Cyber Security Framework

Policy	8N
Officer Responsible	Manager Information Technology
Last Review Date	13/10/2025

Strategic Policy

1. INTRODUCTION

1.1. OBJECTIVE

This Cyber Security Framework establishes the overarching framework for managing cyber security within Blayney Shire Council. It defines Council's commitment to safeguarding the confidentiality, integrity, and availability of its information systems, data, and digital services.

This framework provides a structured, risk-based approach aligned to the Cyber Security Guidelines for NSW Local Government (2024), the NSW Cyber Security Policy, and national standards including the ACSC Essential Eight. It ensures that council operations, public services, and community trust are protected from the impacts of cyber threats.

The purpose is not only compliance but to foster a culture of proactive cyber resilience, equipping Council to address emerging risks in a dynamic threat landscape.

1.2. SCOPE

This framework applies to:

- All council employees, contractors, consultants, volunteers, councillors, and third-party service providers who access or handle council-owned information systems, data, or services.
- All council information and communication technology (ICT) systems, operational technology (OT) systems, Internet of Things (IoT) assets, networks, applications, and data repositories, regardless of whether they are hosted on-premises, in the cloud, or through third parties.
- All activities related to the creation, access, processing, transmission, storage, and disposal of council information, across the entire data lifecycle.

1.3. COUNCIL COMMITMENT

Blayney Shire Council is committed to:

- Embedding cyber security as a fundamental component of its governance, risk management, and operational practices.
- Aligning its cyber security activities with NSW Government guidelines, best practices, and legislative obligations.
- Adopting a continuous improvement approach, regularly reviewing its cyber security posture and uplifting capabilities over time.
- Promoting a strong cyber security culture across the council, ensuring that staff and third-party partners understand and fulfil their security responsibilities.
- Ensuring the council's resilience to evolving cyber threats, balancing innovation, public service delivery, and risk management.

1.4. LEGISLATIVE AND POLICY CONTEXT

This framework is shaped by the following key frameworks and obligations:

- **NSW Cyber Security Policy (latest version)**
- **Cyber Security Guidelines for NSW Local Government (2024)**
- **Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model**
- **Privacy and Personal Information Protection Act 1998 (NSW)**
- **Local Government Act 1993 (NSW)**
- **State Records Act 1998 (NSW)**
- **Other applicable state and federal legislation, standards, and regulatory obligations**

This framework is to be read in conjunction with following Council documentation:

- **Information Technology Security and Usage Policy**
- **Incident Response Plan**
- **Enterprise Risk Management Policy and Plan**

Where relevant, this framework also references international best practices including ISO 27001, NIST Cybersecurity Framework, and the NSW Beyond Digital Strategy.

2. GOVERNANCE AND RESPONSIBILITIES

2.1. GOVERNANCE OVERVIEW

Effective cyber security governance ensures that Council has clear leadership, accountability, and decision-making structures to manage cyber risks, meet compliance obligations, and deliver resilient services to the community.

Council, as the governing body of the Council under the *Local Government Act 1993 (NSW),* maintain ultimate collective accountability for council's risk management framework including determining overall risk appetite.

Governance responsibilities are additionally distributed across executive, management, operational, and third-party levels, following the **Cyber Security Guidelines for NSW Local Government (2024)**, with oversight by the **Audit, Risk and Improvement Committee (ARIC)**, and the Chief Information Security Officer of the Central New South Wales Joint Organisation.

2.2. EXECUTIVE-LEVEL RESPONSIBILTIES

General Manager (GM)

- Appoint a qualified senior officer (CISO or equivalent) with the authority to oversee cyber security.
- Ensure development, implementation, and maintenance of a cyber security strategy and/or plan aligned to business objectives and cyber risk appetite.
- Define Council's risk appetite for cyber security using whole-of-government risk management frameworks.
- Allocate sufficient funding, resources, and executive sponsorship for cyber security initiatives, training, and improvement efforts.
- Attend ARIC meetings and support independent oversight of cyber risks.
- Approve internal cyber security policies and major security decisions.

