





**Murrumbidgee**  
COUNCIL

---

## Cyber Security Policy

	Name	Position	Signature	Date
Responsible Officer	Kaitlin Salzke	Chief Financial Officer		14 September 2023
Authorised By	John Scarce	General Manager		14 September 2023

<b>Document Revision History</b>	
Date adopted by Council:	12 September 2023
Minute Number:	146/09/23
Next Review:	See item 7 of this Policy
Revision Number:	
Review Date:	
Date adopted by Council:	
Minute Number:	
Next Review:	
Revision Number:	
Review Date:	
Date adopted by Council:	
Minute Number:	

September 2023

# Contents

1. Purpose	.....	3
2. Related Policies	.....	3
3. Roles and Responsibilities	.....	3
4. Foundational Requirements	.....	5
5. Cyber Incidents	.....	6
6. Penetration Testing	.....	6
7. Review	.....	6
Annexure 1	.....	7

## 1. Purpose

The purpose of this policy is to document the cyber security policy and framework adopted by Murrumbidgee Council (Council) to manage and improve its resilience to cyber threats.

Cyber threats come in a variety of forms and continuously evolve, therefore the approach to cyber security needs to cover multiple fronts and be flexible to evolve around both business requirements and threats.

Covered within the framework is the general approach of preventing threats through system controls, managing incidents when they occur, and education of staff.

## 2. Related Policies

This policy should be read in conjunction with the following policies:

- *Communication Devices, Internet and Intranet Policy*, which documents Council's requirements and expectations regarding the use of its communications devices (including password requirements, use of multi-factor authentication, etc.);
- *IT Security Policy*, which documents the high-level requirements that Council expects from its ICT systems to ensure information is being protected appropriately;
- *Access Control Policy*, which documents the mechanisms for appropriately controlling and restricting access to information and systems to ensure individuals are provided the right access at the right time for their role.

## 3. Roles and Responsibilities

This section outlines the roles and responsibilities that Council has allocated as part of its cyber security function.

The **General Manager** is responsible for:

- Appointing or assigning an appropriate senior staff member with the authority to perform the duties outlined in this policy;
- Supporting Council's cyber security plan;
- Ensuring Council develops, implements and maintains an effective cyber security plan;
- Determining Council's risk appetite;
- Appropriately resourcing and supporting cyber security initiatives, including training and awareness and continual improvement initiatives to support this policy.

The **Executive Team** is accountable for cyber security, including risks, plans, reporting, and meeting the requirements of the *Cyber Security Guidelines – Local Government* released by Cyber Security NSW.

The **Chief Financial Officer** is responsible for:

- Defining and implementing a cyber security plan for the protection of Council's information and systems;
- Developing a cyber security strategy, architecture and risk management process, and incorporating these into Council's current risk framework and processes;
- Implementing a cyber security plan that includes consideration of threats, risks and vulnerabilities that impact the protection of the organisation's information and systems within the organisation's cyber security risk tolerance;
- Assessing and providing recommendations on any exemptions to organisation information, security policies and standards;
- Attending Audit, Risk & Improvement Committee meetings;
- Managing the budget and funding for the cyber security program.

The **Manager, Corporate and Community Services** is responsible for:

- Implementing policies, procedures, practices and tools to assist with the implementation of Council's cyber security framework;
- Building cyber incident response capability;
- Collaborating with privacy, audit, information management and risk officers to protect Council information and systems;
- Ensuring that consultants, contractors, and outsourced service providers understand the cyber security requirements of their roles;
- Ensuring all staff and providers understand their roles in building and maintaining secure systems;
- Monitoring and enforcing the compliance of Council's managed service provider with Council's cyber security requirements.

The **People & Culture Officer** is responsible for:

- Establishing training and awareness programs to increase employees' cyber security capability;
- Ensuring that all staff understand the cyber security requirements of their roles.

The **Records Officer** is responsible for:

- Acting as a focal point within Council for all matters relating to information management that are required to support cyber security;
- Ensuring that a cyber incident that involved damage or loss is escalated and reported to Council's IT Managed Service Provider and Executive team.

Council's **IT Managed Service Provider** (with the support of Council's Chief Financial Officer and Manager, Corporate & Community Services) is responsible for:

- Investigating, responding to, and reporting on cyber security events;
- Reporting cyber incidents to the General Manager and Cyber Security NSW, if appropriate;

- Ensuring a secure-by-design approach for new initiatives and upgrades to existing systems, including legacy systems;
- Managing and coordinating the response to cyber security incidents, changing threats and vulnerabilities;
- Developing and maintaining cyber security procedures and guidelines;
- Providing guidance on cyber security risks introduced from business and operational change;
- Managing the life cycle of cyber security platforms including design, deployment, ongoing operation and decommissioning;
- Ensuring appropriate management of the availability, capacity and performance of cyber security hardware and applications;
- Providing input and support to regulatory compliance and assurance activities and managing any resultant remedial activity;
- Developing a metrics and assurance framework to measure the effectiveness of controls;
- Providing day-to-day management and oversight of operational delivery.

