END USER SECURITY POLICY

Date Adopted	***18th April 2024***		
Council Minute	***59/04/2024***		
Version	***Version 1***		
Policy Responsibility	***Corporate & Community Services***		
Review Timeframe	***Every 4 Years***		
Last Review Date	***April 2024***	Next Scheduled Review	***April 2028***

INTRODUCTION

Coolamon Shire Council's end user devices (e.g. desktop, laptops, tablets, USB memory sticks or mobile phones) are the primary sources of risk to the Coolamon Shire Council's sensitive information and business applications. Implementation of appropriate information security controls for end user devices can mitigate the risk to Coolamon Shire Council's information and IT systems. Consequently, end user protection is critical to ensuring a robust, reliable and secure Coolamon Shire Council IT environment. Failing to do so may result in an information security incident, causing financial or reputational loss to Coolamon Shire Council.

The purpose of this policy is to set forth acceptable usage norms for Coolamon Shire Council's end user computing resources and to provide guidance to end users on the proper use of these resources, including use of the Internet and BYOD (Bring your Own Device).

INTENDED AUDIENCE

The target audience of this document is all Coolamon Shire Council's councillors, employees (whether permanent, fixed or temporary), volunteers and any third party or sub-contractor that is provided with an electronic identity (e.g. a username and password) to access Coolamon Shire Council information services.

For the purpose of this policy, the term 'employee' or 'end user' includes all groups who have access to Coolamon Shire Council electronic resources. Electronic resources include, but are not limited to; personal computers (including laptops), convergent devices such as; tablets, smart phones, or servers, software, network access (including email, calendar, contacts and other related functions, other internal network resources and Internet access) and information stored on Coolamon Shire Council's systems that is kept or used on-site or off-site, whether before, during or after work hours and/or provided by or at the expense of Coolamon Shire Council.

SCOPE

This policy applies to information assets owned or leased by Coolamon Shire Council, or to devices that connect to the Coolamon Shire Council network or reside at Coolamon Shire Council sites. This policy applies to all end user devices and equipment issued by the Technology Department to Coolamon Shire Council staff, contractors or 3rd parties. It applies to all people using these devices and equipment in the Coolamon Shire Council's offices, off-site, at home, at a client's premises or at any other location; and/or in situations where you are representing Coolamon Shire Council or any of its subsidiaries or may otherwise be identified as a Coolamon Shire Council end user or associate.

END USER CONTROLS

1 User Access and Password Security

Users of Coolamon Shire Council's information systems are personally responsible for the use of their account, creating and protecting passwords that grant them access to resources and must:

- Select lengthy (within reason)
- Select complex passwords and avoid use of simple passwords such as the name of the service itself, your name, "PASSWORD";
- Use Multi-Factor authentication where possible;
- Change their password at first login;
- Change their password as soon as possible if they know or suspect that their account has been compromised;
- Keep passwords secure, and not reveal them under any circumstances;
- Don't reuse old passwords or passwords used for other purposes. E.g., social media, banking, etc;
- Not attempt to use any account other than their own;
- Not share their user account with other individuals.

Passwords must comply with Coolamon Shire Council password policies. Passwords must comply with the following requirements:

- Minimum Length – 8 Characters.
- Complexity – Must contain one capital letter, one lower case letter, one number and one special character (e.g. , ! %).
- Password History – 24 passwords are remembered and cannot be reused.
- Passwords must be changed every 180 days.
- Passwords must be at least a day old before they are allowed to be changed by the user.
- Passwords must not be re-used between different accounts.
- Multifactor Authentication must be used where available.
- Workstations are set to go to sleep after 10mins of inactivity.
- When users leave their desk they must lock or sign-out of the device to stop unauthorised access.

2. Data Storage, Destruction and Disposal

End users must store all Coolamon Shire Council data in the appropriate shared location as provided by Coolamon Shire Council.

End users must regularly manage documents in shared locations and delete files and folders that are no longer required.

Coolamon Shire Council IT retains the right to delete any personal media files stored in shared locations. The local storage of data on a personal device (e.g. laptops, desktops, mobile phones and tablets) will not be backed up, and the loss of any information (in the event of a device failure) will be the responsibility of the user.

End users must take secure backups of files stored locally on personal devices (such as laptops, desktops, mobile phones and tablets) that are not backed up and will not be recoverable in the event that a device is exchanged or a local storage fails or is erased.

Physical documents containing sensitive information must be shredded prior to disposal.

3. Removable Media

Use of unencrypted removable media (e.g. USB drives, external hard drives, CDs/DVDs) to store Sensitive, Confidential or Restricted information is prohibited.

The use of personally purchased removable media is not permitted for business use, unless explicitly authorised to do so by the ICT Support Officer or Executive Manager.