2.3. DIRECTOR-LEVEL RESPONSIBILTIES

Director Leadership Roles

- Oversee the implementation of the cyber security strategy and key initiatives in collaboration with CIO, COO, and CISO, the ARIC and the Central NSW Joint Organisation's Information Security Steering Committee.
- Ensure reporting on cyber security progress, outcomes, and risks to the Executive Committee.
- Champion cyber security awareness and accountability across business units.

2.4. CISO / CIO RESPONSIBILTIES

Chief Information Security Officer (CISO)

- Develop, maintain, and operationalise Council's cyber security strategy, architecture, and risk management processes.
- Define and apply risk treatment strategies for cyber security.
- Provide advice and recommendations on exemptions or changes to security policies.
- Investigate, respond to, and report on cyber security incidents, including to Cyber Security NSW as required.

2.5. MANAGERIAL AND OPERATIONAL RESPONSIBILTIES

Manager Information Technology or Equivalent

- Manage day-to-day implementation of security controls, incident responses, vulnerability management, and security platform lifecycles.
- Develop and maintain cyber security procedures, guidelines, and metrics for performance assurance.
- Provide guidance on cyber risks emerging from business and operational changes.
- Coordinate operational teams to maintain system availability, performance, and security.
- Ensure Council's leadership is informed about cyber risks, required resources, and the implementation progress of the cyber strategy.
- Oversee execution of security controls, project security requirements, and integration of secure-by-design principles into new and legacy systems.
- Support the CISO in ensuring consistent application of security practices across all operations.

Privacy Officer

- Act as the point of contact for all privacy matters, including with the Information and Privacy Commission NSW.
- Ensure privacy obligations are integrated into cyber security practices, particularly around incident response and breach management.
- Assess the privacy impact of new projects and changes.
- Manage privacy complaints and regulatory notifications.

Information Management Officer or Equivalent

- Maintain records and data management aligned with cyber security needs.
- Ensure timely escalation and reporting of information loss or damage incidents.

Internal Audit and Risk

- Provide independent assurance on the effectiveness of cyber risk management, controls, and compliance.
- Validate that the cyber security strategy aligns with Council's overall risk framework.
- Conduct regular cyber risk assessments and report outcomes to the ARIC.

All Council Staff

- Complete mandatory cyber security awareness training.
- Practice secure behaviours, including password management, phishing vigilance, and incident reporting.
- Understand and follow the cyber security responsibilities relevant to their roles.
- Comply with the **Information Technology Security and Usage Policy.**

2.6. THIRD-PARTY RESPONSIBILTIES

Third-Party Service Providers

- Comply with all cyber security requirements as outlined in council contracts.
- Report suspected or actual security incidents and data breaches immediately.
- Participate in periodic compliance reviews, audits, and security performance checks.
- Implement appropriate controls, including multi-factor authentication, access restrictions, data segmentation, and secure offboarding processes.

2.7. AUDIT, RISK AND IMPROVEMENT COMMITTEE (ARIC)

- Provide independent advice to the Council on cyber security risks, issues, and improvement opportunities.
- Monitor Council's implementation of the foundational and detailed requirements outlined in the with the **Cyber Security Guidelines for NSW Local Government (2024).**
- Review internal audit findings and external advice to inform council decisions on cyber risk management.

3. RISK MANAGEMENT

Council has an established **Enterprise Risk Management Policy and Plan**.

3.1. PURPOSE OF RISK MANAGEMENT

Cyber security risk management enables Council to identify, evaluate, and mitigate risks to its information systems, digital assets, and operational services in a structured, proportional, and continuous manner.

This approach ensures Council aligns cyber security activities with organisational objectives, legal obligations, and the evolving threat environment.

