Cyber Security Policy

Policy Details

Policy Category	Council Policy
Date Adopted	17 January 2024
Resolution Number	0124/013
Approval Authority	Council
Effective Date	17 January 2024
Policy Version Number	1.0
Policy Owner	Director of Corporate Services

Supporting documentation

Legislation	• Nil
Policies	• Invoice Fraud Policy • Code of Conduct • The People Management Framework
Delegations	• Nil
Forms	• Nil
Supporting Documents	• Nil

Version History:

Version	Adopted	Comment	eDRMS #
1.0	17/01/24	Council Resolution 0124/013 - Initial Implementation	

Table of Contents

1. Overview

Cyber-crime represents a very real and significant threat to Carpentaria Shire Council, herein referred to as “the Council”. In most cases, the attacks and threats will be targeted at the people who work with or for our company. For this reason, a detailed Cyber Security Policy that outlines the responsibilities and expectations of the Council’s employees and contractors is essential to ensuring we can protect the Council and its assets.

2. Purpose

The Council’s Cyber Security Policy provides the general framework, policies, standards and guidelines required to protect the Council, its digital assets (systems and data), and sensitive information from loss, theft, alteration, disruption or destruction as a result of a cyber related incident.

The Council’s Cyber Security Policy is designed to be a ‘living’ document. It should be regularly updated to reflect the constantly evolving threats and risks the Council faces. It should also be updated when failures or improvements are identified when responding to real world incidents or when general improvements in process, awareness or understanding are identified.

3. Scope

The Council's Cyber Security Policy is applicable to all stakeholders, executives, employees, and contractors of the Council and any other third parties that has custody or access to the Council's digital assets (technology) and sensitive information.

Digital assets include all digital data and digital systems. Some examples include:

- ALL data stored in a digital format
- Technology based production equipment
- Desktop workstations
- Laptop computers
- Tablets
- Smartphones
- Point of Sale (POS) terminals
- Servers
- Removable media and hard drives
- Smart TV's and other smart devices
- CCTV and surveillance systems
- Networking equipment such as routers, firewalls and switches

Examples of sensitive information include:

- Any document marked CONFIDENTIAL, SENSATIVE, or PRIVATE
- All Personally Identifiable Information (PII)
- Information deemed sensitive by Australia's Mandatory Breach Notification Laws
- Any lists containing people's names
- Client or customer lists
- Employee lists
- Financial and account information
- Supplier invoices
- Credit card information
- Contracts
- Research information and data

4. Acceptable Use of Technology Policy

The intentions of the Acceptable Use Policy are not to impose restrictions that are contrary to the Council's established culture of openness, trust and integrity, but rather protect the Council's employees, partners, clients, customers and the Council from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing, and FTP, are the property of the Council. These systems are to be used for business purposes in serving the interests of the Council, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every company employee, contractor and third party who deals with company information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

4.1 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the Council. These rules are in place to protect the employee and the Council. Inappropriate use exposes the Council to risks including virus attacks, compromise of network systems and services, and legal issues.

4.2 Scope

This policy applies to the use of information, electronic and computing devices, and network resources used to conduct the Council business or to interact with internal networks and business systems, whether owned or leased by the Council, the employee, contractor, or a third party. All employees, contractors, consultants, temporary, and other workers at the Council and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the Council policies and standards, and local laws and regulation. Any exceptions to this policy must be approved in writing by the Chief Information Security Officer.

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Council, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Council.

4.3 General Use and Ownership

4.3.1 The Council's proprietary information stored on electronic and computing devices whether owned or leased by the Council, the employee or a third party, remains the sole property of the Council. You must ensure through legal or technical means that confidential and proprietary information is kept both private and secure.

4.3.2 You have a responsibility to promptly report the theft, loss or unauthorised disclosure of the Council's confidential and proprietary information to the Incident Response Team.

4.3.3 You may access, use or share the Council's confidential and proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.

4.3.4 For security and network maintenance purposes, authorised individuals within or engaged by the Council may monitor equipment, systems and network traffic at any time, per the Employee Internet Use Monitoring and Filtering Policy.

4.3.5 The Council reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.4 Security and Proprietary Information

4.4.1 All mobile and computing devices that connect to the corporate network must be secured by a password or passcode.

4.4.2 All devices within the SCADA and Telemetry environment should be secured by a password or passcode. These passwords can be shared with authorised SCADA team members to comply with technical requirements where needed. Remote access user accounts to SCADA systems must be unique for the individual user.

4.4.3 System level and user level passwords must comply with the Password Policy. Providing passwords or access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.4.4 All computing devices must automatically activate a password protected lock (eg. screen saver or screen lock requiring a password to open) if the device is inactive for 10 minutes or more. You must lock the screen or log off when the device is unattended.

