What processes or systems need to be monitored for future planning?*
- *Who is responsible for the migration of new systems or upgrades into the operating environment?*

5.4 Application integrity

The application integrity domain includes all activities that protect the integrity of applications and their information from malicious code.

Queensland Government Mandatory Clauses

5.4.1 Adequate controls must be defined and implemented for the prevention, detection, removal and reporting of attacks by malicious code on all ICT assets.

5.4.2 Vulnerability/integrity scans of core software must be defined and conducted regularly to ensure detection of unauthorised changes.

5.4.3 Anti malicious-code software must be regularly updated with new definition files and scanning engines.

5.4.4 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.

Agency Clauses

5.4.5 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the agency method of insuring only authorised software is used?*
- *Are web applications secured against network attacks such as Structured Query Language (SQL) injections?*

- *What is the agency policy on the prohibited use and installation of software not authorised by the agency including user responsibilities with regards to downloading software from Internet and e-mail sources?*
- *What is the agency policy and method for virus and malicious code protection?*
- *Who is responsible for cleaning and reporting malicious code attacks?*
- *How will users be educated?*

5.5 Backup procedures

The backup procedures domain includes all activities that maintain the integrity and availability of information and applications through the use of backup activities.

Queensland Government Mandatory Clauses

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

Agency Clauses

5.5.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the policy on backup?*
- *What is the policy for logging system activities?*
- *What is the policy on systems maintenance?*
- *What are the authorisation processes?*

5.6 Network security

The network security domain includes all activities that ensure the security of information being passed over networks.

Queensland Government Mandatory Clauses

5.6.1 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.

5.6.2 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.

5.6.3 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.

5.6.4 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.

Agency Clauses

5.6.5 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Who is responsible for network management?*
- *What are the policies and processes for remote access?*
- *Who authorises external connections?*
- *All external perimeter access should be secured using defence-in-depth security systems, including firewall, intrusion detection and prevention systems.*

5.7 Media handling

The media handling domain includes all activities that protect media (both electronic and printed information) from unauthorised disclosure, modification, removal or destruction.

Queensland Government Mandatory Clauses

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

Agency Clauses

5.7.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the process for reusing media? eg. Hard drives, backup tapes.*
- *What is the process for transporting and storing media?*
- *What is the process and who authorises disposal of all types of information? eg. Paper documents, disks, and system documentation?*
- *What is the process for storage, handling and access to all types of information types? eg. How is media to be labelled, use of distribution lists, filing of emails, facsimiles?*

5.8 Information exchange

The information exchange domain includes all activities that maintain the security of information exchanged (internally or externally).

Queensland Government Mandatory Clauses

5.8.1 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.

5.8.2 The type and level of encryption must be authorised and compliant with the requirements of the QGISCF and the NTSAF.

5.8.3 All information exchanges over public networks, including all online or publicly available transactions/systems must be authorised either directly or through clear policy.

Agency Clauses

5.8.4 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What type of information can be sent over public networks (eg. facsimiles/email)?*
- *What checks are in place to check for transmission receipts?*
- *What is the policy in relation to information and communication devices including answering machines, electronic diaries?*

Further information is detailed in the QGISCF and IS38.

5.9 eCommerce

The eCommerce domain includes all activities that ensure the security of e-commerce services and their use.

Queensland Government Mandatory Clauses

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

Agency Clauses

5.9.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What checks are to be carried out prior to instituting e-commerce services?*
- *Who authorises 'online' or publicly available transactions/systems?*

Further information is detailed in the Queensland Government Authentication Framework (QGAF).

5.10 Information processing monitoring

The information process monitoring domain includes all activities that detect unauthorised information processing activities including the use of audit logging.

Queensland Government Mandatory Clauses

5.10.1 Comprehensive operator and audit/fault logs must be implemented.

5.10.2 All ICT assets must be synchronised to a trusted time source that is visible and common to all.

Agency Clauses

5.10.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What system events will be logged, eg. date, IP address, User IDs, unsuccessful logins, alerts from intrusion detection systems (firewall)?*
- *When and who will review and monitor system logs?*
- *Where are they stored?*
- *How long are logs kept for?*
- *Do logs contain confidential information? If so is this information adequately protected?*
- *Have procedures been developed for monitoring use of information processing facilities?*
- *Are these procedures reviewed regularly?*
- *How often should the result of monitoring activities be reviewed?*
- *Is log information and logging facilities protected against tampering and unauthorised access?*
- *Intrusion detection or prevention services should be implemented at critical or essential ingress, egress and end-points within an agency's network domain.*

6 Access management

6.1 Access control policy

The access control policy domain includes all activities that set access and control policies.

