# CYBER SECURITY POLICY

## 16.16.01

## 1. BACKGROUND

Cyber Security is the practice of protecting digital assets and data from malicious attacks. It includes network security, application security, information security, operational security, as well disaster recovery and business continuity.

Weddin Shire Council (Council) has a responsibility to maintain the integrity and security of its data and the security of internal and internet facing digital assets and networks. This ensures that internal and public resources and services are accessible at all times

Council has prepared this policy to develop a standard in which Council operates in order to ensure the security, integrity, and uptime of its devices.

## 2. PURPOSE

The purpose of this Cyber Security Policy is to provide the users (employees, Councillors, consultants, contractors, volunteers, work placement students or any other persons) who use Council's Information and Communications Technology (ICT) resources with a comprehensive policy of the digital assets that require protection, as well as outlining the various threats that may jeopardise our security.

These threats include but are not limited to malware, ransomware, denial of service, hardware failure or data corruption, and compromise of computer systems by attackers.

Additionally, this policy will provide clear rules and controls for safeguarding these assets and protecting Council. This policy aims to ensure that Council complies with the requirements set forth in the NSW Cyber Security Policy and the Cyber Security Guidelines for Local Government issued by the Office of Local Government.

By adhering to this policy, users can play an active role in safeguarding Council's digital assets and data, and contribute to creating a culture of cyber security awareness and best practices.

## 3. POLICY OBJECTIVES

The objectives of this Policy are to:

- Comply with the NSW Cyber Security Policy and the Cyber Security Guidelines for Local Government issued by the Office of Local Government (OLG Guidelines).
- Provide guidance on the acceptable use of devices and online materials.
- Outline the type of business information that can be shared and how it can be shared.
- Outline rules and controls for securing Council's digital assets.

- Outline activity Council monitors in order to maintain the security of our digital assets.

## 4. LEGISLATION

Council and its employees have a responsibility to comply with relevant laws when using Council ICT assets. Council must also comply with relevant legal provisions when monitoring or enforcing requirements set in the policy.

This policy relates to the following legislation:

- *Privacy Act 1988*
- *Security of Critical Infrastructure Act 2018* (SOCI Act)
- *The Criminal Code Act 1995*
- *Local Government Act 1993*
- *State Records Act 1998* (NSW)
- *Weddin Shire Council Policy For Records Management*
- *Weddin Shire Council Information Services Usages Policy*
- *Weddin Shire Council Social Media Policy*
- *Weddin Shire Council CCTV Workplace Surveillance*
- *Workplace Surveillance Act 2005* (NSW)

## 5. APPLICATION/SCOPE

This Policy applies at all times to employees, Councillors, consultants, and contractors, volunteers, work placement students or any other persons who use Council's ICT resources.

Use includes sending and receiving electronic communications. Including email and text, accessing the internet, accessing Council network, use of desktops, laptops, portable devices, and access and use of all applications and data.

The Policy is supported with the Cyber Security Incident Response Management Plan and any other user procedures developed to support the Policy.

## 6. POLICY

### 6.1. Roles and Responsibilities

The following table outlines the roles and responsibilities of personnel. Noting that the positi…on titles may change, however, the responsibilities remain the same.

| Roles | Responsibility |
|---|---|
| The Elected Council | Council has the responsibility to consider draft local policies and the adoption of the local policy. This Policy also applies to Councillors and their own use of Council's ICT Resources. |

| Roles | Responsibility |
|---|---|
| General Manager | The General Manager is responsible for the overall control and implementation of the Policy. |
| Director Corporate Services | The Director Corporate Services is responsible for updating the Cyber Security Policy in line with legislative amendments and/or reviewing and updating as appropriate. They are responsible for implementing the Policy and ensuring compliance. |
| IT Officer/Team Leader Finance | The IT Officer and Team Leader Finance are responsible for the implementation of the Policy and the development of accompanying procedures. |
| MANEX | General Manager, Directors and HR Manager must be accountable for cyber security including risks, plans, reporting and meeting the requirements of the OLG Guidelines. |
| All Council employees, consultants, contractors and volunteers | All Council employees, consultants, contractors and volunteers are required to adhere to the Policy as a user of the digital assets. |
| General Public | The general public must act in accordance with this policy and abide by any determination made as a result of this policy. |

