TASMAN COUNCIL

CYBER SERCURITY POLICY

Policy Number	C 024
Responsible Officer	General Manager
Approval Date	March 2024
Policy to be Reviewed	March 2028

Aim

Tasman Council's Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise Council and our local community.

Practically, we rely on Council's information and communication technology (ICT) systems every day to conduct business efficiently, share business information legitimately between Council staff and others, and to store Council's corporate knowledge, history and records.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Governance Obligations

- Legal compliance
- Risk management

Definitions

Data Breach	An event that causes personal information held by an organisation or agency to be lost or subjected to unauthorised access or disclosure. Examples include: • A device with a customer's personal information is lost or stolen; • A database with personal information is hacked; • Personal information is mistakenly given to the wrong person.
Notifiable Data Breach	An event under the Notifiable Data Breach (NDB) Scheme that occurs in any organisation covered by the *Privacy Act 1988,* and which requires individuals and the Office of the Australian Information Commissioner (OAIC) to be notified when the event is likely to result in serious harm to an individual whose personal information is involved.
Other Persons at the Workplace	A person, other than a Councillor, who carries out work in any capacity for Council, including work as: a) A contractor or subcontractor; b) An employee of a contractor or subcontractor; c) An employee of a labour hire company who has been assigned to work at Council; d) An apprentice or trainee; e) A student gaining wok experience; or f) A volunteer.

Scope

The policy applies to Councillors, employees and other persons at the workplace who have permanent or temporary access to our systems and hardware. It includes people who are authorised to have remote access to Council's systems.

This policy refers to all those covered in the scope of this policy as "authorised users".

Policy

Authorised Access

Access to Council's electronic systems is available only to people with legitimate business needs and who are authorised by Council's General Manager or delegate.

Council's IT provider will only arrange or amend access for people when a request is received from a properly authorised Council delegate. If there is any doubt about the authenticity of a request, Council's IT provider will confirm the request is legitimate before proceeding.

Confidential Data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information, transactions or records;
- Data about customers/councillors/employees;
- Operating procedures;
- Records of Council's operations;
- Information from Closed or Special Council or Committee Meetings; and
- Information designated confidential by resolution of a council or special council meeting.

The *Right to Information Act 2009 (Tas)* and the *Personal Information Protection Act 2004 (Tas)* also apply to Council. If you are concerned about the privacy of personal information held by Council, please refer to Council's Privacy Policy.

Protect personal and company devices

When authorised users use their digital devices to access company emails, accounts or systems, they introduce security risk to our data. Councillors, employees and others who access Council's systems must keep both their personal and Council-issued computer, tablet and mobile phone secure.

Authorised users will:

- Keep all devices protected by effective passwords;
- Use an authorised antivirus product managed or approved by Council's IT provider;
- Ensure devices are not left exposed or unattended while unlocked;
- Install security updates of browsers and systems monthly or as soon as updates are available. (Council owned devices are automatically updated. Only personal devices will need to manually comply with this policy);
- Log into Council accounts and systems through secure and private networks only;

- Not connect any devices that have been configured to use operating systems not supplied by the original manufacturer, for example Apple devices that have been jail broken' and Android devices that have 'root access' installed.

Any mobile device that accesses Council's systems, include email systems, must be enforced with a passcode lock and the ability for Council to remotely remove any of its data from the device at the Council's discretion. Typically, this action would be taken in the event of a mobile device being lost or stolen.

Authorised users must avoid accessing internal systems and accounts from other people's devices or lending their own devices to others. When new employees of Council receive a company-issued device, it may be automatically set up to comply with these policies.

Keep emails safe

Emails often host scams and malicious software (e.g. phishing scams). To avoid a virus infection or data theft, authorised users of Council systems will:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. 'watch this video, it's amazing');
- Be suspicious of clickbait titles (e.g. offering prizes, advice);
- Check email and names of people they receive a message from to ensure they are legitimate;
- Look for inconsistencies or tell-tale give-away (e.g. grammar mistakes, capital letters, excessive number or exclamation marks);
- Attachments opened on iPhone or iPads present little risk of infection. If you are unsure about an attachment, you can attempt to open it on an Apple device first (due to the nature of Android open system and ability to jail-break devices we do not recommend the use of Android devices for testing attachments).

If an authorised users is not sure that an email received is safe, the email must be referred to Council's IT service provider by forwarding a copy to helpdesk@inscopeit.com.au.