Queensland Government Mandatory Clauses

6.1.1 Control mechanisms based on business requirements and assessed/accepted risks for controlling access to all information assets and ICT assets must be established.

6.1.2 Access control rules must be consistent with agency business requirements, information classification, and legal/legislative obligations.

Agency Clauses

6.1.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Have policies been established for the configuration of remote access support applications and utilities?*
- *Who authorises access to systems and business applications? How is authorisation granted?*

Further information is detailed in the IS18 Implementation Guide located in the IS18 toolbox.

6.2 Authentication

The authentication domain includes all activities and measures that ensure users are the persons they claim to be.

Queensland Government Mandatory Clauses

6.2.1 Authentication requirements including on-line transactions and services must be assessed against QGAF.

6.2.2 All authentication of users external to the agency must be implemented in compliance with QGAF.

Agency Clauses

6.2.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Have appropriate authentication mechanisms been applied for users and equipment?*
- *Have appropriate authentication mechanisms been applied for remote users?*
- *Have appropriate authentication controls been implemented to control access to wireless networks?*
- *Do users have a unique identifier (user ID) for their personal use? Has a suitable authentication processes been chosen to substantiate the claimed identity of a user?*

Further information is detailed in QGAF.

6.3 User access

The user access domain includes all activities that ensure authorised access to information and applications.

Queensland Government Mandatory Clauses

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

Agency Clauses

6.3.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *How is access to information systems to be granted? eg. passwords.*
- *Who is responsible for monitoring and reviewing access rights?*
- *Who is responsible and what is the process for the removal and notification of, redundant User IDs and accounts?*
- *Who is responsible for granting access to systems utilities and privilege management?*
- *Are those with privileged access required to sign for access to a system before it's granted?*
- *How is access and use of systems utilities monitored?*

6.4 User responsibilities

The user responsibilities domain includes all activities that ensure users understand their responsibilities to prevent compromise of information or systems.

Queensland Government Mandatory Clauses

No mandatory clauses.

Agency Clauses

6.4.1 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What are users' responsibilities for access and passwords?*
- *Do users follow good security practices in the selection and use of passwords?*
- *Do users ensure that unattended equipment has appropriate protection (eg. computers are locked when left unattended)?*
- *Does the agency adopt clear desk/clear screen policies?*

6.5 Network access

The network access domain includes all activities that ensure network access is restricted to authorised users.

Queensland Government Mandatory Clauses

6.5.1 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

6.5.2 Authorisation must be obtained and documented for access (including new connections) to agency networks.

6.5.3 All wireless communications must have appropriate configured product security features and afford at least the equivalent level of security of wired communications.

6.5.4 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.

Agency Clauses

6.5.5 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Who is responsible for authorising network access (both internal and external connections)?*
- *What is the process for enforced network paths and user authentication for external connection, Node authentication, use of remote diagnostic ports?*
- *How will network domains and groups be segregated?*
- *What network connection controls will be in place? – eg. times, type and size of file transfers to external source.*
- *The number of external gateways allowed access to extranets, internal networks and other security zones should be minimised.*

6.6 Operating system access

The operating system access domain includes all activities that ensure access to operating systems is restricted to authorised users.

Queensland Government Mandatory Clauses

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

Agency Clauses

6.6.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *How is automatic terminal identification used to authenticate connections to specific locations and portable equipment?*
- *What is the secure logon and logoff process for access?*
- *Are there restrictions on connection times in place?*
- *How will passwords be issued and managed – what are the rules for passwords?*
- *How will systems utilities' use be controlled?*

6.7 Application and information access

The application and information access domain includes all activities that ensure access to information and applications are restricted to authorised users.

Queensland Government Mandatory Clauses

6.7.1 Restricted access and authorised use only warnings must be displayed upon access to all systems.

6.7.2 Access to all confidential/sensitive systems must only be allowed after authorised approval.

Agency Clauses

6.7.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Who authorises application access? eg. read, write*
- *Is a record kept of authorised user access to confidential/sensitive systems?*
- *Is this list reviewed and revalidated periodically?*
- *What is the process for authorising access to information when systems share resources? eg. two separate systems are integrated to form a third application or system.*

6.8 Mobile computing and telework access

The mobile computing and telework access domain includes all activities that ensure information security is maintained when using mobile computing and telework facilities.