3.2. RISK MANAGEMENT PRINCIPLES

Council applies the following principles:

- **Risk-Based Approach**: Cyber risks are identified, prioritised, and treated based on their potential impact on council objectives and services.
- **Proportionality**: Controls are applied relative to the sensitivity and criticality of assets, recognising differences between ICT, OT, IoT, and cloud environments.
- **Continuous Improvement**: Risk management processes are iterative, adapting to emerging threats, technology changes, and lessons learned.
- **Alignment with Council Risk Appetite**: Cyber risk decisions reflect Council's defined tolerance and appetite, as set by the General Manager and Executive Leadership, within the broader corporate risk framework.
- **Integration with Enterprise Risk Management**: Cyber risks are incorporated into enterprise-wide risk assessments, reporting, and governance.

3.3. CYBER RISK IDENTIFICATION

Council systematically identifies cyber risks by:

- Maintaining up-to-date inventories of all ICT, OT, IoT, and data assets, including crown jewels and sensitive systems.
- Conducting threat modelling exercises to map likely threat actors, attack vectors, and vulnerabilities.
- Monitoring external intelligence sources (e.g., ACSC advisories, Cyber Security NSW updates) and internal data (e.g., logs, vulnerability scans).
- Identifying risks introduced through new projects, system changes, third-party engagements, or evolving business requirements.

3.4. RISK ASSESSMENT AND ANALYSIS

Once identified, cyber risks are:

- Analysed to assess their likelihood and potential impact on the confidentiality, integrity, and availability of council assets and services.
- Classified and prioritised according to Council's risk assessment framework and aligned with approved risk appetite and tolerance levels.
- Evaluated with both inherent risk (before controls) and residual risk (after controls) considered.
- Documented in risk registers, ensuring traceability and accountability.

3.5. RISK TREATMENT

Council applies one or more treatment strategies for each assessed cyber risk:

- **Mitigation**: Implementing technical, procedural, or organisational controls to reduce risk levels.
- **Transfer**: Using contracts, insurance, or third-party arrangements to shift risk responsibility.
- **Acceptance**: Acknowledging residual risk within defined tolerances and documenting justification and approvals.
- **Avoidance**: Adjusting projects, systems, or processes to eliminate exposure to unacceptable risks.

Significant risks exceeding Council's risk appetite must be escalated through management and reported to the ARIC.

3.6. ONGOING MONITORING AND REVIEW

Cyber risk management is a continuous process, supported by:

- Regular reviews of risk assessments and treatment plans.
- Periodic vulnerability scans, penetration tests, and audits.
- Post-incident reviews, lessons learned, and corrective actions.
- Integration of findings from self-assessments and third-party assessments.
- Updating threat models, asset inventories, and risk registers as the environment changes.

3.7. INTEGRATION WITH BUSINESS OBJECTIVES

Council ensures that:

- Cyber risk considerations are embedded in strategic planning, service delivery, and change management.
- Major initiatives (including digital transformation, smart city projects, and outsourced services) are subject to cyber security risk evaluation.
- Cyber risk management supports Council's public service mission, community trust, and innovation goals, without imposing disproportionate barriers.

4. CYBER SECURITY CONTROLS

4.1. PURPOSE AND CONTEXT

Cyber security controls are the technical, procedural, and organisational safeguards that protect Council's information systems, data, and services from cyber threats.

These controls are designed and implemented in alignment with the **Cyber** Security Guidelines for NSW Local Government (2024), the NSW Cyber Security Policy, and the Australian Cyber Security Centre (ACSC) Essential Eight.

They reflect Council's risk-based approach, ensuring that protections are applied proportionally to the sensitivity and criticality of assets, whether in ICT, OT, IoT, cloud, or hybrid environments.

4.2. FOUNDATIONAL AND DETAILED REQUIREMENTS

Council adopts the foundational and detailed cyber security requirements outlined by the **Cyber Security Guidelines for NSW Local Government (2024)** to strengthen governance, detect and respond to threats, protect critical assets, and recover from incidents effectively.