Council's **Audit, Risk & Improvement Committee** is responsible for:

- Validating that the cyber security plan meets Council's goals and objective, and ensuring the plan supports the Council's cyber security strategy;
- Providing assurance regarding the effectiveness of cyber security controls;
- Assisting to ensure the risk framework is applied in assessing cyber security risks and with setting of risk appetite;
- Assisting Council staff in analysing cyber security risk.

#### **4. Foundational Requirements**

Council will work towards implementing the Foundational Requirements set out in the *Cyber Security Guidelines – Local Government* released by Cyber Security NSW (annexed to this policy). Staff will complete the *Self-Assessment (Basic) template* report on at least an annual basis and provide it to the Executive team and Audit, Risk & Improvement Committee for review. Resolving unmet requirements will form the basis of Council's cyber security improvement plan.

These foundational requirements encompass:

- Implementing cyber security planning and governance;
- Building and supporting a cyber security culture across the organisation;
- Managing cyber security risks to safeguard and secure information and systems;
- Improving resilience, including ability to rapidly detect cyber incidents and respond appropriately.

Implementation of the *Essential Eight* (a series of prioritised mitigation strategies designed by the Australian Cyber Security Centre to help organisations protect themselves against various cyber threats) is also incorporated within these foundational requirements.

## 5. Cyber Incidents

A *cyber incident* is an occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.

Notification and information retention requirements in the event of a cyber security incident are set out in Council's *Communication Devices, Internet and Intranet Policy*.

Once a report is received, the following process will be followed:

1. *Investigate*: Investigate reports to determine whether a breach has occurred, as well as the scope, impact and severity of the incident.
2. *Isolate*: Take appropriate action to isolate impacted systems until a resolution can be applied.
3. *Eradicate & Recover*: Develop a plan for eradicating any threat and repairing damage caused. Consideration will be given to implementing relevant components of Council's *IT Business Continuity Subplan*, managed and maintained by Council's IT managed service provider.
4. *Review*: Conduct a review of the event to determine whether it was a reportable event, and identify any improvements that could be made to the response plan or layers of defence.

It is noted that Council's IT Managed Service Provider also has reporting requirements in the event of a cyber incident.

Council's IT Managed Service Provider also conducts a security check and review of logs as part of its monthly processes, and maintains logging of events through its ticketing system. It is not proposed to implement an additional register at this time.

## 6. Penetration Testing

Council will conduct penetration testing on at least a biennial basis, or when there are major changes to Council's information systems.

## 7. Review

This Policy:

- To be reviewed within the first year of the new Council term
- May be reviewed and amended at any time at Council's discretion (or if legislative or State Government policy changes occur)

This Policy has been drafted with reference to the *Cyber Security Guidelines – Local Government* released by Cyber Security NSW, and should be reviewed with reference to those guidelines.

## Annexure 1

### Foundational Requirements (extract from Cyber Security Guidelines - Local Government)

#### 6. Foundational Requirements

Outlined below are foundational requirements that focus on enhancing planning and governance, developing a cyber security culture, safeguarding information and systems, strengthening resilience against attacks and improved reporting.

	LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
<b>1</b>	Councils should implement cyber security planning and governance. Councils should:					
<b>1.1</b>	Allocate roles and responsibilities as detailed in the Guidelines.					
<b>1.2</b>	Ensure there is a governance committee at the executive level or equivalent (dedicated or shared) to be accountable for cyber security including risks, plans, reporting and meeting the requirements of the Guidelines.					
<b>1.3</b>	Develop, implement and maintain an approved cyber security plan that is integrated with your organisation's business continuity arrangements.					
<b>1.4</b>	Include cyber security in their risk management framework and consider cyber security threats when performing risk assessments.					
<b>1.5</b>	Be accountable for the cyber risks of their ICT service providers with access to or holding of government information and systems and ensure these providers understand and comply with the cyber security requirements of the contract, including the applicable parts of the Guidelines and any other relevant organisational security policies.					
	LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
<b>2</b>	Councils should build and support a cyber security culture across their organisation. Councils should:					
<b>2.1</b>	Implement regular cyber security awareness training for all employees, contractors and outsourced ICT service providers.					
<b>2.2</b>	Increase awareness of cyber security risk across all staff including the need to report cyber security risks.					
<b>2.3</b>	Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied.					
<b>2.4</b>	Ensure that appropriate access controls and security screening processes are in place for people with privileged access or access to sensitive or classified information.					
<b>2.5</b>	Receive and/or provide information on security threats and intelligence with Cyber Security NSW and cooperate with NSW Government to enable management of government-wide cyber risk.					

LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
<b>3</b>	Councils should manage cyber security risks to safeguard and secure their information and systems. Councils should:				
3.1	Implement an Information Security Management System (ISMS), Cyber Security Management System (CSMS) or Cyber Security Framework (CSF).				
3.2	Implement the ACSC Essential Eight <sup>3</sup> .				
3.3	Classify information and systems according to their business value (i.e. the impact of loss of confidentiality, integrity or availability).				
3.4	Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects. Any upgrades to existing systems must comply with your organisation's cyber risk tolerance.				
3.5	Audit trail and activity logging records are determined, documented, implemented and reviewed for new ICT systems and enhancements.				
LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
<b>4</b>	Councils should improve their resilience including their ability to rapidly detect cyber incidents and respond appropriately. Councils should:				
4.1	Have a current cyber incident response plan that integrates with the agency incident management process and the <i>NSW Government Cyber Incident Response Plan</i> .				
4.2	Exercise their cyber incident response plan at least every year.				
4.3	Ensure that ICT systems and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.				
4.4	Report cyber security incidents to their CISO and/or Cyber Security NSW. If relevant, ensure incident reporting is compliant with Federal reporting requirements.				

## 7. The Essential Eight

The ACSC recommends that organisations implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems. Please check the ACSC website for the latest version of the Essential Eight and maturity model<sup>4</sup>.

<sup>3</sup> Strategies to Mitigate Cyber Security Incidents: <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained>

<sup>4</sup> <https://www.cyber.gov.au/acsc/view-all-content/essential-eight>



The ACSC Essential Eight was refreshed on 12 July 2021. This update focused on using the maturity levels to counter the sophistication of different levels of adversary tradecraft and targeting, rather than being aligned to the intent of a mitigation strategy. The redefinition of a number of maturity levels will also strengthen a risk-based approach to implementation of the Essential Eight strategies. As the maturity model has been redefined and many requirements have changed, maturity assessments for the July 2021 model should not be directly compared to earlier versions of Essential Eight.

- FAQ: <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq>
- Essential Eight Maturity Model: <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model>
- Definitions: <https://www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-terminology>
- ISM: <https://www.cyber.gov.au/acsc/view-all-content/ism>

Mitigation Strategy	What	Why
Application control	Checking programs against a pre-defined approved list and blocking all programs not on this list	So unapproved programs including malware are unable to start and preventing attackers from running programs which enable them to gain access or steal data
Patch applications	Apply security fixes/patches or mitigations (temporary workarounds) for programs within a timely manner (48 Hours for internet reachable applications). Do not use applications which are out-of-support and do not receive security fixes	Unpatched applications can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems
Configure MS Office macro settings	Only allow Office macros (automated commands) where there is a business requirement and restrict the type of commands a macro can execute. Also monitor usage of Macros.	Macros can be used to run automated malicious commands that could let an attacker download and install malware
User application hardening	Configure key programs (web browsers, office, PDF software, etc) to apply settings that will make it more difficult for an attacker to successfully run commands to install malware	Default settings on key programs like web browsers may not be the most secure configuration. Making changes will help reduce the ability of a compromised/malicious website from successfully downloading and installing malware.

<b>Restrict administrative privileges</b>	Limit how accounts with the ability to administer and alter key system and security settings can be accessed and used.	Administrator accounts are 'the keys to the kingdom' and so controlling their use will make it more difficult for an attacker to identify and successfully gain access to one of these accounts which would give them significant control over systems
<b>Patch operating systems</b>	Apply security fixes/patches or temporary workarounds/mitigations for operating systems (e.g. Windows) within a timely manner (48 Hours for internet reachable applications). Do not use versions of an Operating system which are old and/or not receiving security fixes	Unpatched operating systems can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems
<b>Multi-factor authentication</b>	A method of validating the user logging in by using additional checks separate to a password such as a code from an SMS/Mobile application or fingerprint scan	Unpatched operating systems can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems
<b>Regular backups</b>	Regular backups of important new or changed data, software and configuration settings, stored disconnected and retained for at least three months. Test the restoration process when the backup capability is initially implemented, annually and whenever IT infrastructure changes.	To ensure information can be accessed following a cyber-security incident e.g. a ransomware incident).