### 6.2. Risk Management Framework

Council must ensure cyber security in the Council's risk management framework and consider cyber security threats when performing risk assessments. This includes:

a) Validating that the policy and its supporting documents meets the Council's business goals and objectives.
b) Providing assurance regarding the effectiveness of cyber security controls.
c) Assisting to ensure the risk framework is applied in assessing cyber security risks and with setting of risk appetite.
d) Assisting the organisation in analysing cyber security risks.

### 6.3. User's Accountability

#### 6.3.1. Reporting Suspicious Items

Users must remain vigilant in identifying and reporting any suspicious or malicious emails or websites to IT immediately. This includes emails that may

contain malicious links, as well as websites that may maliciously attempt to collect login credentials, payment details, personal information, or financial data

To maintain the security of our network, Council has implemented email scanning and web filters. However, despite these measures, there is still a possibility that malicious content may slip through. This scanning allows Council to identify websites that a user has visited in order to undertake remediation

If users believe they may have opened a malicious email, file, or entered information into a malicious website, please contact Council's IT Officer or Team Leader Finance immediately. It is important to note that failure to report such incidents may compromise our organisation's security.

### 6.3.2. Handling of Data

Classify information and systems according to their business value. To ensure the confidentiality and security of data, it must be stored on Council's designated file server under the appropriate location. This will allow for efficient and authorised access to the data, while maintaining its security. The user can work from their local device however it is recommended that users operate from their U:\ drive and transfer to an appropriate location on the fileserver when completed. Data not stored on the fileserver or in the users U:\ drive will not be included in daily backups.

### 6.3.3. Sensitive Data

Sensitive data is any data that includes customer name, address, phone number, driver's licence number, password information, or biometric information. It also includes financial data, access credentials, proprietary information, trade secrets, acquisition plans, and supplier information. Sensitive data should be stored as per Council's Records and Management Policy.

It is prohibited to:

a) Store any sensitive data in personal cloud accounts, such as Dropbox, iCloud, or OneDrive.
b) Store any sensitive data on personal devices, including laptops, phones, or storage devices.
c) Forward emails, including those with or without sensitive data to any personal accounts or devices.

Users must not attempt to modify permissions to gain access to data.

When sharing sensitive data, it is important to ensure that it is undertaken in a secure and authorised manner. When sensitive sharing data externally:

a) Use a Council-approved cloud services where the data is properly encrypted, and access is restricted to authorised personnel only.

b) Share sensitive data via email using password protected zip files with the password being provided via a communication other than email.
c) Mark the file as Confidential before transmitting it to authorised personnel.

When printing sensitive data, the secure print function should be used to ensure that documents are not left unattended on a printer. This allows the User to start the print job once they arrive at the printer.

#### 6.3.3.1. Sharing of photographs of individuals, including children

When sharing photographs of individuals, including children, it is essential to exercise caution and ensure that proper approval has been obtained for any images that may be used commercially or on social media. Prior consent must be obtained from the subjects or their legal guardians before using their images for any commercial or promotional purposes.

To take photos of individuals for commercial or promotional purposes, the Media/Photo Consent and Release Form should be filled out and stored within Council's Record system.

### 6.3.4. Non-sensitive Data

It is preferable to share documents internally via links in email rather than emailing attachments directly. This practice ensures that the data is stored in a secure environment and that access to the data is restricted to authorised personnel only. It also helps prevent the unintentional distribution of attachments to the wrong parties. It also helps prevent the doubling up of files across the network.

Council reserves the right to change the user's password to access the information in the case that it is not stored in the appropriate network location. Failure to save on the network may also be subject to disciplinary action. Users handling data must exercise due diligence and caution when sharing such data to ensure its confidentiality and security.

All data generated or produced by employees while using Council-owned devices or systems given permission to use for work related purposes shall remain the sole property of Council. Such data includes, but is not limited to, documents, emails, reports, and any other digital content generated during the course of official duties.

Users are strictly prohibited from deleting or tampering with any Council data or files, unless authorised to do so as part of their regular duties or by a designated authority. The deliberate deletion of data without proper authorisation may result in disciplinary action, as it jeopardises the integrity of Council's information and may hinder critical operations. This includes files and emails.

If additional access to File Server resources are required, Users must fill in the Request to Access Folder Form and return to the Corporate Services Department (IT Officer).

#### 6.3.5. Email

To ensure Councils data integrity and users privacy, users are strictly prohibited from using Council email for personal purposes, including signing up for social media or subscribing to non-work-related items. Similarly, personal email must not be used for any Council-related purposes, such as sending or receiving work-related communications, sending Council data, or conducting official Council business.

Council email can be accessed via webmail on personal devices when approval has been granted. Under no circumstances should a user forward emails, including those with or without sensitive data to any personal accounts or devices.

#### 6.3.6. Lock Screens

Council mandates the use of automatic screen locks to prevent unauthorised access to devices when left unattended. Users must manually lock their screens before leaving their workstations (pressing Windows Key and L together).

Locking screen prevents unauthorised access to data by other Users who do not have the necessary clearance to view the data. It also reduces the risk of someone gaining unauthorised access to the network while masquerading as someone else.

Under no circumstances should a User attempt to do anything that would prevent their screen from being locked when left unattended. This includes any action that would disable or modify the automatic screen lock feature.

### 6.4. System Controls

#### 6.4.1. Website Filtering

Council implements web filtering in order to protect our network from website that may introduce a security risk such as malware or phishing. Software we use blocks websites based on categories recommended by our Security vendors. This filtering can inadvertently block websites that may be required for work purposes.

Filtering means that websites visited by a user are logged and can be reviewed by the Corporate Services Department in the case of security breach, suspected policy breach or in order to investigate a workplace incident.

To request a website be unblocked, Users must fill in the Request to Unblock Website Form and return to the Corporate Services Department (IT Officer). Websites will not be unblocked if a valid work case cannot be proven.

### 6.4.2. Removable Media

The use of USB storage devices is strictly limited to situations where it has been expressly authorised by a staff member's Team Leader/Manager or Director. This includes but is not limited to; USB sticks, SD Cards, CD\DVD, and External Hard Drives. In the event that a User needs to utilise portable removable media, it must first be scanned by IT before being plugged into any device.

In addition, Users should refrain from plugging in personal mobile phones, tablets, or other USB-chargeable devices into their workstation for charging purposes. To charge such devices, a suitable adapter must be utilised. Adapters for work related devices can be provided by IT upon request.

Council provided devices cannot be charged on public charging docks.

### 6.4.3. Software Installation

Installation of software is limited to approved applications that may be installed by IT exclusively from the Software file share. Prior to installation, all software programs must undergo a thorough vetting process that includes checksum verification and certificate authentication when applicable after downloading. It is important that all software is kept current with the latest versions for installation purposes.

Before IT can initialise any software install, the relevant staff member must obtain formal approval from their respective Team Leader/Manager or Director by filling in the Software Installation Request form.

### 6.4.4. Equipment Disposal

When equipment is no longer needed and is due for disposal, it must be returned to IT for proper disposal. This measure is necessary to ensure that all data contained within the equipment is securely erased, and the equipment is disposed of in an environmentally responsible manner.

It is essential to ensure that all disposed hardware is included in the Software and Hardware Register, which is maintained by IT. This register helps to keep track of all Council hardware assets and ensures that all hardware is accounted for during the disposal process.

### 6.4.5. Software and Hardware Register

To ensure the accountability of Council-owned devices, Council maintains a Software and Hardware Register. This register helps identify the location of

physical hardware and whom it is assigned to, while also allowing Council to identify software vulnerabilities on specific machines to streamline the software updating process.

Employees must only use Council devices for work purposes, even outside of work hours. The use of Council devices for personal reasons is strictly prohibited, as it increases the risk of cyber security incidents and compromises the integrity of Council data.

Employees are prohibited from swapping devices with other employees without obtaining prior approval from their respective Team Leader/Manager or Director and in consultation with the Corporate Services Department. Any such swap must be communicated to IT in order to update the register. If a new devices is assigned, the old devices must also be returned to IT and not given to another User without prior approval.

Upon termination of employment, end of a consultancy or contract, all portable devices must be returned to IT so they can be reset and reused, or disposed of in an appropriate manner. It is important to return all accessories including all cables and peripherals.

### 6.4.6. Device Storage

Portable devices including laptops, phones, tablets, must be stored securely and make use of lock screen passwords. Devices, other than work provided mobile phone should not be taken home unless approval is granted by their respective Team Leader/Manager or Director.

If taking a portable device on business or taking a device home; the device under no circumstances should be left unattended within a vehicle or in any other public area.

### 6.4.7. Software Update

Applying updates is critical to ensure the ongoing security of applications, drivers, operating systems and firmware. In doing so, it is important that patches or updates are applied consistently and in a secure manner.

Workstations are configured to patch Windows automatically whereas Servers are to be manually updated at the first convenience following a “Patch Tuesday”.

All employees are required to reboot their workstations at the first available convenience to install updates. Windows Updates will prompt users when updates have been downloaded and ready to install.

If a user has not scheduled a reboot and the device reboots automatically Council is not responsible for any data lost. It is on the user to ensure files are saved and the reboot will happen at an appropriate time.

### 6.4.8. Backups

Data backups should follow the 3-2-1 principle. That is; three backups, two on-site but on different media and at least one copy off-site.

Backups and are performed daily with incremental, full backups, and replications at various times of the day. At least one backup is offline meaning a backup disk must be rotated daily. IT or another authorised staff member should perform this rotation following correct procedure. This rotation is critical to ensuring that data can be restored in the event of a catastrophic incident such as ransomware or hard drive failure.

To maintain proper records, the backup drives must be labelled with the day of the week when they are intended for use. After rotation, backup drives must be stored securely in Council's safe. Backups disks are rotated daily on business days meaning there are five (5) days of previous backups.

### 6.4.9. Council WiFi

Council has two WiFi Networks for undertaking business. The Main Network allows access to network servers and resources and is to be used for staff only with council provided equipment. Council provided Mobile Phones and Tablets should not be connected to the Main Network, but instead be connected to the Guest Network.

The Guest Network is also available for visitors to the Council Office, Depot, or Community Hub if internet connectivity is required.

### 6.4.10. Public WiFi

If working remotely public WiFi must not be used. This can introduce security risks if the network is malicious or a malicious actor in on the network. Public WiFi should not be accessed from any Council device.

Council maintained networks (minus Library Guest network) and Users home networks are not considered to be Public WiFi and can be utilised if device has been approved for use at home.

### 6.4.11. Computer Surveillance Records

Council reserves the right to carry out computer surveillance of any user at any such time that Council chooses without further notice to any user. Council is able to access the following at any time without further notice to any user:

- Storage volume and hard drive storage
- Website History
- Downloaded volumes
- Suspected malicious code

- Emails and text messages – for Council supplied devices including deleted items from backup/achieve.
- Mobile phone telephone records – for Council supplied devices.

Council retains logs, backups and archives related to these activities. These records are property of Council and are subject to State and Federal Laws and may be used as evidence in legal proceedings, or in workplace investigations into alleged misconduct.

### 6.5. Work From Home

#### 6.5.1. Remote Access

Virtual Private Networks (VPN) Remote Access is granted to users who require connection to internal services and data when they are outside the office or working from home. During the VPN configuration, the User will be required to download a software two-factor authentication app. This supplies a rolling code when a user signs into the VPN. This code should be treated in the same regard as your password. A personal device can be utilised for the purpose of generating 2FA codes.

Under no circumstance should you allow any other member of staff to use your credential in order to access the network remotely. Approval for VPN can be obtained by seeking approval from their respective Team Leader/Manager or Director by filling in the VPN Access Request form.

VPN access is only to be used on Council provided devices unless other approved by a users respective Team Leader/Manager or Director

### 6.6. Employee Terminations

When an employee is leaving the Council, whether through their resignation or immediate action, it is important to revoke their access to systems and accounts at the completion of their final workday. This includes disabling domain logins, email access, and remote access, all while ensuring that this action does not hinder their ability to complete their work prior to departure. This serves to restrict access once their employment with the Council ends. A procedure has been established to ensure a thorough offboarding process for Users of Councils Digital Assets.

### 6.7. Procurement

Where applicable, cyber security requirements are built into procurement. For example in the transmission of a contractor’s or consultant’s data shared with Council or vice versa.

### 6.8. Awareness and Training

Council is required to implement regular cyber security awareness training for its users. Increase awareness of cyber security risks for all users and including the

need to report cyber security risks. At a minimum, this policy, the Cyber Security Incident Response Plan and its procedures should be a reviewed every 12 months.

New Council employees will be inducted into Council's Cyber Security Policy and its procedures as part of their induction process.

## 7. DEFINITIONS

| Key Terms | Meaning |
|---|---|
| Council | Weddin Shire Council |
| Cyber Security | The practise of protecting devices, user accounts, and data from malicious attacks. |
| Sensitive Data | Any data that includes customer name, address, phone number, driver's licence number, password information, or biometric information. It also includes financial data, access credentials, proprietary information, trade secrets, acquisition plans, and supplier information. |
| Devices | Any computing device including Desktops, Laptops, Tablets and Phones. |
| Malicious Actor | An individual or group who may attempt to gain unauthorised access to computer systems or network for malicious purposes. |
| Patch Tuesday | Term for when Microsoft, Adobe, and Oracle release updates for their products. Due to time zone differences, it occurs in Australia on the Wednesday following the second Tuesday of the month. |
| Peripherals | A component that can be added to a device in order to increase its capabilities. Peripherals include keyboards, mice, printers, scanners, external hard drives, webcams, monitors, speakers, and USB flash drives. |
| Threat | Any potential event, action, or circumstance that has the capability to exploit vulnerabilities in computer systems, or networks, leading to harm, damage, or unauthorised access. |
| Users | Council employees, Councillors, consultants, contractors, volunteers, and work placement students. |

| **Title: Cyber Security Policy** | | |
|---|---|---|
| **Department: Corporate Services** | | |
| **Version** | **Date** | **Author** |
| 0.1 | Draft | Josh Dawes |
| 1.0 | 16 November 2023 | Adopted Resolution 257/23 |
| | | |
| This policy may be amended or revoked at any time and must be reviewed at least annually since its adoption (or latest amendment). The Director Corporate | | |

| | | |
|---|---|---|
| Services will be responsible for the review of this policy. Review of this policy will incorporate relevant legislation, documentation released from relevant state agencies and best practice guideline.<br><br>**Review Date: 16 November 2024** | | |
| **Amendments in the release** | | |
| **Amendment History** | **Date** | **Detail** |
| | | |
| | | |
| | | |
| **Annexure Attached:** | | |
| **Noreen Vu**<br>**General Manager** | | |