Key areas include:

- Establishing a governance framework where security controls are continuously monitored, reviewed, and improved.
- Maintaining comprehensive inventories of systems, data, applications, and physical devices to ensure visibility and accountability.
- Identifying critical systems and data ("crown jewels") that require enhanced protection measures.
- Ensuring segregation of critical assets and enforcing secure configurations, patching, and update processes.
- Implementing regular vulnerability and risk assessments to inform security control decisions.

4.3. ESSENTIAL EIGHT ALIGNMENT

Council explicitly integrates the ACSC Essential Eight mitigation strategies as its baseline technical control framework. These strategies are applied to all relevant systems, tailored to their environment, and continuously uplifted to meet target maturity levels.

The Essential Eight comprises:

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privileges

6. Patch operating systems
7. Multi-factor authentication (MFA)
8. Regular backups

Maturity levels are determined through self-assessment and third-party evaluation, ensuring that Council progressively improves its cyber resilience over time.

4.4. ACCESS MANAGEMENT AND IDENTITY SECURITY

Strong access management is central to protecting council systems.

Council enforces principles of least privilege, ensuring that users have only the minimum access required to perform their duties.

Multi-factor authentication is mandated for all privileged and remote access accounts, with routine reviews of account permissions, logins, and dormant or orphaned accounts.

Access controls extend across staff, contractors, third-party providers, and automated systems, ensuring consistent application of authentication and authorisation safeguards.

4.5. NETWORK AND INFRASTRUCTURE SECURITY

Council maintains protections across its networks, including segmentation between critical and non-critical systems, secure perimeter defences (such as firewalls), and working to uplift routine monitoring of network traffic for anomalies or malicious activities.

Encryption uplift is on the roadmap to ensure its applied to sensitive data in transit, while secure configuration baselines are established and maintained across network devices, servers, and endpoints.

4.6. DATA PROTECTION AND PRIVACY

Data is protected across its lifecycle — from creation and collection, through storage and use, to archival and destruction — in accordance with the **Privacy and Personal Information Protection Act 1998 (NSW)** and State Records obligations.

This includes applying encryption to sensitive data at rest, maintaining secure backups, enforcing data retention and destruction policies, and applying privacy-by-design principles in system and process development.

4.7. OPERATIONAL TECHNOLOGY (OT) AND INTERNET OF THINGS (IOT) SECURITY

Critical OT systems (such as utilities, infrastructure, and smart hub platforms) are segregated from general ICT networks, monitored for threats, and maintained under strict patching and access control regimes.

4.8. THIRD-PARTY AND SUPPLY CHAIN SECURITY

Third-party providers are required to meet Council's cyber security standards as defined in contracts, including implementing appropriate controls, participating in security assessments, and notifying Council of incidents or changes in risk posture.

Legacy contracts are reviewed periodically to identify and address cyber security gaps, while new contracts incorporate minimum security requirements, performance metrics, and compliance obligations.

4.9. CHANGE, CONFIGURATION AND VULNERABILITY MANAGEMENT

Council maintains change management practices that incorporate cyber security impact assessments for system upgrades, patches, and modifications.

Configuration baselines are documented and enforced, ensuring consistency across environments.

Vulnerability management is proactive, with ongoing improvements to continuous scanning, prioritised remediation, and integration of threat intelligence to address emerging risks.

4.10. CONTINUOUS MONITORING AND IMPROVEMENT

Council commits to continuous monitoring, regular testing (including penetration tests, and adaptive improvements informed by self-assessments, audits, lessons learned from incidents, and external best practices.

Metrics and performance indicators will be used to track control effectiveness, with regular reporting to executive leadership and the ARIC.

5. INCIDENT MANAGEMENT

5.1. PURPOSE AND IMPORTANCE

Effective incident management enables Council to detect, respond to, and recover from cyber security incidents in a timely, coordinated, and controlled manner.

