Information Security Policy (IS18)

Corporate Services
CORP_33

COUNCIL POLICY			
Date Adopted by Council	23 March 2022	**Council Resolution**	2022/03/23.3
Effective Date	23 March 2022	**Next Review Date**	23 March 2025
Responsible Officer(s)	Manager Innovation and Technology	**Revokes**	AP_CORP_02

Purpose

The purpose of this policy is to describe the Whitsunday Regional Councils approach to protecting its information assets and to inform those impacted by the policy of their respective obligations and responsibilities.

The Whitsunday Regional Council recognises the requirement to provide guidance, governance, and operational artefacts in relation to information security including.

- Development, maintenance and implementation of an Information Security Policy, Information Security Management System (ISMS), and ICT Facilities User Policy that is appropriate relative to Council's functions and the risks that it faces.
- The identification of Council's information assets and their custodians.
- The identification and management of risks associated with information assets relative to infrastructure, platforms, data, and applications while information is in storage, in transit and in use.
- Regular independent audit of information security controls and measures to determine their effectiveness and to identify opportunities for improvement.
- Establishing and maintaining information resources, including IT systems, to be appropriately protected from compromise and misuse (both intentional and otherwise).
- Establishing and maintaining suitable Information Security training tools to ensure Council employees understand their role in protecting information assets; and
- Remaining accountable for the secure performance of outsourced services and functions.

The Whitsunday Regional Council recognises that information is a valuable strategic asset that supports the achievement of the Councils mission. The value derived for information assets is dependent upon the achievement of three objectives:

1. Observing the appropriate confidentiality obligations associated with each kind of information asset.
2. Maintaining the integrity of the information asset used by the Council; and
3. Enabling the availability of the information assets in the formats required at the times needed.

Information and Communication Technologies (ICT) are critical components in achieving the above objectives for all information assets owned or managed by Council.

Scope

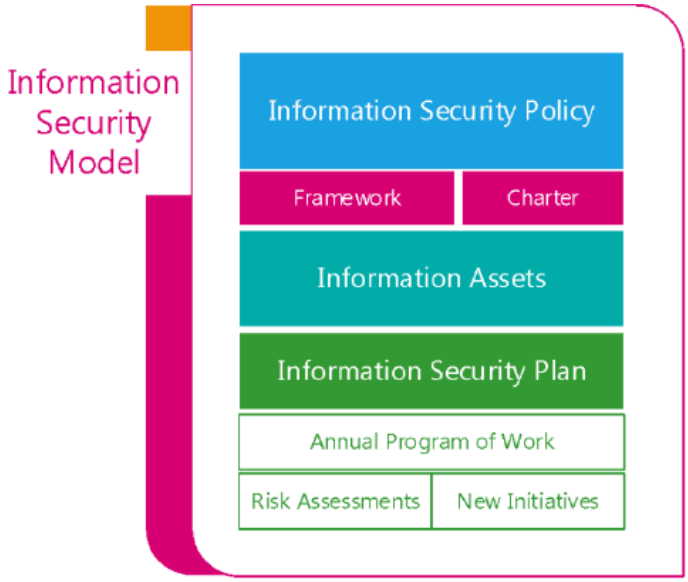
This policy is applicable to all council employees, contractors, volunteers, temporary, casual workers, councillors, controlled entities and associated third parties who have reason to access any of Councils information assets owned or controlled by Whitsunday Regional Council.

Information Security Policy (IS18)

Corporate Services
CORP_33

This policy governs access to and use of Council's information assets and any information and communication technology assets which create, process, store, view or transmit information.

This policy is part of an integrated model of information security artefacts used by the Whitsundays Regional Council.



Applicable Legislation

Information Security Standards AS/NZS ISO/IEC 27001:2013

Information Security Standards AS/NZS ISO/IEC27002:2013

Queensland Government Information Standards IS18:2018

Queensland Government Information MGNT Policy Framework v2.0 (2017)

Information Privacy Act 2009

Queensland Financial and Performance Management Standard

Controlled Objectives for Information Technology (COBIL) 5

Queensland Public Records Act 2002

Commonwealth Privacy Act 1998

Policy Statement

The Whitsundays Regional Council is committed to provide a secure information environment for residents, visitors, and employees.