4.4.5 Employees should only use Council email account for business purposes only.

4.4.6 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.5 Unacceptable Use

The following activities are, in general, prohibited. Employees and contractors may be exempted from these restrictions during the course of their legitimate job responsibilities (eg. Systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee or contractor of the Council authorised to engage in any activity that is illegal under local, state, federal or international law while utilising company owned or leased resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.5.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

(a) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Council.

(b) Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Council or the end user does not have an active license is strictly prohibited.

(c) Accessing data, a server, systems or an account for any purpose other than conducting the Council business, even if you have authorised access, is prohibited.

(d) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

(e) Introduction of malicious programs into the network or server (eg. viruses, worms, Trojan horses, e-mail bombs, etc).
(f) Subject to 4.4.2 revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
(g) Using a company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
(h) Making fraudulent offers of products, items, or services originating from any company account.
(i) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
(j) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
(k) Port scanning or security scanning is expressly prohibited unless prior notification to IT officer is made and written approval received.
(l) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
(m) Circumventing user authentication or security of any host, network or account.
(n) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
(o) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
(p) Providing information about, or lists of, company employees to parties outside the Council unless required for Council-related duties.

4.5.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realise they represent the Council. Whenever employees state an affiliation to the Council, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Council.

Email accounts should only be used for business purposes. This excludes:

(a) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
(b) Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
(c) Unauthorised use, or forging, of email header information.
(d) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
(e) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
(f) Use of unsolicited email originating from within the Council's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Council or connected via the Council's network.

(g) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.5.3 Blogging and Social Media

The following blogging and social media activities are strictly prohibited:

(a) Blogging and/or posting to social media by employees, using the Council's property and systems is prohibited, unless the employee is authorised to do so as part of their role. Blogging and/or posting to social media by employees, using personal computer systems, is subject to the terms and restrictions set forth in this Policy.

(b) Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material when engaged in blogging or posting to social media.

(c) Employees shall not engage in any blogging or social media posting that may harm or tarnish the image, reputation and/or goodwill of the Council and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging, posting to social media, or otherwise engaging in any conduct prohibited by the Council's Non-Discrimination and Anti-Harassment policy if applicable.

(d) Employees may also not attribute personal statements, opinions or beliefs to the Council when engaged in blogging or posting to social media. If an employee is expressing his or her beliefs and/or opinions in blogs or social media posts, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the Council. Employees assume any and all risk associated with blogging and posting to social media.

(e) Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the Council's trademarks, logos and any other intellectual property may also not be used in connection with any blogging or social media posting activity. For further guidance on the use of social media refer to Council's Social Media Policy.

5. Password Construction Guidelines

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the network.

This guideline provides best practices for creating secure passwords and applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

Strong passwords should be long and complex, ideally with a minimum of 14 characters, which should include a mix of numbers and special characters. The use of passphrases, passwords made up of multiple words is good practice. Examples include "*It's time for vacation*" or "*block-curious-sunny-leaves*". Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of "Welcome123" "Password123" "Changeme123"

In addition, every work account should have a different, unique password. To help support users maintain multiple passwords, use 'password manager' software that is authorised and provided by the Council.

Whenever possible, enable the use of multi-factor authentication.

6. Authentication Policy

Strong credential management and authentication is a critical component of information security. A poorly chosen password may result in unauthorised access and/or exploitation of our resources. All staff, including contractors and vendors with access to company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any company facility, has access to the Council network, or stores any non-public company information.

6.1 Password Creation

6.1.1 All user-level and system-level passwords must conform to '5. Password Construction Guidelines'.

6.1.2 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

6.1.2 User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

6.2 Password Policy

6.2.1 Subject to 4.4.2 passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, confidential company information. Exclusion for local PC SCADA user accounts is excepted.

6.2.2 Passwords must not be inserted into email messages, or other forms of electronic communication, nor revealed over the phone to anyone.

6.2.3 Passwords may be stored only in "password managers" authorised by the Council.

6.2.4 Do not use the "Remember Password" feature of applications (for example, web browsers) unless the computer or device is secured by your password.

6.2.5 Any user suspecting that his/her password may have been compromised must report the incident to the Incident Response Team, which includes the ICT Support Officer (contact Ali Hassan - ali.hassan@carpentaria.qld or 07 4745 2202). Further guidance and contact information is provided in the Incident Response Plan.

6.3 Multi-Factor Authentication

6.3.1 Multi-factor authentication must be enabled on all cloud based accounts with administrator privileges.

6.3.2 Multi-factor authentication should be required for all remote access connections to the corporate network.

6.3.3 Whenever available, multi-factor authentication must be enabled on all email and cloud services accounts. Exceptions are permitted when connecting from a Trusted Location, such as the council network.

6.3.4 Multi-factor authentication should be implemented for accounts with remote access to SCADA or Telemetry systems.

6.3.5 Wherever possible, the multi-factor authentication methods used should be U2F or authenticator apps for authentication and should avoid the use of SMS and email for delivery of one time passcodes, where possible. There is a current exception for some SCADA systems with SMS and or certificate based 2FA only possible.