This ensures Council minimises operational, reputational, legal, and financial impacts while aligning with the **Cyber Security Guidelines for NSW Local Government (2024)**, the **NSW Cyber Security Policy**, and relevant privacy and regulatory frameworks.

A mature incident management capability not only addresses immediate threats but contributes to long-term resilience and continuous improvement.

5.2. INCIDENT MANAGEMENT FRAMEWORK

Council maintains an **Incident Breach Response Plan** in conjunction with managed service provider Incident Response Plans, and continues to uplift its incident management framework so that it includes:

- Defined roles, responsibilities, and escalation pathways.
- Clear classification of incident types and severity levels.
- Integrated workflows for detection, analysis, containment, eradication, recovery, and post-incident review.
- Alignment with council-wide business continuity and disaster recovery (BCP/DR) frameworks.
- Predefined communication strategies, both internal and external, including public communications where appropriate.

This framework applies to all council systems, data, services, and third-party providers and is regularly tested and updated to reflect evolving threats and lessons learned.

5.3. DETECTION AND REPORTING

Council is planning to establish and uplift:

- Continuous monitoring across its ICT, and cloud environments, using tools such as security information and event management (SIEM) systems, intrusion detection/prevention systems, and endpoint detection platforms. Currently Microsoft Defender for Endpoint is used for endpoint protection.
- Incident management frameworks so that incidents are reported through established channels, with clear procedures for staff, contractors, and third-party providers to escalate suspected or confirmed events.
- Guidance for reporting obligations include incidents that compromise the confidentiality, integrity, or availability of systems or data, as well as privacy breaches covered under the **Privacy and Personal Information Protection Act 1998 (NSW)**.

5.4. RESPONSE AND CONTAINMENT

Upon identification of an incident, the response team will coordinate actions to:

- Contain the spread and prevent further damage.
- Identify the root cause and affected systems.
- Preserve forensic evidence where required.
- Communicate with affected stakeholders, including internal leadership, Cyber Security NSW, law enforcement (if applicable), and regulatory bodies.

Council prioritises response activities based on the criticality of impacted services and the potential consequences to community operations.

5.5. RECOVERY AND RESTORATION

Once containment and eradication are complete, Council undertakes structured recovery processes, which may include system rebuilds, data restoration from secure backups, revalidation of system integrity, and reconnection to the broader network.

Recovery activities are integrated with Council's BCP/DR plans, ensuring service continuity for critical operations.

Systematic verification and testing are conducted before full resumption of services.

5.6. POST INCIDENT REVIEW AND IMPROVEMENT

Every significant incident triggers a formal post-incident review, capturing:

- A timeline of events.
- Root cause analysis.
- Effectiveness of detection, response, and recovery efforts.
- Lessons learned and improvement opportunities.

Outcomes inform updates to policies, procedures, controls, training, and risk registers, ensuring continuous enhancement of Council's security posture.

5.7. EXTERNAL REPORTING AND COMPLIANCE

Council fulfils all mandatory reporting obligations, including:

- Notification to Cyber Security NSW of significant incidents as required under the NSW Cyber Security Policy.
- Reporting privacy breaches to the Information and Privacy Commission NSW where applicable.
- Engaging with law enforcement or regulatory agencies for criminal or compliance-related matters.

- Providing required updates to the Audit, Risk and Improvement Committee (ARIC) and executive leadership.

These processes will be documented and then tested and reinforced through scenario-based exercises and tabletop simulations at least annually.

6. TRAINING AND AWARENESS

6.1. PURPOSE AND IMPORTANCE

A resilient cyber security posture depends not only on technology and governance but also on people.

Council recognises that staff, contractors, councillors, and third-party partners play a pivotal role in protecting information assets and services.

Human error, lack of awareness, and insufficient capability are among the most significant contributors to cyber incidents. Therefore, Council commits to fostering a strong cyber security culture underpinned by training, awareness, and continuous learning.

