Mackay
REGIONAL COUNCIL

ADMINISTRATIVE POLICY

Acceptable Usage of Council Information, Communication and Technology (ICT) Systems

POLICY NO	008
DEPARTMENT	Organisational Services
PROGRAM	Shared Services Centre – Information Services
APPROVED BY CEO	

1. Scope

This Policy applies to anyone who accesses Council's ICT Systems (**"Users**"), including:

- Council employees;
- Contractors, consultants, labour hire workers;
- Volunteers;
- Students on work experience;
- All employees and volunteers who undertake work or provide services at the Mackay Entertainment and Convention Centre (MECC), Artspace, Botanical Gardens, Sarina Sugar Shed and Greenmount Homestead; and
- Councillors.

Compliance with this Policy is a condition of being granted access to Council's ICT Systems.

2. Purpose

2.1 To ensure any asset that stores or accesses Council information including but not limited to computer systems, PCs, mobile devices and telephones is secure.

2.2 To minimise the impact of incidents on the Council's image, reputation, business operations and profitability.

2.3 To ensure compliance with regulatory requirements

2.4 To protect information so as to minimise the risk of financial and other loss to the Council.

2.5 To establish the accountability for employee actions in regards to protecting, disclosing, accessing, destroying and modifying Council information.

2.6 To support the strategic endeavours of Council by being safe, secure and reliable.

3. Policy statement

The use of Council's ICT Systems is a privilege provided to Users to enable them to effectively and efficiently undertake the duties associated with their employment or engagement. This includes:

- To conduct official Council business.
- To conduct business-related research.
- To investigate and access information on suppliers' (or potential suppliers) products.
- To provide support for products, services and systems being used by or provided by Council.
- To collaborate and communicate with business colleagues and clients.
- For approved staff professional development.

All material used, retrieved, created or sent using Council's ICT Systems remains the property of Council, including any personal email. Council retains the right to access any material at any time that is stored on Council's ICT Systems.

If a User is uncertain about their obligations under this Policy, they should speak to their manager or supervisor.

Use of Council's ICT Systems in a way that is a breach of this Policy may lead to disciplinary action, including but not limited to termination of employment/ engagement.

4. Definitions

To assist in interpretation the following definitions shall apply:

Council shall mean Mackay Regional Council.

Council's ICT Systems shall mean any and all systems forming part of the Mackay Regional Council Information, Communications and Technology (ICT) environment and includes, but is not limited to, Council’s Local Area Networks (LANs), Multi-Function Devices (MFDs), Printers, Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), Intranet, website, internet, email, computer systems, Corporate and vendor software, servers, cloud-based software and infrastructure services, networking equipment, remote access, personal computers (PCs), notebook computers, tablet computers, smart phones, other mobile phones, communications equipment, digital cameras, hand held devices (e.g. iPads or other mobile devices), USB memory sticks and other removal storage devices (e.g. external hard drives).

Incidental Personal Use means a use that is not a Council business purpose which:

- Takes place before or after working hours, during breaks or occasionally during working hours; and

- Is not excessive and does not interfere with the ability of a User to perform his/her duties or complete work for Council.

Social Media includes but is not limited to:

- Social networking sites, such as Facebook, Myspace, Bebo, Friendster, Tinder, Twitter, LinkedIn, and any other social networking sites as they develop in the future;
- Video, picture and photo sharing sites, including Flickr, Instagram, Pinterest and YouTube, and any other video, picture or photo sharing sites as they develop in the future;
- Blog sites, including professional and personal blogs;
- Online forums, text based chat room and interactive sites, including Google Groups;
- Online encyclopaedias, such as Wikipedia or Wikispaces;
- Virtual worlds and mash-ups, including Second Life and other sites that allow Users to create a physical identity and socialise with other users; and

- Other websites on the internet that enable comments to be posted on-line either publicly or via email.

This definition of Social Media is not exhaustive and Council may deem a particular medium or platform to constitute Social Media from time to time.

Systems Administrator shall mean any staff member with systems administration rights to Council's ICT Systems.