7. Clean Desktop Policy

Maintaining a clean desk is an important practice that ensures all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilise when trying to reduce the risk of security breaches within the workplace.

The purpose of this policy is to establish the minimum requirements for maintaining a “clean desk” – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site.

This policy applies to all employees and contractors either working on premise or remotely when performing work related activities for the Council.

7.1 Clean Desktop Policy requirements

7.1.1 Employees and contractors are required to ensure that all sensitive/confidential information in hardcopy is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

7.1.2 Computer workstations and laptops must be locked when workspace is unoccupied.

7.1.3 Any Restricted, Confidential or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

7.1.4 File cabinets containing Restricted, Confidential or Sensitive information must be kept closed and locked when not in use or when not attended.

7.1.5 Keys used for access to Restricted, Confidential or Sensitive information must not be left at an unattended desk.

7.1.6 Laptops and devices not in use must be either locked with a locking cable or locked away in a drawer / cabinet when not in use.

7.1.7 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

7.1.8 Printouts containing Restricted, Confidential or Sensitive information should be immediately removed from the printer.

7.1.9 Upon disposal Restricted, Confidential and/or Sensitive documents should be shredded or placed in the locked confidential disposal bins if available.

7.1.10 Whiteboards containing Restricted, Confidential and/or Sensitive information should be erased.

7.1.11 Authorised devices that form part of SCADA or Telemetry systems should be marked with unique anti-tamper stickers/devices.

8. Employee Internet Use Monitoring and Filtering Policy

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within the Council's network. This policy is designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

This policy applies to all company employees, contractors, vendors and agents with a company-owned or personally-owned computer or workstation connected to the Council network.

This policy applies to all end user initiated communications between the Council's network and the Internet, including web browsing, email, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

8.1 Web Site Monitoring

The IT department or and approved external IT provider shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

8.2 Access to Web Site Monitoring Reports

General trending and activity reports will be made available to senior management or the Incident Response Team as needed upon request to the IT department or external IT provider. Senior management or the Incident Response Team may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the senior management or the Incident Response Team upon written or email request to the IT department or external IT provider from a Human Resources Representative that has been approved by senior management.

8.3 Internet Use Filtering System

The IT department or external IT provider shall block access to Internet websites and protocols that are deemed inappropriate for the Council's corporate environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email

8.4 Internet Use Filtering Rule Changes

The IT department or external IT provider shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

8.5 Internet Use Filtering Exceptions

If a site is mis-categorised, employees may request the site be un-blocked by submitting a ticket to the IT department or external IT provider's help desk. An IT department employee or external IT provider will review the request and un-block the site if it is mis-categorised.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorised, they must submit a request to their Human Resources representative. HR will present all approved exception requests to the IT department or external IT provider in writing or by email. The IT department or external IT provider will unblock that site or category for that associate only. The IT department or external IT provider will track approved exceptions and report on them upon request.

9. Email Policy

Electronic email is the primary communication and awareness method in use within the Council. Misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

The purpose of this email policy is to ensure the proper use of the Council email system and make users aware of what the Council deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within the Council Network.

This policy covers appropriate use of any email sent from a company email address and applies to all employees, contractors, vendors, agents and third parties operating on behalf of the Council.

9.1 Email Policy Requirements

9.1.1 All use of email must be consistent with company policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

9.1.2 Council email accounts should only be used for company business-related purposes. Personal use and Non-company related commercial uses are prohibited.

9.1.3 Email should be retained only if it qualifies as a company record i.e. if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

9.1.4 Email that is identified as a company record shall be retained according to the Council's Record Retention Schedule if applicable.

9.1.5 The Council email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any company employee should report the matter to their supervisor immediately.

9.1.6 Users are prohibited from automatically forwarding company email to a third party email system (noted in 9.1.8 below). Individual messages which are forwarded by the user must not contain company restricted, confidential or sensitive information.

9.1.7 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct company business, to create or memorialise any binding transactions, or to store or retain email on behalf of the Council. Such communications and transactions should be conducted through proper channels using company-approved documentation. Personal usage of these systems is not prohibited as long as company business is not conducted using these systems.

9.1.8 Company employees shall have no expectation of privacy in anything they store, send or receive on the Council's email system.

9.1.9 The Council may monitor messages without prior notice. The Council is not obliged to monitor email messages.

10. Social Media Policy and Guidelines

Social media and networking is increasingly becoming a standard component of work and personal life. While companies are increasingly embracing social media technologies as a way of promoting products and services and improving employee retention, the potential for confidential data leakage or employee abuse is ever present.

The purpose of this policy and accompanying guidelines is to outline to all employees, contractors and other individuals performing work for the Council, acceptable use of social media networking applications both on the job and in personal usage situations.

10.1 Speaking on Behalf of the Council

Some employees and individuals performing work on behalf of the Council will, by the nature of their position, be knowledgeable about certain aspects of the Council and may be authorised to speak on the behalf of the Council.