6.2. CYBER SECURITY AWARENESS PROGRAM

Council maintains a structured Cyber Security Awareness Program designed to embed secure behaviours, reinforce policy compliance, and reduce human-related vulnerabilities.

The program addresses the needs of all staff and stakeholders, providing clear, relevant, and practical knowledge tailored to their roles.

It encompasses foundational security principles, organisational policies, threat awareness (such as phishing, social engineering, and ransomware), data handling requirements, incident reporting procedures, and acceptable use standards.

Content is regularly updated to reflect emerging threats, lessons learned from incidents, and changes in policy or technology.

6.3. MANDATORY TRAINING REQUIREMENTS

Council staff, contractors, and councillors are required to complete cyber security training:

- At induction or onboarding.
- Annually thereafter as part of mandatory refresher training.
- As needed following significant incidents, control failures, or identified knowledge gaps.

Completion of training is tracked and reported to management, with non-compliance escalated for follow-up action.

6.4. ROLE SPECIFIC AND ADVANCED TRAINING

Staff with elevated privileges, such as system administrators, information security personnel, privacy officers, or executive leadership, receive or will receive targeted training aligned with their responsibilities.

This includes deeper knowledge of security configurations, incident management, risk assessment, privacy obligations, and decision-making under cyber pressure.

Where relevant, third-party providers and contractors are required under contract to demonstrate equivalent cyber security training and awareness for staff supporting council systems.

6.5. EXERCISES, SIMULATIONS AND CONTINUOUS LEARNING

To reinforce learning and test practical readiness, Council conducts or will conduct:

- Phishing simulations to evaluate user susceptibility and reinforce secure email behaviours.
- BCP Tabletop exercises and scenario-based drills to validate incident response capabilities, including coordination between ICT, business units, executive leadership, and third-party providers.
- Lessons-learned sessions following incidents, near misses, or emerging threat advisories to ensure knowledge is transferred and embedded.

These activities are designed not as punitive measures but as continuous improvement opportunities, fostering a learning culture where staff feel empowered and equipped to uphold cyber resilience.

6.6. PROMOTING A CYBER-SECURE CULTURE

Beyond formal training, Council promotes or will promote cyber security as a shared organisational value, integrating security messages into staff communications, leadership briefings, and public service initiatives.

Secure behaviours are recognised and reinforced, contributing to an environment where every individual understands their role in protecting council services and community trust.

7. THIRD-PARTY MANAGEMENT

7.1. PURPOSE AND IMPORTANCE

As Council increasingly relies on external service providers, contractors, suppliers, and technology partners to deliver critical services, the risks introduced by these third parties become integral to Council's overall cyber security posture.

Council recognises that third-party vulnerabilities can become direct exposures, threatening the confidentiality, integrity, and availability of council data, systems, and services.

Therefore, it is essential to establish robust third-party management practices that ensure consistent application of cyber security standards and maintain resilience across the supply chain.

7.2. THIRD-PARTY RISK GOVERNANCE

Third-party management is integrated into Council's overall governance and risk frameworks and practices.

Cyber risks arising from suppliers and partners are identified, assessed, and managed in alignment with Council risk management processes, with executive oversight and reporting to the Audit, Risk and Improvement Committee (ARIC). Contracts, service-level agreements (SLAs), and memoranda of understanding (MOUs), where possible, are structured to embed clear cyber security requirements, performance expectations, and compliance obligations.

7.3. PRE-ENGAGEMENT RISK ASSESSMENT

Before entering into any agreement with a third-party provider, Council conducts:

- Due diligence on the provider's cyber security capabilities, maturity, and track record.
- Risk assessments that consider the provider's access to council data, systems, or services; the sensitivity of assets involved; and the potential impact of a security failure.
- Reviews of contractual terms to ensure inclusion of minimum-security standards, data protection clauses, breach notification requirements, audit rights, and liability provisions.

Where gaps or risks are identified, mitigation strategies are developed, or engagement is reconsidered.