5. Areas of responsibility

5.1 The policy owner is responsible for overseeing the implementation, adherence to and review of this policy.

5.2 System and information owners are responsible for managing the risk associated with relevant systems and information and ensuring compliance with policies, standards, procedures and guidelines. They are also responsible for reporting non compliances and associated actions to the CIO.

5.3 All Council permanent and temporary employees, contracted staff, consultants and other workers are responsible for ensuring personal compliance with this policy and related standards and procedures.

6. Exemptions

6.1 The policy owner is responsible for approving and monitoring all exemptions to the policy.

6.2 Exemptions to this policy must be expressly authorised in writing by the CIO who will ensure that the channel, system or information owner understands, acknowledges and accepts the risk associated with the exemption – and will notify the Executive Risk Manager

7. Breaches of this Policy

Maintaining the security and integrity of Council's ICT Systems is the responsibility of all Users.

All Users should report unacceptable use of Council's ICT Systems to their immediate manager or supervisor or an appropriate Council officer.

7.1 <u>Notification of Security Breaches and Incidents</u>

Users must advise Information Services staff of any suspected breaches of security or threats to Council's ICT Systems. For example, Users should advise Information Services staff immediately if it is suspected that:

- a virus may be on a computer;

- an unauthorised person has gained access to the network, information systems or a computer;
- a User has been given unnecessarily high access permissions; or
- a User has access to systems that they should not have access to.

7.2 Non-Compliance

Without limitation, a breach of this Policy by a User may form grounds for:

- disciplinary action, including dismissal - this will depend on the circumstances and could include a warning (verbal/written), counselling, demotion, dismissal or a deduction from salary or wages (Users are referred to Council's Disciplinary Procedure Policy – POL-64.009); and/or

- termination of the contract of engagement for a contractor or consultant; and/or

- a requirement to make payment to Council of compensation or damages arising as a result of the breach.

In some circumstances, Council may disclose information about unacceptable use of Council's ICT Systems to law enforcement agencies and/or other statutory authorities.

8. The Policy

8.1 This Security Policy and access to the Security Standards must be available to, understood, formally accepted and adhered to by all Council staff.

8.2 All Council staff have a responsibility to protect Council and to minimise the risk that might result from inappropriate use of such information.

8.3 Security standards and procedures must be developed and reviewed annually to ensure they continue to support the objectives of this policy.

8.4 All information technology and physical assets must be secured in accordance with the relevant information security standards and procedures.

8.5 Council assets are to be made available to authorised people only, according to least privilege, and must only be used in accordance with the relevant security standards and procedures. Access must be approved by managers.

8.6 All Council information rated confidential or internal use only must be protected against intentional or unintentional access or disclosure.

8.7 All Council information and systems must be protected and maintained to ensure that integrity is assured.

8.8 All Council information and systems must be protected and maintained to ensure that availability is assured.

8.9 All access to Council information and systems must be auditable to ensure accountability and non repudiation of actions.

8.10 Defence in depth must be applied to the design, development and deployment of all Council systems to ensure a balanced security approach.

8.11 The design, development, deployment, and maintenance of systems must be done in consultation with the CIO and in accordance with the security standards and procedures.

8.12 All Council systems and services must comply with relevant national and international standards identified by the Executive Risk Owner in consultation with the CIO.

8.13 Security incident management response procedures must be implemented.

8.14 Information security risks and exemptions must be included in the risk management framework and reviewed at least annually.

8.15 Management will carry out an annual review of the policy to ensure ongoing compliance with legal and industry requirements.

9. Amendments

9.1 All amendments to this policy must be approved by the CEO

10. Review of Policy

This Policy will be reviewed when any of the following occur:

10.1 Related policies or documents of Council are amended or replaced.

10.2 Other circumstances as determined from time to time by a resolution of Council.

Notwithstanding the above, this Policy is to be reviewed at intervals of one (1) year, subject to Council's discretion and operational requirements.

Version	Reason / Trigger	Change	Endorsed / Reviewed	Date
1.0	Review of Policy	Amendments to Policy	SLPT/CEO	