Queensland Government Mandatory Clauses

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

Agency Clauses

6.8.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *the development of information security policies and procedures for devices (eg. laptop and notebook computers; palm tops; smart cards; mobile phones; portable storage devices)*
- *these policies and procedures should be based on the results of risk assessments and provide the policy and instructions for such issues as:*
  - *physical storage and protection of equipment, for example use in public places and transporting equipment*
  - *personal usage*
  - *protection of the information held on the device (eg backup's, virus protection)*
  - *access mechanisms (eg, password) for example authentication methods.*
- *policies and procedures should be clearly documented to authorise and control teleworking activities, and cover issues including:*
  - *physical security of the site*
  - *authorisation processes and system access*
  - *security of the telecommunications link*
  - *lack of control of information, for example, access by family, friends*
  - *increased risk of disclosure or unauthorised use of information*
  - *increased risk of unauthorised access to agency network and systems*
  - *support and maintenance of hardware and software updates*
  - *backup procedures*
  - *access security aspects (writing down of instructions for login including passwords).*
- *policy on connection of privately owned devices to agency networks. eg. authentication measures, access controls, virus and malicious codes and physical/personnel security.*

7 System acquisition, development and maintenance

7.1 System security requirements

The system security requirements domain includes all activities that ensure security requirements are articulated during the development of new systems, or when planning enhancements to existing systems.

Queensland Government Mandatory Clauses

7.1.1 Security controls must be commensurate with the security classifications of the information contained within, or passing across information systems, network infrastructures and applications.

7.1.2 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.

7.1.3 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.

7.1.4 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.

7.1.5 Accurate records must be maintained to show traceability from original business requirements to actual configuration and implementation, including appropriate justification and authorisation.

Agency Clauses

7.1.6 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What are the security controls that should be addressed in new systems or upgrades? eg. input data validation, internal processing, message authentication, output data validation?*

7.2 Correct processing

The correct processing domain includes all activities that prevent errors, loss, unauthorised modification or misuse of information in systems.

Queensland Government Mandatory Clauses

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

Agency Clauses

7.2.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Do access controls include the validation of input data, internal processing and output data?*
- *Are additional controls in place for sensitive, valuable or critical information?*

- *Has data input to applications been validated? Are validation checks incorporated into applications?*
- *Has data output from applications been validated?*

7.3 Cryptographic controls

The cryptographic controls domain includes all activities that protect the integrity, confidentiality and authenticity of information by using cryptographic controls.

Queensland Government Mandatory Clauses

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

Agency Clauses

7.3.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Has a cryptographic control policy been established and implemented?*
- *Has a risk assessment been used to determine whether a cryptographic control is appropriate?*
- *Are all cryptographic keys protected against modification, loss, disclosure and destruction?*
- *Is equipment used to generate, store and archive keys physically protected?*
- *Has activation and deactivation dates for cryptographic keys been defined?*

Further information is detailed in the NTSAF.

7.4 System files

The system files domain includes all activities that ensure system files are adequately protected.

Queensland Government Mandatory Clauses

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

Agency Clauses

7.4.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *How is access to system files granted?*
- *Who is responsible for monitoring and recording changes to systems?*
- *What is the policy on keeping previous versions of software?*
- *What checks are in place for assessing impact of new systems or changes on existing systems?*
- *Who is responsible for authorisation of new systems or other changes?*
- *Where will system test data originate? How will operational data be monitored & authorised?*
- *How will program source code be monitored and maintained?*

7.5 Secure development and support processes

The secure development and support processes domain includes all activities that ensure the ongoing security of applications.

Queensland Government Mandatory Clauses

7.5.1 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.

7.5.2 Audit logs are maintained in accordance with the Queensland Government Information Security Controls Standard (QGISCS).

Agency Clauses

7.5.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the change request process for systems?*
- *Who can authorise changes to systems (eg timing in relation to business activities)? Who carries these out?*
- *What is the process for upgrading software changes – who assesses changes and impacts on current systems, business activities and costs?*
- *What checks are in place for ensuring that outsourced software development addresses agency information security requirements?*
- *What is the process for testing and evaluating software?*

7.6 Technical vulnerability management

The technical vulnerability management domain includes all activities that reduce risks arising from the exploitation of technical vulnerabilities.

Queensland Government Mandatory Clauses

7.6.1 Processes to manage software vulnerability risk for all IT security infrastructures must be developed and implemented.

7.6.2 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.