4. Email and Internet Security

End users are responsible for all electronic activities initiated by them (e.g. email, web browsing and application usage) and electronic content stored by them on Coolamon Shire Council IT assets.
End users should not use corporate email for personal use.
Coolamon Shire Council end users must not:

- Follow web-links or instructions provided by email, unless certain of their origin and function;
- Send Coolamon Shire Council's information through unauthorised messaging applications or social media platforms (e.g. WhatsApp, Facebook, etc.)
- Send messages or download content that support illegal or unethical activities;
- Change the security settings of their email software or Internet browser on a Coolamon Shire Council device (e.g. laptop, desktop);
- Send Sensitive, Confidential or Restricted information via unencrypted email
- Send emails containing passwords in clear text, or account information such as log-on ID and password combinations;
- Use corporate devices or identities to browse, search or interact with the dark web, such as those that require the Tor web browser.

5. Social Media Use

End users are trusted to act responsibly when using social media sites such as Facebook, Twitter, wikis, blogs, YouTube, and LinkedIn.

Coolamon Shire Council information must only be shared over official, authorised communication channels. Coolamon Shire Council information must not be shared on social media sites.

When accessing social media sites on Coolamon Shire Council computers or devices:

- End users may be subject to logging and monitoring checks;
- Access may be restricted to social media sites; and
- Inappropriate social media websites will be blocked.

When accessing or contributing on social media sites, end users must:

- Not place comments representing or giving the impression of representing Coolamon Shire Council, unless explicitly authorised to do so.
- Exercise good judgement when blogging or posting.
- Not post or view material that is illegal, obscene, defamatory, threatening, harassing, discriminatory, racist, or hateful to another person or entity.
- Be aware that information hosted on social media is unverified and must not be used without confirming its authenticity for decision making.

Coolamon Shire Council information must not be sent via unauthorised messaging platforms based on its classification and sensitivity (e.g. WhatsApp, Facebook Messenger, WeChat, etc.) and must only be transmitted using Coolamon Shire Council approved and authorised messaging systems.

6. Mobile Computing Devices

In this policy, the term "Mobile Device" refers to an easily portable computing device. These devices can typically process and store information and have an ability to connect to a network. The most common Mobile Devices are laptops, tablets, smartphones and wearables.
Mobile Devices are designated as either "Coolamon Shire Council Owned" or "Privately Owned or BYOD".

Personal devices or BYOD devices are to only be used where controls have been implemented to manage Coolamon Shire Council Information on such devices, e.g. information storage policies, Mobile Device Management (MDM) software etc.

Only authorised devices are permitted for professional use. Only the owner of the device may be permitted to use approved BYODs to access Coolamon Shire Council's resources. Users must not grant access to their devices to unauthorised individuals.

The end user or the owner of the mobile device must:

- Allow Coolamon Shire Council to install Coolamon Shire Council's mobile device management software onto his/her device.
- Employ reasonable physical security measures for the mobile device and is expected to secure it whether or not it is actually in use or being carried.
- Inform Coolamon Shire Council, upon termination of employment, of any approved mobile devices contract or agreement, to be submitted for inspection prior to departure, if required.

To ensure the integrity and security of our information system and assets, the following requirements must be observed with respect to the use of all Mobile devices.

- Mobile Device Management software should be installed and enabled and must not be removed or tampered with. This software enables the IT department to enforce minimum security features on mobile devices.
- Mobile devices must not be used to store unencrypted passwords. To ensure security of Coolamon Shire Council systems, encryption should be applied (for example, through an encrypted password management application).
- Mobile devices should never be used to store sensitive information, such as health information about clients.
- Mobile devices carrying confidential Coolamon Shire Council information must not be left unattended and should be physically secured.
- Mobile devices must not be used to store pirated software or illegal content.
- Users must not bypass access controls on device operating systems added by suppliers.
- Mobile device use should be in accordance with all relevant laws, including road traffic laws (which place restrictions on the use of mobile devices while driving) and work health and safety laws. For the avoidance of doubt, Coolamon Shire Council will not pay for any fines imposed due to breach of laws.

In the event a device is lost or stolen, end users or device owners must report the incident immediately.

In an event of loss, theft or sale of a mobile device, Coolamon Shire Council's IT team must remotely wipe the device and/or Coolamon Shire Council corporate information that may be stored on it.

Where possible, if end users are required to work outside of usual hours of business, or outside of their usual place of business, they should do so on Coolamon Shire Council's systems. However, if an end user is required to perform work on a BYO device (e.g. staff owned and operated, personal computers, laptops, tablets, personal digital assistants, and other mobile devices) they should ensure that:

- The personal device has adequate virus protection; and
- No confidential information or data is stored on the personal device, and any data created, formed, or stored on the personal device is deleted once it is no longer required by the end user for their work function;

7. Remote access

When working from home or at an offsite location, end users:

- Must never provide their login or email password to anyone, not even family members;
- Must keep conversations confidential. Don't discuss work issues where others may hear, including elevators and lobbies;
- Must not use personal email or cloud storage accounts for work;
- Must make sure their home WiFi is password protected;
- Must always lock laptop screen before stepping away — and use a laptop lock if in an unsecured area.