10.1.1 You must not speak on behalf of the Council unless you are authoritative on the subject and have been authorised, in writing, to speak on behalf of the Council by your manager or responsible company executive.

10.1.2 You must not share information that is confidential or proprietary. Only public available information or information which you have been authorised to share may be disseminated.

10.1.3 Be transparent. Clearly identify yourself, that you work for the Council, and what your role is.

10.1.4 Be professional. This includes being honest, respectful and factual at all times.

10.1.5 Do not refer to the products or services of vendors, clients, customers or partners without obtaining their consent.

10.1.6 Do not use content, images or any other form of copyrighted material without the appropriate permission and credit referencing.

10.2 Personal Use of Social Media Activities

It is understood that some employees and individuals performing work on behalf of the Council will be active on social media.

10.2.1 If you are discussing products or services provided by the Council, then you must identify yourself as an employee and make it clear that the views are yours and do not represent the views of the Council.

10.2.2 You must not speak disparagingly about the Council, its employees or officers, or any product or service provided by the Council.

10.2.3 You may not sell or endorse any product or service which would compete with products or services sold by the Council.

10.2.4 No personal views should be presented when representing the Council.

11. Removable Media Policy

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information. The purpose of this policy is to minimise the risk of loss or exposure of sensitive information maintained by the Council and to reduce the risk of acquiring malware infections on computers operated by the Council.

This policy applies to all the Council employees and contractors, and all computers and servers operating in the Council.

Company staff may only use the Council's removable media in their work computers. The Council's removable media may not be connected to or used in computers that are not owned or leased by the Council without explicit permission from the Council's IT department, Incident Response Team or external IT provider.

Ideally, contractors should not be using removable devices, except Council's removable media, when using Council equipment. USB scanners can be used if need be. Otherwise, contractors should email or share relevant files with Council staff.

Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it should be stored in an encrypted state.

Exceptions to this policy may be requested on a case-by-case basis by the Council -exception procedures.

12. Remote Access Policy

Remote access to the Council's corporate network is essential to maintain access and productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of the Council, we must mitigate these external risks to the best of our ability.

The purpose of this policy is to define rules and requirements for connecting to the Council's network from any host. These rules and requirements are designed to minimize the potential exposure to the Council from damage which may result from unauthorised use of the Council's resources. Such damage includes the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical company internal systems, and fines or other financial liabilities incurred as a result of those losses.

This policy applies to all company employees or contractors with a company-owned or personally-owned computer or workstation used to connect to the Council's network. This policy applies to remote access connections used to do work on behalf of the Council, including reading or sending email, operating production systems, and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to the Council's networks.

12.1 Remote Access Policy Requirements

It is the responsibility of company employees, contractors, vendors, agents and third parties with remote access privileges to the Council's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Council.

General access to the Internet through the Council network is strictly limited to company employees and contractors (hereafter referred to as "Authorised Users"). When accessing the Council network from a personal computer, Authorised Users are responsible for preventing access to any company computer resources or data by non-Authorised Users. Performance of illegal activities through the Council network by any user (Authorised or otherwise) is prohibited. The Authorised User bears responsibility for and consequences of misuse of the Authorised User's access. For further information and definitions refer to Acceptable Use of Technology Policy and the Employee Internet Use Monitoring and Filtering Policy.

Authorised Users will not use the Council's networks to access the Internet for outside business interests.

12.1.1 Secure remote access must be strictly controlled with encryption (ie. Application Proxy Services, Virtual Private Networks (VPNs)), strong pass-phrases, and multi-factor authentication.

12.1.2 Where relevant, network segmentation and segregation should be implemented (i.e. Virtual Local Area Networks (VLANs), internal NAT firewall to prevent access to sensitive systems (eg: SCADA)) to separate traffic belonging to the same security domain. The VLANs should not be used to separate network traffic between networks belonging to different security domains, nor separate traffic between the company's networks and public network infrastructure. VLANs should not share VLAN trunks.

12.1.3 If VLANs are implemented, network devices managing VLANs should be administered from the most trusted security domain.

12.1.4 Remote access to SCADA or telemetry systems should be secured as per 12.1.1.

12.1.5 Authorised Users shall protect their login and password, even from family members.

12.1.6 While using a company-owned computer to remotely connect to the Council's corporate network, Authorised Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control (eg. the users home network, their mobile hotspot and not publicly accessible Wi-Fi hotspots in cafes or airport lounges for example) or under the complete control of an Authorised User or Third Party.

12.1.7 All hosts that are connected to the Council's corporate networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

12.1.8 Personal equipment used to connect to the Council's networks must meet the requirements of the Council-owned equipment for remote access.

12.1.9 Multi-factor authentication is required for any user account with Remote Access privileges and is to be implemented in line with the Authentication Policy.

