Cyber / Information Security Policy

Date Adopted: 26 March 2024

Version: 1.0

Policy Objectives

We are committed to continuously improving our cybersecurity posture through regular reviews, updates to policies and procedures, and staying informed about emerging threats and best practices.

This cybersecurity policy reflects our dedication to maintaining a secure and resilient digital environment at Maitland City Council. Adherence to these principles is crucial to safeguarding the trust and confidence of our community and stakeholders. Everyone associated with Maitland City Council must adhere to cybersecurity best practices.

This policy will be periodically reviewed and updated to ensure its relevance and alignment with the evolving cybersecurity threat landscape and organisational objectives.

Policy Scope

This Cyber Security Policy reflects our commitment to transparency and collaboration in maintaining a secure digital environment. We encourage our community members and employees to actively participate in upholding these responsibilities for the collective benefit of our community.

This policy sets the guardrails for maintaining the security of information systems, networks, and data within Maitland City Council. It applies to all employees, contractors, and third-party entities with access to our digital infrastructure.

Policy Statement

At Maitland City Council, we prioritise the security of information to safeguard the interests of our community and ensure the integrity, confidentiality, and availability of digital assets. Our commitment to information security is a shared responsibility of our employees, the public, and those organisations with whom we do business.

Cyber Security Responsibilities

At Maitland City Council, we prioritise the security of information to safeguard the interests of our community and ensure the integrity, confidentiality, and availability of digital assets.

Shared responsibility to Cyber/Information Security

Our commitment to ensuring information security is a shared responsibility of our employees, the public, and those organisations with whom we do business. We approach cyber and information security at seven (7) levels, each supporting the one above.

1. **Policy Adherence**

   All individuals associated with Maitland City Council are required to comply with this Cyber Security Policy. Non-compliance may result in disciplinary actions or legal consequences.

2. **Maitland City Council**

   We are dedicated to implementing and maintaining robust information security measures to protect against unauthorised access, disclosure, alteration, and destruction of sensitive information.

3. **Security Awareness Training**

   Regular training programs will be conducted to enhance the awareness and knowledge of staff and the public regarding potential data breaches, information security threats, and best practices.

4. **Employees**

   Employees must adhere to information security policies and guidelines to protect sensitive information. This includes exercising caution in handling information, using secure access protocols, and promptly reporting security incidents.

5. **Third-Party**

   Third-party businesses that provide services to Maitland City Council are expected to adhere to information security standards and guidelines. Compliance will be assessed before and during engagement to ensure the security of shared information.

6. **Public**

   Our community members are encouraged to be vigilant and report any suspicious activities that may compromise information security. Public cooperation is essential in maintaining a secure digital environment.

7. **Incident Reporting**

   Employees and the public are responsible for promptly reporting any suspected or actual security incidents to the designated channels. Reporting ensures timely mitigation and resolution.

Cyber Security Risks

Maitland City Council regularly assesses and mitigates cybersecurity risks through proactive identification, evaluation, and response strategies. This includes periodic security assessments, vulnerability management, and incident response planning.

Risk-based approach to Cyber/Information Security

Maitland City Council conducts risk assessments to mitigate the most critical and probable threats. This method adapts our cybersecurity strategy, ensuring protective measures evolve alongside the changing threat landscape.

1. **Risk Identification**

Maitland City Council proactively identifies potential cybersecurity risks. This involves continuous threat intelligence, vulnerability assessments, and engagement with cybersecurity experts (Cyber NSW) to comprehensively recognize and understand the diverse cyber threats that may impact Maitland City Council.

2. **Risk Assessment**

A formal cybersecurity risk assessment process evaluates identified cyber threats' likelihood and potential impact. This process considers information sensitivity, system criticality, and the potential for service disruption.

3. **Risk Mitigation and Controls**

Appropriate cybersecurity controls and mitigation strategies have been implemented to reduce the risk of cyber threats. This includes deploying security technologies, regular software updates, and enforcing access controls to maintain the resilience of our digital environment.

