INFORMATION & COMMUNICATION TECHNOLOGY SECURITY POLICY

Head of Power
Local Government Act 2009

Objective
To provide a governing framework for the security and management of electronic information within Council.

Definitions/Application
Application
This Policy governs access to and use of the Council's electronic information and any information and communication technology (ICT) assets which create, process, store, view or transmit information.

Policy Statement
Moreton Bay Regional Council is responsible for a significant amount of information held in electronic formats, and it is critical that this information be protected appropriately.

This policy seeks a consistent approach to the implementation of information security to protect information assets and any ICT assets which create, process, store, view or transmit information against unauthorised use or accidental modification, loss or release.

Council will adhere to the following ten ICT Security Principals (based on the Queensland Government Information Standard 18 (IS18)):

ICT SECURITY PRINCIPLES

Principle 1 - Policy, planning and governance
Council management will recognise the importance of, and demonstrate a commitment to maintaining a robust Council information security environment. At a minimum, Council will:

- develop an Information Security Policy Implementation Plan, ensuring alignment with Council business planning, general security plan and risk assessment findings.
- establish and document information security internal governance arrangements (including roles and responsibilities) to implement, maintain and control operational information security within the Council.
- establish and document information security external governance arrangements to ensure that third party service level agreements and operational level agreements clearly articulate the level of security required and are regularly monitored.

Principle 2 - Asset management
Council will implement procedures for the classification and protective control of information assets. As a minimum, Council will ensure:

- all information assets are assigned appropriate classification and control in accordance with the Queensland Government Information Security Classification Framework (QGISCF)
- all ICT assets that create, store, process or transmit security classified information are assigned ICT asset custodians and are also assigned appropriate controls in accordance with the QGICSF.
Principle 3 - Human Resources management
Council will minimise the risk of loss or misuse of information assets by ensuring that security controls are incorporated into Council human resource management, including the development of supporting policies and processes. At a minimum, Council will:

- implement induction and ongoing training and security awareness programs, to ensure that all employees are aware of and acknowledge the Council’s ICT Security Policy, their security responsibilities and associated security processes
- document and assign 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 Council.

Principle 4 - Physical and environmental management
The level of physical controls implemented will 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, Council will ensure that:

- they meet the requirements of the QGISCF.
- policies and processes are implemented to monitor and protect the use and/or maintenance of information assets and ICT assets away from premises.
- policies and processes are implemented for the secure disposal or reuse of ICT assets which are commensurate with the information asset’s security classification level.

Principle 5 - Communications and operations management
Operational procedures and controls will be documented and implemented to ensure that all information assets and ICT assets are managed securely and consistently, in accordance with the level of required security. Council will at a minimum ensure:

- the Network Transmission Security Assurance Framework (NTSAF) is used to ensure the security of data during transportation over communication networks.
- a network security guideline is developed and documented in line with the NTSAF to guide network administrators in achieving the appropriate level of network security.
- adequate controls are defined and implemented for the prevention, detection, removal and reporting of attacks of malicious code on all ICT assets.
- comprehensive systems maintenance processes and procedures including operator and audit/ fault logs, information backup procedures and archiving must be implemented.
- 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 within Council and with third parties are compliant with legislative requirements and consistent with the QGISCF.
- processes are developed and implemented to periodically review and test firewall rules and associated network architectures to ensure the expected level of network perimeter security is maintained.
**Principle 6 - Access management**

Control mechanisms based on business requirements, assessed/accepted risks, information classification and legislative obligations will be in place for controlling access to all information assets and ICT assets. At a minimum, Council will ensure that:

- authentication requirements, including on-line transactions and services, are assessed against the Queensland Government Authentication Framework (QGAF).
- policies and/or procedures for user registration, authentication management, access rights and privileges are defined, documented and implemented for all ICT assets.
- 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.

**Principle 7 - System acquisition, development and maintenance**

During system acquisition, development and maintenance, security controls will be established and will be commensurate with the security classifications of the information contained within, or passing across, information systems, network infrastructure and applications. Council will at a minimum ensure:

- security requirements are addressed in the specifications, analysis and/or design phases and internal and/or external audit are consulted when implementing new or significant changes to financial or critical business information systems.
- processes (including data validity checks, audit trails and activity logging) are established in applications to ensure development and support processes do not compromise the security of applications, systems or infrastructure.
- authentication processes are consistent with the QGAF.
- processes are developed and implemented to manage software vulnerability risk for all IT security infrastructures.

**Principle 8 - Incident management**

Effective management and response to information security incidents is critical to maintaining secure operations. Council at a minimum will:

- ensure information security incident management procedures are established to ensure appropriate responses in the event of information security incidents, breaches or system failures.
- ensure all information security incidents are reported and escalated (where applicable) through appropriate management channels and/or authorities.
- establish and maintain an information security incident and response register and record all incidents.
- ensure that information security incidents caused by employees are investigated and where it is found that a deliberate information security violation or breach has occurred, that formal disciplinary processes are applied.

**Principle 9 - Business continuity management**

A managed process including documented plans will be in place to enable information and ICT assets to be restored or recovered in the event of a disaster or major security failure. At a minimum, Council will:

- establish an information and ICT asset disaster recovery register to assess and classify systems to determine their criticality.
- establish plans and processes to assess the risk and impact of the loss of information and ICT assets on Council business in the event of a disaster or security failure.
- develop methods for reducing known risks to Council information and ICT assets.
• ensure business continuity and information and ICT asset disaster recovery plans are maintained and tested to ensure systems and information are available and consistent with Council business and service level requirements.

Principle 10 - Compliance management
Council will ensure compliance with, and appropriate management of, all legislative and reporting obligations relating to information security. Council at a minimum will:

- ensure that all reasonable steps are taken to monitor, review and audit Council information security compliance.
- all Council information security policies, processes and requirements including contracts with third parties, are reviewed for legislative compliance on a regular basis and the review results reported to appropriate Council management.

Review Triggers

This Policy is reviewed internally for applicability, continuing effect and consistency with related documents and other legislative provisions when any of the following occurs:

1. The related documents are amended.
2. The related documents are replaced by new documents.
3. Amendments which affect the allowable scope and effect of a Policy of this nature are made to the head of power.
4. Other circumstances as determined from time to time by a resolution of Council.

Notwithstanding the above, this Policy is to be reviewed at least once every two years for relevance and to ensure that its effectiveness is maintained.

Responsibility

This Policy is to be:

1. implemented by all officers and Councillors; and
2. reviewed and amended in accordance with the "Review Triggers" by the Manager Information and Communication Technology.

Version Control

Council Resolution number: 13/1534 Date: 27 August 2013

Related Links:
ICT Security Policy Reference Guidelines