Agency Clauses

7.6.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Does the agency have a current and complete inventory of assets?*
- *Is timely information obtained about technical vulnerabilities of information systems?*
- *Has the agency's exposure to technical vulnerabilities been evaluated?*
- *Are vulnerability monitoring, risk assessment, patching and asset tracking undertaken?*
- *Has a timeline been defined to react to notification of potential vulnerabilities?*
- *When vulnerabilities are identified, how are actions managed?*
- *Are risks associated with the action assessed?*
- *Are patches tested and evaluated before they are installed?*

8 Incident management

8.1 Event/weakness reporting

The event/weakness reporting domain includes all activities that ensure information security events and weaknesses are communicated to allow remedial action to be taken.

Queensland Government Mandatory Clauses

8.1.1 Establish and maintain an information security incident register and record all incidents.

8.1.2 All information security incidents must be reported and escalated (where applicable) through appropriate management channels and/or authorities.

8.1.3 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.

8.1.4 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.

Agency Clauses

8.1.5 [*Insert agency specific clauses*].

8.2 Incident procedures

The incident procedures domain includes all activities that ensure a consistent and effective approach is applied to the management of information security incidents.

Queensland Government Mandatory Clauses

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

Agency Clauses

8.2.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What is the process and policy for Agency security incident reporting?*
- *What type of security incidents must be reported? Weaknesses?*
- *How is the information to be collected?*
- *Who is the information to be reported to?*
- *Who is responsible for following up security incident reports?*
- *What are reportable software malfunctions?*
- *Who is responsible for following up and resolving malfunctions?*
- *What is the reporting structure for reporting these?*
- *How procedures be communicated to staff?*
- *What are the procedures to be carried out for each type of incident?*
- *What are the escalation processes for criminal information security violations?*

9 Business continuity management

9.1 Business continuity

The business continuity domain includes all activities that counteract interruptions to business activities and to protect critical business processes from the effect of interruptions or failures of ICT systems or disasters and to ensure their timely resumption.

Business continuity also includes business continuity risk assessment, developing and implementing plans to address continuity management, and testing and maintenance of business continuity plans.

Queensland Government Mandatory Clauses

9.1.1 Methods must be developed to reduce known risks to information and ICT assets including undertaking a business impact analysis.

9.1.2 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.

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

Agency Clauses

9.1.4 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Is there an understanding of the impact interruptions will have on the agency?*
- *Has appropriate insurance been purchased?*
- *Have all possible events been identified?*
- *Are all business continuity plans within the agency consistent?*

9.2 ICT disaster recovery

The ICT disaster recovery domain includes all activities related to ensuring the availability of ICT systems and services including the restoration of ICT systems and services following an event which disrupts their delivery or the continued operation of ICT systems and services despite the loss of operational ICT equipment.

ICT disaster recovery supports business continuity activities, but is distinct in focussing on the restoration of ICT services rather than on the restoration of business services themselves (which even if heavily dependent on ICT can often be maintained for short periods using manual systems).

Queensland Government Mandatory Clauses

9.2.1 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.

9.2.2 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.

9.2.3 ICT disaster recovery plans must have clearly defined maximum acceptable downtimes.

9.2.4 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.

9.2.5 Maximum acceptable downtimes for ICT services must also be defined in service and operational level agreements with external parties.

9.2.6 Copies of ICT disaster recovery plans must be stored in multiple locations including at least one location offsite.

Agency Clauses

9.2.7 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *What impact will a disaster have on the agency?*
- *Has the agency identified and prioritised critical ICT processes and systems?*
- *Have additional preventative and mitigating controls been identified?*
- *Have all possible events been identified?*
- *Has the probability of a disaster occurring been calculated (eg. time, damage scale and recovery period)?*

10 Compliance management

10.1 Legal requirements

The legal requirements domain includes all information security activities relating to compliance with legal requirements.

Queensland Government Mandatory Clause

10.1.1 All legislative obligations relating to information security must be complied with and managed appropriately.

10.1.2 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.

10.1.3 Processes to ensure legislative compliance across all agency activities must be developed and implemented.

Agency Clauses

10.1.4 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Are information security controls compatible with all legal and legislative needs?*
- *Are approaches to right to information and information privacy clearly stated?*

10.2 Policy requirements

The policy requirements domain includes all information security compliance activities relating to information security policies and standards.

Queensland Government Mandatory Clauses

10.2.1 All reporting obligations relating to information security must be complied with and managed appropriately.

10.2.2 The Information security compliance checklist must be submitted annually to the ICT Policy and Coordination Office in line with the IS18 reporting requirements.