4. **Risk Monitoring**

Continuous monitoring of identified cybersecurity risks is conducted to ensure the effectiveness of controls over time. Regular reviews with our cybersecurity partners are undertaken to adapt to emerging cyber threats and evolving technology landscapes.

Data Protection and Privacy

We are committed to protecting the privacy and confidentiality of the data we handle. Compliance with relevant data protection regulations will be our priority, and measures will be in place to ensure the lawful and ethical use of information.

The council assesses the risk to data and the potential impact on the confidentiality, integrity, and availability of the information we store and handle. We ensure that information is accessible only to those authorised to have access, safeguard the accuracy and completeness of information and processing methods, and ensure that authorized users have access to information and associated assets when required.

Data protection is primarily governed by two critical pieces of legislation concerning data privacy and security: Privacy and Personal Information Protection Act 1998 (NSW) and the Health Records and Information Privacy Act 2002 (NSW)

Maitland City Council is obligated under the Notifiable Data Breach (NDB) scheme, introduced as part of amendments to the Privacy Act, which mandates the notification of eligible data breaches to the Office of the Australian Information Commissioner (OAIC) and affected individuals. For more details, please refer to Maitland City Council's Data Breach Policy.

Access Control

Effective access control measures are essential for preventing unauthorized access to sensitive information, ensuring the reliability of our systems, and maintaining the trust of the community we serve.

The council recognises the importance of protecting the privacy of community members. Access controls are designed to safeguard sensitive information and uphold individuals' privacy rights. Regular privacy impact assessments will be conducted to ensure ongoing compliance with relevant privacy laws and regulations.

Our access philosophy is based on the least privilege principle, where users are granted the minimum level of access required to fulfill their job responsibilities. Maitland City Council has implemented robust user authentication mechanisms to ensure only authorised personnel can access sensitive systems and data. Multi-Factor Authentication (MFA) has been employed where applicable, adding an extra layer of security to user credentials accessing our systems. This approach minimises the risk of unauthorised access and potential misuse of sensitive information.

Public access to Maitland City Council IT services requires user acceptance of access before using our public-facing services, ensuring a secure and compliant environment while safeguarding our digital infrastructure.

As part of our ongoing access review, real-time monitoring and logging of access activities have been implemented to detect and respond to suspicious or unauthorised activities.

Security Audits and Assessments

Maitland City Council is committed to upholding a resilient cybersecurity posture by implementing this Security Audits and Assessments Policy. We strive to safeguard the trust of our community and ensure the continuous protection of our digital assets.

Maitland City Council follows: the NIST Cybersecurity Framework and the Australian Signals Directorate Information Security Manual and the Australian Signals Directorate Essential Eight best practices and compliance standards are relevant to the public sector.

Security audits and assessments are in place to measure the effectiveness of our cybersecurity controls, policies, and procedures. Security audits and assessments are conducted annually, with additional assessments triggered by significant changes in our digital environment. This approach ensures a continuous and adaptive cybersecurity strategy.

Maitland City Council regularly engages with qualified internal or external cybersecurity professionals. We conduct collaborative security audits to ensure impartiality and thoroughly assess our security controls. Post-audit, a detailed report is generated encompassing vulnerabilities, risks, and recommended remediation actions. The findings and remediation actions are promptly reported to the Audit, Risk and Improvement Committee (ARIC), and responsible departments and individuals are notified. A structured timeline is then followed to implement the necessary remediation measures, ensuring the continuous enhancement of our cybersecurity posture.

Reporting a Cybersecurity Security Incident

A cybersecurity incident is any event that compromises the confidentiality, integrity, or availability of our information systems, networks, or data. This includes, but is not limited to, unauthorised access, data breaches, malware infections, denial-of-service attacks, and other malicious activities.