7.4. SECURITY REQUIREMENTS DURING ENGAGEMENT

Throughout the lifecycle of the engagement, third-party providers are required to:

- Comply with Council's security standards and policies, as well as all contractual cyber security obligations.
- Maintain secure configurations, patching, access controls, and monitoring over systems and services supporting council operations.
- Notify Council promptly of any suspected or confirmed security incidents, breaches, or material changes in risk posture.
- Participate in periodic compliance reviews, including audits, attestations, and performance reviews where required.

Council reserves the right to request evidence of cyber security controls, certifications, or independent assessments to validate compliance.

7.5. MANAGING LEGACY AND HIGH-RISK CONTRACTS

Recognising that older agreements may not reflect current security expectations, Council periodically reviews legacy contracts to identify gaps or weaknesses.

Where significant risks are identified, mitigation actions are taken, which may include renegotiation, additional controls, or risk acceptance with documented executive approval.

For high-risk engagements such as those involving critical infrastructure, sensitive data, or privileged system access, enhanced oversight, technical controls, and incident coordination arrangements are implemented.

7.6. OFFBOARDING AND TERMINATION

At the conclusion of an engagement, Council ensures that:

- All system and data access granted to the third-party provider is promptly revoked.
- Any council data held by the provider is securely returned, deleted, or destroyed, in accordance with contractual terms and legal obligations.
- Knowledge transfer, handover, and post-engagement reviews are conducted to identify lessons learned and inform future engagements.

7.7. INTEGRATION WITH BROADER SECURITY FRAMEWORK

Third-party management is not a standalone activity but is integrated into Council's overall cyber security, incident management, risk, and compliance frameworks.

This ensures that risks introduced through the supply chain are monitored, reported, and addressed alongside internal risks, maintaining a holistic view of Council's threat landscape.

8. COMPLIANCE AND MONITORING

8.1. PURPOSE AND COMMITMENT

Council is committed to ensuring that its cyber security policies, controls, and practices are consistently applied, regularly evaluated, and continuously improved.

Compliance is not a one-time exercise but an ongoing obligation, aligning with the **Cyber Security Guidelines for NSW Local Government (2024)**, the **NSW Cyber Security Policy**, the **ACSC Essential Eight** and other legal, regulatory, and contractual requirements.

Through structured monitoring, assessments, and reporting, Council maintains accountability, demonstrates due diligence, and builds stakeholder confidence in its cyber resilience.

8.2. INTERNAL COMPLIANCE MONITORING

Council maintains mechanisms to monitor compliance with its cyber security policy and related procedures across all operational areas.

This includes regular reviews of system configurations, access controls, patching, backup processes, training completion rates, and incident response preparedness.

Compliance monitoring responsibilities are clearly assigned to designated roles, including the CISO/Manager Information Technology, privacy officers, and system owners, with oversight by executive leadership and the Audit, Risk and Improvement Committee (ARIC).

Where non-compliance is identified, corrective actions are documented, tracked, and reported, ensuring that issues are addressed promptly and systematically.

8.3. SELF-ASSESSMENT AND CAPABILITY MATURTIY

Council conducts annual cyber security self-assessments against alignment with the **Cyber Security Guidelines for NSW Local Government (2024)**, and the **ACSC Essential Eight**.

These assessments evaluate Council's performance against foundational and detailed requirements and essential security controls, helping to:

- Identify gaps and improvement opportunities.
- Track progress over time, including Essential Eight maturity uplift.
- Inform executive reporting, budget decisions, and resource planning.

Where results are formally documented, they are reviewed by executive leadership and provided to the ARIC for independent oversight.

8.4. INDEPENDENT ASSURANCE AND AUDITS

To strengthen accountability and transparency, Council complements self-assessments with:

- Internal audits focusing on cyber security risks, controls, and compliance, conducted in accordance with Council's Internal Audit Plan.
- External audits or assessments by independent parties, where required by regulation, best practice, or contractual obligations.
- Validation of third-party provider compliance through attestations, certifications, or on-site assessments, where appropriate.