13. Social Engineering Policy

Social Engineering is the activity of manipulating someone to take an action they ordinarily wouldn't do if they knew the consequences. This includes actions like handing over passwords, confidential information or opening infected and malicious files that can enable access to computers or networks. It can also include manipulation and impersonation tactics to pressure or trick employees to pay invoices that aren't real or to make payments to different bank accounts.

These types of attacks are rapidly becoming the method of choice for bad actors looking to access computer systems and steal data or money. The Council acknowledges the high exposure its employees and contractors are subjected to by these attacks. The Council is committed to developing a security culture that supports its employees in identifying these types of attacks and providing them with the resources and guidance they need to effectively respond and report.

This policy has 2 purposes:

1) To make employees aware that (a) fraudulent social engineering attacks occur, and (b) there are procedures that employees can use to detect these attacks. In particular:
    a. Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks.
    b. Employees know who to contact in these circumstances.
    c. Employees recognise they are an important part of the Council's security. The integrity and awareness of an employee is one of the best lines of defence for protecting sensitive information and unauthorised access regarding The Council's resources.
2) To create specific procedures for employees to follow to help them identify the situation and make the best choice when:
    a. Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect the Council's sensitive information.
    b. The employee is being "pressured" or "encouraged" or "tricked" into sharing sensitive data or taking an action that is against the interest of the Council.

This policy is applicable to all employees and contractors of the Council.

13.1 Identifying Social Engineering Techniques and Attacks

Sensitive information of the Council should not be shared with an Unauthorised individual (this includes people attempting to impersonate Authorised individuals such as CEO's and CFO's) if he/she uses words and/ or techniques such as the following:

a) An "urgent matter"
b) A "forgotten password"
c) A "computer virus emergency"
d) Any form of intimidation from "higher level management"
e) Any "name dropping" by the individual which gives the appearance that it is coming from legitimate and authorised personnel.
f) The requester requires release of information that will reveal passwords, model, serial number, or brand or quantity of company resources.
g) The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.
h) The techniques are used by a person that declares to be "affiliated" with the Council such as a sub-contractor.
i) The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company.
j) The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

13.2 Defending Against Social Engineering Techniques and Attacks

a) All employees and contractors must attend and complete security awareness training within 30 days from the date of employment and every 12 months thereafter.
b) All finance, human resources, and helpdesk employees or contractors must attend and complete specialty security awareness training pertaining to their roles within 30 days from the date of employment and every 6 months thereafter in addition to the general security awareness training undertaken by all employees.
c) If one or more circumstances described in section 13.1 is detected by an employee or contractor, then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.
d) If the identity of the requester CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.
e) If the supervisor or manager is not available, that person MUST contact the Incident Response Team.
f) If a member of the Incident Response Team is not available, the person described in section 13.1 MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

13.3 Invoice Approvals and Payment Policy

Business Email Compromise (BEC) and Invoice Email Fraud is an increasing financial fraud attack where a bad actor intercepts or duplicates invoices from suppliers and attempts to have the accounts payable employee of the business change the bank details, diverting the funds to the bank accounts controlled by the bad actor.

The Council has developed specific guidelines and procedures on how invoices should be processed and what steps need to be taken when bank account details are requested to be changed.

The Council's Invoice Approvals and Payment Protocol is included in the Invoice Fraud Policy and should be reviewed and familiarised by all accounts payable employees, contractors and administrative managers.

14. Security Awareness Training Policy

Historically, cyber security has been viewed largely as an IT issue but as IT controls have gotten better, bad actors have found that targeting people (the human factor) provides a much easier and faster way to achieve their outcomes.

Employees are on the front line of these attacks and equipping them with key knowledge and skills is essential to ensuring the overall cyber security of the organisation.

The Council wants all of its employees to be safe at work and at home when using technology and the Internet. The Council recognises that regular education, awareness training, and a strong "top-down" security culture is the best way to achieve this.

This policy applies to all company employees and contractors.

14.1 Security Awareness Training Policy Requirements

14.1.1 All senior executives, leadership team, and board members should undertake awareness training to better understand cyber risk, how it affects the organisation and what their roles and responsibilities are in developing and leading a strong security culture.

14.1.2 All employees and contractors shall receive training on what their roles and responsibilities are as outlined in this Cyber Security Policy as part of their initial employee/contractor induction and then periodically throughout each year.

14.1.3 All employees and contractors shall receive general cyber security awareness training and participate in cyber security awareness training and assessment exercises at least once per year or when related incidents occur.

14.1.4 All human resources, finance, and accounts payable employees and contractors shall receive speciality cyber security training on threats specific to their roles and responsibilities at least once per year and reinforced periodically throughout the year or when related incidents occur.

15. Administrative Privileges Policy

Gaining access to user accounts with administrative privileges is one of the primary objectives of bad actors looking to breach computers and corporate networks. They provide almost unlimited access to install software, create accounts, steal or destroy data, and pivot to other networks. For this reason, user accounts with administrative privileges should be kept to an absolute minimum and protected with strong credentials.