All employees, contractors, and stakeholders are responsible for promptly reporting any suspected or observed cybersecurity incidents. All internal incidents should be reported to the designated IT or cybersecurity point of contact within the organisation. Timely reporting is crucial for initiating a rapid and effective response to promptly contain and remediate the incident.

Maitland City Council will establish an Incident Response Team of cybersecurity professionals, IT personnel, legal representatives, and relevant stakeholders. This team will be responsible for assessing

the severity of incidents, coordinating response efforts, and ensuring compliance with legal and regulatory requirements. As part of the incident, an investigation and analysis will be performed to determine the nature and scope of the incident, and this may involve collaboration with external cybersecurity experts, law enforcement, or other relevant authorities.

Affected parties will be informed of the incident and its impact as soon as practicable. Communication will be transparent, providing necessary information without compromising the ongoing investigation by Maitland City Council's breach notifications that we have issued.

Training and Awareness

The council provides regular training to Council staff and contractors on the importance of safeguarding personal information, identifying and reporting a suspected data breach, and the data breach response process.

Accessibility of this Policy

This policy will be publicly available on the Council's website and the staff intranet.

Policy Definitions

General Manager	• Provide executive leadership and support for the council's cybersecurity initiatives • Advocate for cybersecurity awareness and best practices at all organisational levels • Ensure that cybersecurity is integrated into the overall organisational risk management strategy • Allocate resources, budget, and support for cybersecurity programs and initiatives • Stay informed about the evolving cybersecurity landscape and emerging threats • Foster a culture of accountability and responsibility regarding cybersecurity across the organisation • Collaborate with the Executive Manager of Customer and Digital Services to align cybersecurity with organisational goals
Executive Manager Customer and Digital Services	• Develop and oversee the implementation of the council's cybersecurity strategy • Conduct risk assessments to identify and prioritise cybersecurity threats • Coordinate incident response and recovery efforts • Ensure compliance with cybersecurity policies, standards, and regulations • Provide cybersecurity awareness training to staff • Collaborate with other departments to integrate cybersecurity into business processes • Review and approve cybersecurity policies and procedures • Implement and manage cybersecurity controls and measures
Manager ICT Operations	• Implement and manage cybersecurity controls and measures • Monitor and analyse security alerts and incidents • Conduct regular security audits and vulnerability assessments • Manage relationships with external cybersecurity vendors and partners • Monitor network traffic for unusual activity and security threats

	• Implement and maintain network security solutions • Investigate and respond to security incidents related to the network • Collaborate with system administrators to ensure secure network configurations
Cyber Security Analyst	• Develop and deliver cybersecurity awareness training programs • Create educational materials and resources to promote cybersecurity best practices • Conduct simulated phishing exercises to test employee awareness • Provide ongoing communication on emerging cybersecurity threats and trends
Incident Response Team	• Respond promptly to cybersecurity incidents and breaches • Contain and mitigate the impact of security incidents • Collaborate with law enforcement and regulatory authorities when necessary • Conduct post-incident analysis and prepare incident reports • Ensure compliance with legal and regulatory requirements during incident response

Policy Administration

Business Group:	Customer and Digital Services
Responsible officer:	Manager Enterprise Architecture
Council reference:	Council Meeting 26 March 2024 – Item 11.2
Policy review date:	3 Years from Date of Adoption
File number:	35/1
Relevant legislation	• Australian Signals Directorate Essential Eight • Health Records and Information Protection Act 2002 (NSW) • Privacy And Personal Information Protection Act 1998 (NSW) • Privacy and Personal Information Protection Regulation 2019 (NSW) • State Records Act 1998 (NSW)
Related documents	• Privacy Management Plan • Records Management Policy • Privacy Policy • Data Beach Policy

Policy History

VERSION	DATE APPROVED	DESCRIPTION OF CHANGES
1.0	26/3/2024	New Policy – Cyber/Information Security