Audit findings are reported to the ARIC, with management responsible for implementing agreed-upon recommendations and reporting progress.

8.5. PERFORMANCE METRICS AND REPORTING

Council will establish performance metrics (key risk indicators, key performance indicators) to monitor the effectiveness of its cyber security program.

Metrics will be tailored to operational realities and cover areas such as incident response times, vulnerability remediation rates, training completion, system uptime, and third-party compliance.

Regular reports will be provided to executive leadership, the ARIC, and other governance bodies, enabling informed oversight and decision-making.

8.6. REGULATORY AND EXTERNAL REPORTING

Council fulfils all external cyber security reporting obligations, including:

- Providing required updates to Cyber Security NSW under the NSW Cyber Security Policy.
- Reporting privacy breaches to the Information and Privacy Commission NSW, where applicable.
- Supplying cyber risk and performance data in accordance with state government requirements or public reporting expectations.

Council remains transparent with stakeholders and the community where appropriate, balancing disclosure obligations with operational and security considerations.

8.7. CONTINUOUS IMPROVEMENT INTEGRATION

Compliance and monitoring activities are not simply tick-box exercises but are integrated into Council's continuous improvement approach.

Findings from assessments, audits, and performance monitoring inform updates to policies, controls, training, and strategic plans, ensuring that the cyber security program evolves in response to changing threats, technologies, and organisational needs.

9. POLICY REVIEW AND MAINTENANCE

9.1. PURPOSE AND COMMITMENT

Council recognises that cyber security is a dynamic and continuously evolving domain, driven by technological change, emerging threats, regulatory developments, and organisational growth.

To ensure this Cyber Security Framework remains relevant, effective, and aligned with the **Cyber Security Guidelines for NSW Local Government (2024)**, Council commits to structured, regular review and maintenance processes.

9.2. REVIEW CYCLE

The Cyber Security Framework is formally reviewed:

- At least once every 12 months and referred to Council for adoption when required.
- As aligned with Council's broader policy review schedule.
- Following significant cyber security incidents, audits, regulatory changes, or shifts in organisational risk appetite.
- In response to lessons learned, technology upgrades, or changes in threat landscape identified through Council's continuous improvement processes.

The review process ensures that this framework remains consistent with Council's cyber security strategy, risk management framework, and external obligations.

9.3. REVIEW AND UPDATE RESPONSIBILITIES

The Manager of Information Technology or delegate is responsible for leading this framework review process, and engaging stakeholders across:

- Executive leadership and governance bodies (including the General Manager and ARIC).
- Business units, technical teams, privacy and legal advisors.
- Third-party partners where applicable.

Updates are drafted, reviewed, and endorsed through formal approval channels, ensuring alignment with Council's governance and change management protocol.

9.4. CHANGE MANAGEMENT

Policy changes are subject to controlled change management processes, ensuring that:

- Stakeholders are consulted appropriately, including impacted business units and governance bodies.
- Change rationale, impacts, and dependencies are documented.
- Communications plans are developed to inform staff, contractors, and third-party providers of updated requirements.
- Training and awareness updates are implemented where necessary.

Council maintains an audit trail of all policy changes, approvals, and communications.

9.5. INTEGRATION WITH CONTINUOUS IMPROVEMENT

Policy review is not a standalone task but forms part of Council's broader continuous improvement efforts, ensuring alignment with:

- Self-assessment and audit findings.
- Performance monitoring and metrics.
- Incident and breach lessons learned.
- Threat intelligence and external advisory updates.

This integrated approach ensures that Council's cyber security posture evolves in line with best practice, emerging risks, and community expectations.

End

	Date	Minute No.
Adopted:	**23/06/2025**	**2506/012**
Last Reviewed:	**23/06/2025**	**2506/012**
Next Review:	**28/09/2029**	