This policy applies to all company employee and contractor user accounts that are used to authenticate company-owned or personally-owned computers, workstations, or servers that connect to the Council network or Internet.

15.1 Administrative Privileges Policy Requirements

15.1.1 Employee and contractor user accounts, including all members of the IT department, senior executives, leadership teams and board members, should not have administrative privileges that allow them to administer workstations, laptops or the Council's corporate networks.

15.1.2 Dedicated user accounts with administrative privileges should be created and used specifically for administrative tasks either by the IT department or within specific groups/units for day-to-day administration tasks of user workstations.

15.1.3 User accounts with administrative privileges should have the highest level of password criteria requirements e.g. changing administrator passwords regularly and with staff changeover, and having long unique passphrases.

15.1.4 User accounts with administrative privileges that are used to access the Council servers, cloud services, networking devices or other critical infrastructure must be secured with multi-factor authentication wherever it is possible to do so.

15.1.5 User accounts with administrative privileges should never be used for day-to-day user access.

15.1.6 User accounts with administrative privileges should not have associated email accounts.

15.1.7 User accounts with administrative privileges should always be logged out immediately after administration tasks have been completed.

15.1.8 User accounts with administrative privileges should always be kept to a minimum.

16. Digital Asset Inventory Policy

With the increasing up take and integration by business of technology platforms, digital systems and storage of digital data, it is increasingly important to have and maintain an up to date inventory of where these digital assets are, who has access to them, and how important they are in terms of value, privacy, and day to day operations.

The Council acknowledges that technology plays an important part in the organisation's day to day operations and value, and that maintaining a comprehensive and up to date digital asset inventory is essential to ensuring the high value assets are being identified so that they can be protected from attack and recovered in the event of an incident or disaster.

This policy applies to all company-owned or leased hardware devices, digital data storage repositories and cloud services accounts.

16.1 Digital Asset Inventory Policy Requirements

16.1.1 A Digital Asset Register is to be created that can be kept both secure and private, with password protection as mandatory and ideally re-enforced with multi-factor authentication if available.

16.1.2 A company employee will be identified at all times as the Digital Asset Register Manager who will be responsible for ensuring the register is kept up to date and maintained. Currently, the Digital Asset Register Manager is the IT Officer.

16.1.3 The Digital Asset Register Manager should be notified within 14 days of the implementation or decommissioning of any relevant company digital asset so that the register can be kept up to date.

16.1.4 Access to the register should be limited to the Digital Asset Register Manager, the Incident Response Team, and the team responsible for the Council's backup and recovery management.

16.1.5 The register should include the following asset categories at a minimum:

a) **Name**: Name of the asset
b) **Type**: Digital data or digital system
c) **Description**: A brief description of the digital asset
d) **Location**: Where the digital asset is located. (eg. office location, cloud provider, etc)
e) **Implement date**: Date that the digital asset was installed, commissioned or created
f) **Decommission date**: Date that the digital asset was decommissioned, removed or deleted.
g) **Security level**: Identification of the security level priority of the digital asset in the following ranges:
    - **High** (contains personally identifiable data, trade secrets, intellectual property, financial data, core networking or security devices with high sensitivity that if exposed or lost could cause large, material damage or loss)
    - **Moderate** (working papers and files, finance workstations / laptops, production workstations / laptops or other confidential documents with moderate sensitivity that if exposed or lost could cause significant damage or loss)
    - **Low** (publicly available information or information with low sensitivity that if exposed or lost would cause no or low impact to the organisation.)

h) **Operational priority**: Identification of the operational priority of the digital asset in the following ranges:
   - **High** (a critical asset that must be available within 4-8 hours from loss of access or interruption.)
   - **Moderate** (an important asset that must be available within 2-5 days from loss of access or interruption.)
   - **Low** (an asset that must be available within 1-2 weeks from loss of access or interruption.)

i) **Value**: Identification of the value of the digital asset in the following ranges:
   - **High** (a high value asset that would cause extreme loss to the organisation if lost or destroyed.)
   - **Moderate** (a moderate value asset that would cause substantial loss to the organisation if lost or destroyed.)
   - **Low** (a low value asset that would cause minimal loss to the organisation if lost or destroyed.

j) **Users with access**: a list of employees, contractors or users that have access to the asset. This can include groups like, all employees, or finance employees.

16.1.6 The Digital Asset Register Manager should notify the Incident Response Team and the team responsible for the Council's backup and recovery management of any changes to the register in a timely manner. Examples of notification response times include:

a) Ideally, notification of the addition or removal of any digital asset to the register should be made to the relevant team/s within 7 days of the change but should never exceed;
b) 14 days for any digital asset with a security categorisation and / or operational priority of High,
c) 30 days for any digital asset with a security categorisation and / or operational priority of Moderate, or
d) 60 days for any digital asset with a security categorisation and / or operational priority of Moderate.

16.1.7 The Digital Asset Register Manager shall conduct an audit and review of the Digital Asset Register at least once per year to ensure it is correct and up to date.