Confidentiality, integrity, and availability of Councils information assets are required for Council to maintain both its services and its legal obligations.

This policy is written to be consistent with the Information Security Standards AS/NZS ISO/IEC 27001:2013, AS/NZS ISO/IEC27002:2013, and the Commonwealth Privacy Act (1988) requirements relating to the protection and secure disposal of personal information.

Furthermore, Councils entire information security model is developed in reference to the Queensland Government Information Security Framework and association Information Standard on Information Security (IS18:2018).

1. Information Security Management Framework

Council will maintain a formal Information Security Management System (ISMS) that includes, but is not limited to, the following elements:

- A formal Information Security Governance Framework.
- A risk-based approach to digital informs asset protection.
- The defined approach for the documentation and ongoing maintenance of information assets and IT system assets, owners, risks, and controls.
- Identification of applicable legislation and organisational compliance strategies.
- Security audit approach.
- Establishment of metrics to formally measure policy compliance and ISMS effectiveness.

The Manager Innovation and Technology is responsible for:

- Day-to-day management of the Councils information security management programs, including all information security audits and reviews.
- Forming necessary working groups and/or reference groups that are representative of the Council to review and, where appropriate, approve policies, procedures, and standards.
- Communicating policy responsibilities to all Council stakeholders and advising on compliance; and
- Authoring and maintaining the additional information security artefacts that support the achievement of the Councils information security objectives.
- Assessing the effectiveness of the Councils information security management program; and
- Reporting on the effectiveness of the Council information security management to the Director Corporate Services and to the relevant IT governance Committee.

The Director Corporate Services is responsible for reporting on the effectiveness of the Councils information security management to the Senior Executive and the Council.

2. Information Asset Classification

Council will maintain a formal Information Classification Framework that includes, but is not limited to, the following elements:

- A series of classification categories that reflect the sensitivity and criticality of the information or IT system asset in question.
- Guidelines for the effective selection and usage of classification categories; and
- The identification of nominated owners for all information and system assets.

The Information Owners are responsible for:

- Assigning a security classification to their respective assets, to reflect the sensitivity and criticality of the information or IT system asset in question; and
- Ensuring asset description and classification are formally documented and maintained.

- The Manager Innovation and Technology is responsible for:
- Authoring and maintaining the Information Classification Framework.
- Day-to-day management of the Councils Information Classification Framework.
- Assessing the effectiveness of the Councils Information Classification Framework.
- Reporting on the effectiveness of the Council Information Classification Framework to the Director Corporate Services and to the relevant IT governance Committee.

The Director Corporate Services is responsible for reporting on the effectiveness of the Councils Information Classification Framework to the Senior Executive and the Council.

3. Access to Information Assets

Access to information assets must be restricted to authorised users and mechanisms must be in place to prevent unauthorised access.

All individuals requiring access or a change in access to Councils IT resources must submit a written request via the New User Form approval by the Manager. The user's identity will be recorded in Councils Active Directory as a user account and in relevant business systems as a user with appropriate permissions to enable control and auditing of access and usage. This excludes guests and visitors that only have limited access to wireless, community-based technologies, audio visual or telephony resources.

Active Directory and the Human Resources system are the two sources of truth for staff and user information.

When creating user accounts on Active Directory, the following principles are to be applied:

- All identities must be assigned a unique name in Active Directory and have a unique number recorded against the account based on the employee identifier generated by the Human Resources system.
- Staff identities in Active Directory are to be made up of the staff members First Name and Surname separated by a full stop (.). Where duplicate names exist, the second and subsequent names will also contain the staff members middle initial also separated by a full stop (.).
- Guest/visitor identities in Active Directory and associated applications are only to be active for the minimum time required for the guest/visitor to achieve their objective using a Council Support Account.
- Guest access is provided based on approved support access requests to ICT for the agreed period and only to the required system/device.
- Guest access passwords generated for this access are one-time use only.
- All accounts created in Active Directory will require the end user to authenticate to access the network. Where possible, when authenticating to Councils network from within Council buildings, single factor authentication only will be required (password). When authenticating from outside of Councils physical buildings, two factor authentications (password plus another factor) will be established as the standard.
- Access privileges assigned to users will be designed on a least-privilege basis relative to requirement.
- All generated system passwords must adhere to standards outlined in the ICT Facilities User Policy.