Agency Clauses

10.2.3 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Is the security of information systems regularly reviewed?*
- *Are these reviews performed against the agencies security policies?*
- *Are all security processes and procedures carried out correctively? Is this regularly reviewed?*
- *Are results of reviews recorded, maintained and reported?*
- *Are independent reviews carried out? What action is taken for non-compliance?*

10.3 Audit requirements

The audit requirements domain includes all audit activities relating to information security activities.

Queensland Government Mandatory Clause

10.3.1 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.

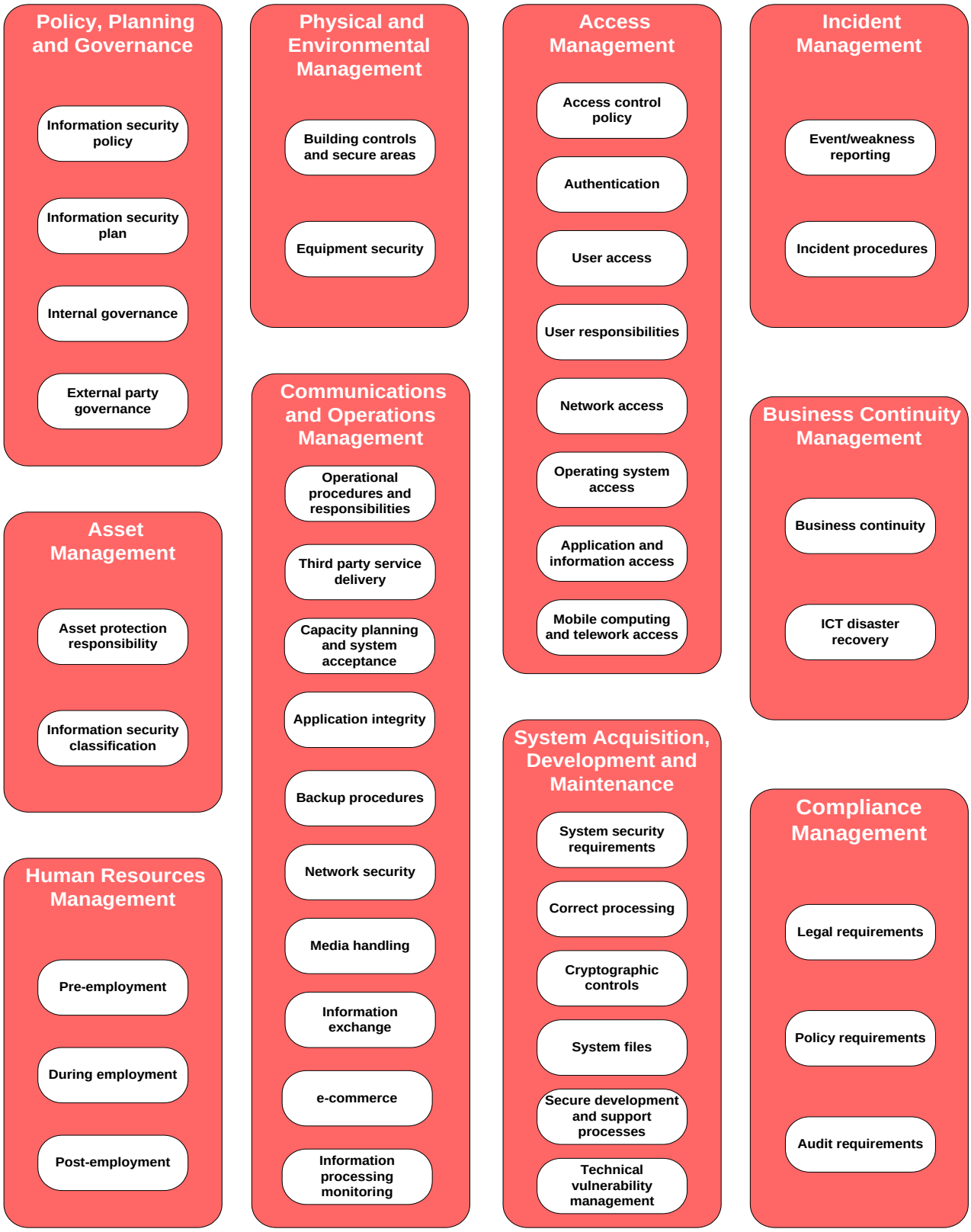
Agency Clauses

10.3.2 [*Insert agency specific clauses*].

Agencies should also consider the following:

- *Are controls established to safeguard operational systems and audit tools during audits?*
- *Are controls established to safeguard the integrity and prevent misuse of audit tools?*
- *Are audits planned to minimise the risk of disruptions to business processes?*

Appendix A Information security policy framework



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

Appendix B Information security policy structure