17. Backup and Recovery Policy

With the increasing reliance on technology, being able to recover key digital assets to an operational state in a timely manner, in the event of an incident, can be critical to the ability of the organisation to continue to operate. Digital assets include employee data, citizen data and system configurations of SCADA/Telemetry systems.

Having a structured and tested backup and recovery strategy is a key component of the Council's ability to defend itself from cyber related incidents as well as other general disasters.

It is unlikely that the Council will be able to defend all of its digital assets. For this reason it will be essential to develop a backup and recovery strategy that is based on defending the digital assets with the highest value and operational importance.

This policy applies to all company-owned or leased hardware devices, digital data storage repositories and cloud services accounts and to the team and/or provider responsible for the Council's backup and recovery strategy.

17.1 Backup and Recovery Policy Requirements

17.1.1 The digital assets to be included in the Council's backup and recovery strategy must be based off a Digital Assets Register that is regularly updated and maintained, and that categorises digital assets by Security Level, Operational Priority and Value.

17.1.2 The Council's management and leadership in consultation with expert advice and guidance will be responsible for defining the desired recovery time and history retention requirements for the Council's digital assets based on their Operational Priority and Value.

17.1.3 Digital assets with a Security Level of High must be encrypted in transit and at rest and should be stored in a secure offsite location with access to the backup store repository secured with multi-factor authentication.

17.1.4 Digital assets with a Security Level of Moderate should be encrypted at rest and should be stored in a secure offsite location with access to the backup store repository secured with multi-factor authentication.

17.1.5 Backups of digital assets with a Value of High should be encrypted in transit and at rest and must be stored in a secure offsite location with access to the backup store repository secured with multi-factor authentication.

17.1.6 Backups of digital assets with a Value of Moderate should be encrypted at rest and should be stored in a secure offsite location with access to the backup store repository secured with multi-factor authentication.

17.1.7 All backups of digital assets that have a categorisation of High must be tested for full operational recovery at least once within 30 days of creation and then periodically once per year.

17.1.8 All backups of digital assets that have a categorisation of High must be tested for full operational recovery at least once within 14 days of creation and then once per year.

17.1.9 All backups of digital assets that have a categorisation of Moderate must be tested for full operational recovery at least once within 30 days of creation.

17.1.10 All backups of digital assets that have a categorisation of Low should be tested for full operational recovery at least once within 60 days of creation.

17.1.11 Backup schedules for digital assets that have been decommissioned should be removed and backup files should be deleted/removed in line with the Council's history retention policy.

17.1.12 The Council's backup and recovery strategy should be reviewed annually alongside the Digital Asset Register to ensure all digital assets are accounted for and are being protected in line with their categorisations.

18. Update and Patching Policy

Bad actors use malware to exploit vulnerabilities in operating systems and applications to take control of computers and other connected devices. Implementing an update and patching programme to address and rectify these vulnerabilities is an essential step in protecting the organisation's digital assets from exploitation.

The Council is committed to ensuring all digital systems, operating systems, devices and applications are kept up to date and have all available security patches applied in a timely manner.

This policy applies to all company-owned or leased hardware devices, and any external devices that are used by employees that connect to the Council's corporate network.

18.1 Update and Patching Policy Requirements

18.1.1 All workstations, laptops and devices should be set to automatically install operating system and application updates and patches with the user not being able to cancel the process

18.1.2 All company server operating systems and installed applications should be updated in a managed state by the IT department or an external IT provider on a monthly basis or sooner.

18.1.3 All company devices including but not limited to routers, firewalls, switches, modems, printers, photocopiers, TV's, network attached storage devices (NAS), CCTV, WiFi, and security systems should have firmware updates set to automatically install wherever possible or be manually installed by the IT department or an external IT provider on a 6 monthly basis or sooner.

18.1.4 All SCADA and Telemetry systems should have all updates installed manually to avoid the risk of unplanned outages due to failed automatic updates. Update installation is to be performed by the IT department/ managed providers/SCADA technicians on a periodic basis, i.e. 6 months or sooner.

18.1.5 A process should be developed for SCADA and Telemetry systems to safely introduce vendor-supported software updates and patches. Only vendor-supported applications and operating systems should be introduced.

18.1.6 Employees or contractors that use personal devices to connect to the Council's corporate network must verify that their device is set to automatically install operating system and application updates and patches without requiring their intervention.

18.1.7 Wherever relevant, any webservers used by the Council to host publicly available content should have firmware, operating systems and application updates and patches set to automatically install. If automatic installation is not possible, installation should be managed by the Webserver administrator on monthly basis or within 7 days of being notified by a vendor of critical updates and 30 days of notification of important or lower rated updates.

19. Anti-Virus Policy

Anti-virus software should be a foundational element of any cyber risk management plan. Whilst it cannot be and should not be relied on as a silver bullet, it provides valuable protection against a wide range of malware.