- All server access requires two factor authentication from within and outside the network.

Whitsunday Regional Council reserves the right to grant, limit or withdraw access to some or all its IT resources either temporarily or permanently at any time.

In addition to Councils corporate network, Council also operates secondary networks to allow guest and community wireless access. These networks will operate in isolation to Councils corporate network and not require identity or authentication processes.

The Information Owners are responsible for reviewing user accounts and access privileges on an annual basis to confirm that application users are still authorised for access appropriately.

The Manager Innovation and Technology is responsible for:

- Reviewing and approving requests for access.
- Reviewing user accounts and access privileges on an annual basis to confirm that network users are still authorised for access appropriately.
- Maintaining audit logs of application access details.
- Day-to-day management of the Councils information access tools.
- Assessing the effectiveness of the Councils information access tools.
- Reporting any information access breaches (attempted or succeeded) to the Director Corporate Services and to the relevant IT governance Committee; and
- Reporting on the effectiveness of the Council information access tools to the Director Corporate Services and to the relevant IT governance Committee.

The Director Corporate Services is responsible for reporting on the effectiveness of the Councils information access tools and any information access breaches (attempted or succeeded) to the Senior Executive and the Council.

4. Network and Communications

The Council's IT network infrastructure must be configured and maintained to protect information assets according to the following requirements:

- Incoming internet traffic must access only approved IT resources and services.
- All internet traffic must enter and exit Council's network either via Firewall security or via a Demilitarized Zone.
- Network traffic will be monitored for signs of malicious activity.
- All Council owned IT assets connected to the Council network will maintain a basic level of security as recommended by the Manager Innovation and Technology. This must include:
    - Anti-virus software that is up to date and actively running; and
    - Appropriate and available operating system security updates are installed.

The Manager Innovation and Technology is responsible for:

- Day-to-day management of the Councils network security tools.
- Assessing the effectiveness of the Councils network security tools.
- Reporting any network security breaches (attempted or succeeded) to the Director Corporate Services and to the relevant IT governance Committee; and

- Reporting on the effectiveness of the Council network security tools to the Director Corporate Services and to the relevant IT governance Committee.

The Director Corporate Services is responsible for reporting on the effectiveness of the Councils network security tools and any network access breaches (attempted or succeeded) to the Senior Executive and the Council.

5. Mobile Computing

Council owned mobile computing devices must be protected from physical theft and/or damage and configured in such a way that prevents unauthorised access to the data stored on device.

Mobile computing devices in the context of this policy refers to devices such as:

- Notebook and laptop computer equipment.
- Tablet and mobile devices; and
- IoT or data collection devices.

Mobile device users must ensure that mobile computing devices are never left unattended in a public place or unattended and visible in a vehicle. Furthermore, all mobile devices must be physically secured when not in the user's possession.

All mobile computing devices must:

- Require password/passcode for device access.
- Utilise, where possible, up-to-date anti-malware software; and
- Where supported, allow remote erase functionality.

In the event of a lost or stolen device, a security breach or unacceptable usage (as per the IT Facilities User Policy) being detected, Council may remotely wipe the mobile device, returning it to factory setting.

The Council will take no responsibility for the loss of any personal information stored or downloaded onto a Council owned mobile device (data, photos, music, apps etc.) in the event of damage or loss.

Mobile device users must:

- Abide by Councils IT Acceptable Use Policy.
- Not rely on mobile computing devices as the sole repository for their data.
- Ensure data stored primarily on mobile devices is backed up to the Council's network storage systems.
- Not alter the configuration or Councils mobile computing devices, including the mobile phone carrier arrangements, without written approval from the Manager Innovation and Technology; and
- Immediately report any lost or stolen mobile computing devices to their supervisor and the Manager Innovation and Technology.