8. System and Network Security

Coolamon Shire Council end users must not:

- attempt to compromise the security of a computer;
- access data, a server, or an account for any purpose other than for Coolamon Shire Council duties or business, even if access is authorised, unnecessary access is prohibited;
- export software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question;
- introduce malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc.);
- reveal account passwords to others or allow use of individual accounts by others. This includes family and other household members when work is being done at home;
- use a Coolamon Shire Council system / 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;
- make fraudulent offers of products, items, or services originating from any Coolamon Shire Council account;
- breach security controls or disrupt network communication (except for IT or security staff responsible for maintenance and troubleshooting). For the 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;
- port scanning or security scanning is expressly prohibited with the exemption of the IT team;
- execute any form of network monitoring that will intercept data not intended for the end user's host, unless this activity is a part of the end user's normal job/duty;
- circumvent user authentication or security of any host, network, or account;
- introduce honeypots, honeynets, or similar technology on the Coolamon Shire Council network (with the exception of the Security team or equivalent);
- interfere with or deny service to any user other than the Coolamon Shire Council's host (for example, denial of service attack);
- use any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the internet/intranet/extranet'
- provide information about, or lists of, Coolamon Shire Council end users to parties outside Coolamon Shire Council unless already classified as "public", and;
- Attempt to attach any unauthorised device to the Coolamon Shire Council business network.

9 Security Incident Reporting

Security Incidents are adverse events which pose a threat to Coolamon Shire Council's information systems and services. Security incidents can originate from intentional (deliberate actions against an information system) or unintentional actions (human error).

Examples of potential security incidents include abnormal computer behaviour, which may be caused by a computer virus, malware, worm, a non-escorted guest, disclosure of information to a unauthorised person, lost or stolen physical access cards, removable media, laptops and passwords and unauthorised access to an information system or physical premise.

In case Coolamon Shire Council's end users observe any unfamiliar activity on their workstation, they shall immediately disconnect the system from the network and report the incident to the IT service desk or their immediate supervisor (or equivalent). The following steps enumerate the actions to be taken by end users on encountering an incident:

- Immediately report any unfamiliar activity or suspected security incident to the Coolamon Shire Council's IT service desk on email IT@coolamon.nsw.gov.au
- End users shall comply with the directions given by the IT service desk to facilitate a quick response, repair of the system, restoring the service and analysis of the incident.

End users must not:

- Perform an action (e.g. delete system files) to eradicate or contain a suspected security incident unless explicitly instructed by the Coolamon Shire Council's IT service desk or security team; and
- Disclose information relevant to security incidents to unauthorised entities.

10 Copyright and Intellectual Property

When using Coolamon Shire Council or own devices, networks or storage media Coolamon Shire Council's end users must not:

- Store, transmit, or make available unauthorised copies of copyrighted material using Coolamon Shire Council resources or IT systems; or
- Use peer-to-peer file transfer services or take actions likely to promote or lead to copyright infringement.

When using Coolamon Shire Council's resources and IT systems, end users must:

- Only use licensed software officially installed/registered and owned by Coolamon Shire Council;
- Only use the applications to which they have authorised access;
- Comply with the terms of license signed by Coolamon Shire Council for software programs, online databases, online software packages, etc.
- Ensure copyright material is only retrieved, copied or used with the permission of the copyright owner under the terms of a copyright licensing agreement, or as permitted by law.

Coolamon Shire Council end users must not:

- Install or use any unauthorised software;
- Make/use illegal copies of licensed software;
- Use software that they suspect to be unlicensed; or download, copy, store, transmit, and stream material such as music, video, movie, or other copyrighted files without the express permission of the copyright holder or as permitted by law.

POLICY GOVERNANCE

Policy Enforcement

Each member of staff is expected to fully comply with this policy. If there is any failure to observe the policy, disciplinary measures may be taken. The measures taken will vary according to the breach and the circumstances of the breach. However, the right is reserved to immediately terminate the employment of any staff member who is in serious breach of this policy.

Handling Exemptions

The control exception process allows Coolamon Shire Council's end users (where technological or operational constraints or a legitimate business requirement exists) to request an exception from a defined control within this Policy. Exemptions requests must be reviewed and assessed by the ICT Support Officer and approved by the Executive Manager. All control exemptions must be documented with a rationale and reported to the Executive Manager. Control exemptions are to be reviewed on a periodic basis.

ASSOCIATIONS & RELATIONSHIPS

Legislation	
Policies	
Procedures/Protocols, Statements, Documents	

REVIEW

This policy may be reviewed at any time or as required in the event of legislative changes. Unless otherwise required the policy will be reviewed at least once during a term of Council.

Version 1 Adopted: Council Meeting held 18 April 2024 (Minute No. 59/04/2024)