The Council recognises that a next-generation, up to date anti-virus solution is a good way to both detect and prevent malware installation that can lead to further exploitation, loss of control, or damage to the organisation's digital assets.

This policy applies to all company-owned or leased hardware devices, and any external devices that are used by employees that connect to the Council's corporate network.

19.1 Anti-Virus Policy Requirements

19.1.1 All workstations, laptops and servers operating within the Council's corporate network that use the Microsoft Windows or Apple iOS and Android operating systems must have anti-virus software installed that is set to automatically update on a daily basis.

19.1.2 All workstations or laptops used by employees or contractors to remotely connect to the Council's corporate network that use the Microsoft Windows or Apple iOS and Android operating systems must have anti-virus software installed that is set to automatically update on a daily basis.

19.1.3 Anti-virus software must be installed on any Windows based SCADA or Telemetry system.

19.1.4 If available, and if deemed necessary by either senior management or the Incident Response Team, anti-virus software should be installed on any mobile device or tablet that connects to the Council's corporate network.

19.1.5 Users should not be able to disable the anti-virus software from operating or updating.

19.1.6 All notifications or alarms triggered by the anti-virus software must be reported immediately to the Incident Response Team.

20. Firewall Policy

Connecting corporate networks and employees to the Internet is an essential part of many aspects of modern business. Whilst Internet connectivity provides enormous benefits, it also introduces serious security risks.

Being able to control access through the point where corporate networks meet public networks, commonly referred to as the “gateway”, is essential to securing the digital assets of the business. An open, uncontrolled Internet gateway can be compared to a business operating with no front door.

The Council recognises that protecting the corporate network and the Council’s digital assets with an appropriately configured and managed firewall is essential to reducing the impact and likelihood of malicious activity occurring over and through the Internet gateway.

This policy applies to the IT department or external IT provider responsible for maintaining the Council’s IT infrastructure and all the Council’s employees and contractors.

20.1 Firewall Policy Requirements

20.1.1 The Council shall install and maintain a software or hardware firewall at any point where the corporate network connects to the public Internet.

20.1.2 The Council shall install and maintain a software or hardware firewall for any SCADA or Telemetry systems, where possible and appropriate.

20.1.3 The firewall firmware / software should be kept up to date by the IT department or an external IT provider on a regular basis or within 7 days of being notified by a vendor of critical updates and 30 days of notification of important or lower rated updates.

20.1.4 All firewalls should be configured to provide the minimum amount of access required to perform the business operations of the Council.

20.1.5 The firewall configuration / configuration file should be reviewed by an external IT provider / expert that was not responsible for the initial configuration to ensure that the configuration is correct and performing the desired and expected level of control.

20.1.6 All public facing firewalls should receive vulnerability and penetration testing at least once per year or after any significant reconfiguration.

20.1.7 All servers should activate software firewalls whenever they are available, subject to technical dependencies.

20.1.8 Wherever possible and available, software firewalls should be activated on workstations, laptops and other devices that are used by employees and contractors that are connected to the corporate network or directly to the Internet, subject to technical dependencies.

21. Incident Response Policy

Being able to respond to an incident in a timely and co-ordinated manner is essential to ensuring the organisation can remain operational and that potential and actual losses can be minimised.

The Council recognises that being prepared to respond to a cyber incident or disaster takes planning, coordination, clear guidance, timely access to information, the necessary resources and a team approach.

The Council's Incident Response Policy is intended to address the key elements that are required in the Council's Incident Response Plan and the responsibilities of the Incident Response Team and the Council's employees and contractors.

21.1 Incident Response Policy Requirements

21.1.1 The Council is to develop, implement and maintain an Incident Response Plan that will act as the central source of guidance on how to identify, manage and respond to all cyber related incidents and disasters.

21.1.2 An Incident Response Team must be identified and documented within the Incident Response Plan along with their role, responsibilities, and contact details.

21.1.3 The Incident Response Plan must include guidance on how to comply with any local laws relating to breach notifications.

21.1.4 All company employees and contractors should be educated in the Incident Response Plan and what their roles and responsibilities are in relation to identification, reporting and managing suspected cyber incidents or disasters.

21.1.5 The Incident Response plan should be reviewed on an annual basis to ensure all contact details are up to date and that any other required changes or updates can be made.

21.1.6 It is highly desirable that the Incident Response Plan be tested once per year by the Incident Response Team and any other relevant employees or contractors.

21.1.7 To support the Incident Response Team, logging should be enabled for SCADA and Telemetry systems with logs stored in a centralised location.

22. Policy Compliance

22.1 Compliance Measurement

The Chief Information Security Officer and Incident Response Team will verify compliance to this policy and the policies contained within through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

22.2 Exceptions

Any exception to the policy must be approved by the Chief Information Security Officer in advance and in writing.

22.3 Non-Compliance

An employee, contractor or external provider found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract.

Adopted by Council on 17 January 2024 by Resolution 0124/013.

Mark Crawley
Chief Executive Officer