Manage passwords properly

Password leaks are dangerous since they can compromise Council's entire IT infrastructure. Not only should passwords be secure so they cannot be easily hacked, they should also remain secret. For this reason, Councillors, employees and others with authorised access to Council systems must:

- Choose password with a complexity of a minimum of 6 alphabetical, 2 numeral/special characters and 1 case sensitive, and avoid information that can be easily guessed (e.g. birthdays). Good passwords don't have to be hard to remember. An example of a good password that's easy to remember is '15 Yellow Ducks' or 'it rains 9 times out of 10'; an example of a password that's hard to remember is 'o4!5rGcB35a';
- Remember passwords instead of writing them down. Anyone who needs to write down a password is obliged to keep the paper or digital document confidential and destroy it when their work is completed;
- Exchange credentials only when absolutely necessary and with the permissions of the General Manager or Council delegate. If exchanging them in person isn't possible,

authorised users should telephone instead of emailing the other person, and only exchange credentials if they personally recognise the person they are talking to;
- Passwords are scheduled to the changed every 90 days. Council's IT service provider should be contacted immediately if there is a security risk with a current password.

Transfer data securely

Transferring data introduces security risk. Authorised users must:

- Avoid transferring sensitive data (e.g. customer information, employee records, council minutes) to other devices outside Council. This includes via portable storage devices, directly connected (e.g. plugged in) tablets or phones. When mass transfer of such data is needed employees must ask Council's IT provider for help on how to do this securely;
- Share confidential information over the council network system and not over public wifi or private connection;
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies to protect the data; and
- Report scams, privacy breaches and hacking attempts to Council's IT provider immediately.

Council's IT service provider need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, authorised users must report perceived attacks, suspicious emails or phishing attempts immediately to Council's IT Provider and Council's Corporate Services Manager.

Council's IT Provider will investigate promptly, resolve the issue and send an alert to all users when necessary. We encourage authorised users to contact them with any questions and concerns.

Additional measures

To reduce the likelihood of security breaches, Councillors, employees and other authorised users must:

- Report stolen or damaged equipment as soon as possible to the Corporate Services Manager and Council's IT Provider;
- Change all account passwords immediately when a device is stolen;
- Report a perceived threat or possible security weakness in Council systems;
- Not download suspicious, unauthorised or illegal software to their Council equipment; and
- Avoid accessing suspicious website.

Authorised users of Council's IT systems must also comply with Council's policy addressing social media and internet usage.

Council's IT provider must install and maintain effective anti-malware software and access authentication systems and ensure all remote access is protected by a secure VPN connection.

Council's IT provider must ensure that multi-factor authentication is in place for Office365 for all authorised users.

Council will request that its IT provider conduct an IT Security Assessment annually. This assessment will be modelled from the Australian Signals Directorate (ASD) Essential Eight Maturity Model. Any findings of of security from this annual assessment will be implemented by Council to ensure a safe and secure IT system. Information on the Essential Eight Maturity Model can be found here Essential Eight | Cyber.gov.au.

Remote employees

Since they will be accessing Council accounts and systems from a distance, users authorised to access systems remotely must follow all data encryption, protection standards and setting, and ensure the private network is secure.

Remote users can seek advice from Council's IT provider regarding the security of their own private networks to make sure it complies with this policy.

Protecting and preserving Council's data

Council's IT provider will maintain appropriate back up for Council's servers and ensure that back-ups are available in the event of an interruption to the system. In consultation with Council, Council's IT provider will prepare and maintain an effective Disaster Recovery Plan/Business Continuity Plan for its IT systems and facilities. This Plan will include:

- Agreed maximum outage times and target recovery times for each element of Council's IT system;
- Scheduled testing, this may be performed by an another external agent and not the Council's current IT provider;
- Provision for reports of the outcomes of testing to be sent to Council after each test;
- Regular reviews of the Plan that take into account outcomes of testing, changes in systems or system risks or other changes required to reflect Council's operating environment.

Council's IT provider will provide proactive advice to Council on emerging risks to its IT environment and assist Council to mitigate these.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action. Council will examine each incident on a case-by-case basis, but action may include:

- For first-time, unintentional, small-scale security breach: Council may issue a verbal warning and offer additional training to the user about security.
- For intentional, repeated or large-scale breaches or those that cause severe financial or other damage: more severe disciplinary action, up to and including termination, may be imposed.

Additionally, users of Council's IT systems who disregard security instructions will face progressive discipline, even if that behaviour has not resulted in a security breach.

All system users must take security seriously. Everyone, from our local community to councillors, employees and stakeholders, should feel that their data is safe.

Ethically and legally, councillors, employees and other authorised users must proactively protect our systems and databases by being vigilant and keeping cyber security top of mind.

Associated documents

- Strategic Risk Register
- Privacy Policy
- Use of Communication Devices & Social Media

Policy approval

This policy was approved at the ordinary council meeting held on 27 March 2024, resolution number 10/03.2024/C.

Blake Repine
General Manager

Disclaimer
That this policy be read in conjunction with any and all other Council and/or management policies.

Acceptance of Cyber Security Policy

Authorised User	Tasman Council
Signature:	Signature:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date: