CYBER SECURITY POLICY

CYBER SECURITY POLICY

TABLE OF CONTENTS

1. INTRODUCTION

The Water Industry Operations Association of Australia (WIOA) is committed to implementing robust protective measures to effectively manage external threats that may compromise the integrity of the organisation's systems and to safeguard against potential harmful actions from external parties.

2. POLICY STATEMENT

This policy outlines the principles for developing, implementing, and upholding measures that safeguard the organisation's cyber assets. These assets encompass computer equipment, software, operating systems, storage media, electronic data, and network accounts. The objective is to prevent any form of exploitation or misuse that could compromise the organisation's cybersecurity.

3. APPLICABILITY

This policy applies to:

- All employees, contractors, volunteers, and others undertaking work at WIOA,
- Visitors to the office and various workplaces or participating in authorised WIOA activities including all personnel affiliated with third parties, and
- To all equipment owned or leased by the WIOA, and to all equipment authorised by the WIOA for the conduct of the organisation’s business.

4. CONTEXT

WIOA aims to provide a reasonable level of personal privacy for its users. However, it is essential for users to acknowledge that the data they generate on WIOA’s systems remains the property of WIOA. Due to the imperative need to safeguard WIOA’s network, the confidentiality of information stored on any network device owned by WIOA cannot be guaranteed. As a precautionary measure, WIOA reserves the right to conduct periodic audits of networks and systems to ensure compliance with this policy.

Information held by the organisation will be categorised into different levels of confidentiality. Particularly sensitive information will be granted special protection.

Employees and volunteers are obligated to observe all necessary cybersecurity procedures diligently. This includes safeguarding passwords, ensuring secure access to computers, and maintaining protective software.

Any breach of this policy by an employee may result in disciplinary action, ranging from warnings to potential dismissal.

5. RESPONSIBILITY OF CHIEF EXECUTIVE OFFICER (CEO), EMPLOYEES, VOLUTEERS, ETC

All employees have responsibility for cyber security, but specifically:

a) The CEO bears the responsibility of ensuring:

- Staff members are informed and acquainted with this policy
- Appropriate actions are taken to address any breaches of this policy brought to the attention of management
- Appointment of a competent cyber security officer. For WIOA is will be our I.T support, Compusult 63 Wyndham St, Shepparton

b) The Cyber Security Officer holds the responsibility of:

- Keeping the CEO informed about any alterations in the organisation's cyber security requirements
- Submitting an annual report on the organisation's cyber security to the board

c) All employees and volunteers are responsible for:

- Familiarising themselves with the cyber security policy and procedures
- Ensuring that their use of cyber media adheres to this policy

In case of any uncertainty or ambiguity regarding the requirements of cyber security policies or procedures in a particular instance, employees and volunteers are encouraged to consult their respective supervisors.

6. LEVELS OF CONFIDENTIALITY

From time to time WIOA should issue cyber security procedures appropriate to different levels of confidentiality.

The Association shall classify the information it controls in the organisation's computer system files and databases as either non-confidential (open to public access) or confidential (in one or many categories).

The cyber security officer is required to review and approve the classification of the information and determine the appropriate level of security that will best protect it.

SYSTEM TAXONOMY

SECURITY LEVEL	DESCRIPTION	EXAMPLE
RED	This system contains confidential information – information that cannot be revealed to personnel outside the company. Even within the company, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life-threatening consequences and/or an adverse financial impact on the business of the company.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information
GREEN	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access server and application(s). Management workstations used by systems and network administrators.
WHITE	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
BLACK	This system is externally accessible. It is isolated from RED and GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public web server with non-sensitive information.

DATA TAXONOMY

Our I.T Provider if required to store credit card details, drivers licenses etc, will then elevate their storage requirements.

7. ACCESS CONTROL AND COMPUTERS

Access to the organisation's digital resources is governed by a system of user permissions based on role and security clearance levels. Each team member will have access only to the data and systems required for their specific responsibilities. To enhance security, identity and access management protocols are enforced, including secure login procedures and multifactor authentication (MFA) for sensitive systems where available.

Password Management

All users are responsible for securing their login credentials. Passwords must be unique and adhere to established complexity standards. Use of password management tools is recommended to securely generate and store passwords. Sharing login credentials is prohibited, and users must ensure that no unauthorised individuals can access their accounts.

Inactivity and Screen Locking

To safeguard unattended devices, all workstations, PCs, and laptops must automatically activate a screen lock after 10 minutes of inactivity. Alternatively, users should lock or log out of devices when not in use.

Password Update Protocol

To maintain account security, passwords should be managed securely, with a strong preference for unique, complex passwords generated and stored within an approved password manager. Regular password changes are typically not required unless there is evidence of compromise or unauthorised access. When properly managed, passwords can remain stable to reduce the risk of forgotten credentials and user error associated with frequent changes.

For accounts without multi-factor authentication (MFA), or where password managers are not used, periodic password changes may still be necessary to maintain security standards. Account lockouts will occur automatically after five unsuccessful login attempts to prevent unauthorised access. If users require assistance with a locked account or suspect any password compromise, they should immediately contact IT support.

Restricted Access and Monitoring

Access to sensitive files and administrative functions is tightly controlled. User attempts to access restricted files or areas are monitored, and any unauthorised attempts will be flagged for security review. System administrators are assigned unique, elevated access credentials, issued upon request and approval, and must adhere to the same security protocols as user-level accounts.

Device Security

All devices connected to the organisation's network must have up-to-date antivirus software, firewalls, and security patches. Access logs and device connections will be reviewed periodically to ensure compliance and detect any unusual activity.

Our membership data is stored in our **membership CRM**, Mition.

The platform is serverless, edge technology, which shields all the WIOA client portal and data, and is protected by Microsoft built in Denial of Service tools which are always being refined. Mition continues to use the latest version of core OS/Software versions.

Captcha has recently been added (I am not a robot) to any Forms in Mition as well.

Two Factor Authentication (2FA) is now in place for all users and required every 30 days.

8. CYBER SECURITY INCIDENT RESPONSE

The CEO is responsible for an incident response plan to prepare for and respond to a cyber incident. An annual scenario plan workshop should be conducted, with all staff, outlining the steps to follow should an incident occur. Steps to include:

8.1 PREPARE & PREVENT

- Ensure all staff follow the cyber safe policy and procedures to help employees understand how to prevent an attack and to identify potential incidents
- At scenario planning identify the assets that are important to the business – financial, information and technology assets
- Consider the risks to these and the steps to take to reduce the effects of an incident
- Create roles and responsibilities so everyone knows who to report to if an incident occurs, and what to do next

8.2 CHECK AND DETECT

All staff need to check and identify any unusual activities that may damage the business information and systems. Unusual activity may include:

- Accounts and your network not accessible
- Passwords no longer working
- Data is missing or altered
- Your hard drive runs out of space
- Your computer keeps crashing
- Your customers receive spam from your business account
- You receive numerous pop-up ads

If staff encounter a security incident, they need to document any evidence (e.g., take screen shots) and report it to the IT Administrator and CEO immediately

8.3 IDENTIFY AND ASSESS

- Find the initial cause of the incident and assess the impact so you can contain it quickly
- Determine the impact the incident has had on your business
- Determine its effects on your business and assets if not immediately contained

8.4 RESPOND

- Limit further damage of the cyber incident by isolating the affected systems. If necessary, disconnect from the network and turn off the computer to stop the threat from spreading
- Remove the threat
- Recover from the incident by repairing and restoring your systems to business as usual

8.5 REVIEW

- Identify if any systems and processes need improving and make those changes
- Evaluate the incident before and after, and any lessons learnt
- Update your cyber security incident response plan based on the lessons learnt so you can improve your business response

9. MONITORING, EVALUATION, AND REPORTING

The Chief Executive Officer is responsible for monitoring and evaluating the implementation and effectiveness of this policy and for reviewing this policy as required.

10. LAST UPDATED

Approval and Review

Lead Author	CEO
Approver	WIOA Board
Date endorsed	November 2024
Date reviewed	November 2024
Timeframe for next review	12 months