The Manager Innovation and Technology is responsible for:

- Day-to-day management of the Councils mobile computing management tools.
- Assessing the effectiveness of the Councils mobile computing management tools.
- Reporting any mobile computing breaches (attempted or succeeded) to the Director Corporate Services and to the relevant IT governance Committee; and

- Reporting on the effectiveness of the Council mobile computing management to the Director Corporate Services and to the relevant IT governance Committee.

The Director Corporate Services is responsible for reporting on the effectiveness of the Councils mobile computing management tools and any mobile computing access breaches (attempted or succeeded) to the Senior Executive and the Council.

6. Physical and Environmental

Physical security and environmental controls protecting Council's information assets will meet the following requirements:

- Physical information assets deemed critical to the Council must be housed in an approved location with sufficient access controls, barriers, and perimeter defences.
- All users with physical access to locations housing critical information assets must be documented, monitored, and recorded.
- Sufficient environmental controls must be implemented including power backup and air-conditioning to protect critical information assets from damage and to ensure its reliable operation; and
- Access to IT facilities must be restricted to authorised users only.

The Manager Innovation and Technology is responsible for:

- Day-to-day management of the Councils information asset physical security approvals.
- Reporting any information assets physical security breaches (attempted or succeeded) to the Director Corporate Services and to the relevant IT governance Committee; and
- Reporting on the effectiveness of the Council information assets physical security management to the Director Corporate Services and to the relevant IT governance Committee.

The Director Corporate Services is responsible for reporting on the effectiveness of the Councils information assets physical security management and any information assets physical security access breaches (attempted or succeeded) to the Senior Executive and the Council.

7. Disaster Recovery

Council will aim to ensure critical information assets are recoverable in the event of a disaster.

The Council must develop and maintain a Disaster Recovery Framework that enables:

- Risk reduction in the event of a disaster or serious incident.
- Availability of information assets required to support critical Council processes to agreed levels.
- Compliance with regulatory requirements; and
- Integrated with Councils Business Continuity policies and processes.

The Council will develop and maintain a disaster recovery plan that is:

- In alignment with the organisations.
    - Disaster Recovery Framework.
    - Business Continuity Plan.
    - Risk Management Framework; and
    - Emergency Management Plan.

- Periodically tested (at a minimum on an annual basis).
- Communicated to all relevant stakeholders; and
- Aligned to business/operational needs.

The Manager Innovation and Technology is responsible for:

- Overseeing the development and maintenance of the IT Disaster Recovery Framework and Plan.
- Ensuring that the IT Disaster Recovery controls are adequate and tested.
- Assessing the effectiveness of the Councils IT Disaster Recovery Framework and Plan; and
- Reporting on the effectiveness of the Council IT Disaster Recovery Framework and Plan to the Director Corporate Services and to the relevant ICT Governance Committee.

The Director Corporate Services is responsible for reporting on the effectiveness of the Councils IT Disaster Recovery Framework and Plan to the Senior Executive and the Council.

Definitions

CEO refers to the Chief Executive Officer of the Whitsunday Regional Council appointed in accordance with the Local Government Act 2009.

Council refers to the Whitsunday Regional Council.

Councillor – refers to an elected member of Council.

Employee refers to all council employees, contractors, volunteers, temporary, and casual workers.

ICT refers to Information Communication and Technology functions.

IT refers to the Innovation and Technology Branch of Whitsunday Regional Council. It can also be used interchangeably with Information Technology.

Related Documents

ICT Disaster Recovery Framework and Plan

Network Access Request Form

IT Acceptable Use Policy

Australian Government Information Security Manual (ISM) - https://www.cyber.gov.au/acsc/view-all-content/ism

Self-Assessment Tool - https://www.qgcio.qld.gov.au/reporting-app/pages/assessment-tools

Human Rights Compatibility Statement

This Policy has been assessed as compatible with the Human Rights protected under the *Human Rights Act 2019.*