Cyber Security NSW

Cyber Security Guidelines – Local Government 2024-2025

Issued January 2025

Contents

1. Purpose

The Cyber Security Guidelines – Local Government (the Guidelines) outlines cyber security standards recommended for NSW local government by Cyber Security NSW. The Guidelines are designed to be read by General Managers, Chief Information Officers, Chief Information Security Officers (or equivalent) and Audit, Risk and Improvement Committees (ARIC).

The Guidelines should form the basis of an internally developed cyber security policy for NSW councils. Compliance with the Guidelines is strongly encouraged but remains **voluntary**.

Terms used in this guideline are defined in Section 11 - Glossary, located near the end of this document.

2. Introduction

Strong cyber security is an important component of the NSW Beyond Digital Strategy[1], enabling the effective use of emerging technologies and ensuring confidence in the services the NSW local government provides. Cyber security covers all measures used to protect systems – and information processed, stored or communicated on these systems – from compromise of confidentiality, integrity and availability.

Councils should establish effective cyber security policies and procedures and embed cyber security into risk management practices and assurance processes. When cyber security risk management is done well, it reinforces organisational resilience, making entities aware of their risks and helps them make informed decisions in managing those risks. This should be complemented with meaningful training, communications and support across all levels of the council.

3. Self-Assessment templates

Councils may use the example self-assessment templates provided to help track their progress. Two templates have been provided:

1. Self-Assessment (Basic): This template breaks down the Foundational Requirements into non-detailed requirements. This allows councils to track the implementation of basic cyber security fundamentals. Councils are encouraged to use the ‘Comments’ field to input further information about implementation or non-compliance.

   This template is recommended for smaller councils or those who may find more detailed reporting too strenuous.

[1] https://www.digital.nsw.gov.au/strategy

2. Self-Assessment (Detailed): This template provides specifics to implement under each Foundational Requirement, allowing a more in-depth view of cyber security posture. Councils are encouraged to use the ‘Comments’ field to input further information about implementation or non-compliance.

   This template is recommended for councils seeking a more detailed view of their cyber security posture.

Each Foundational or Detailed requirement holds equal importance and should be implemented accordingly. Councils may choose to select not implemented or partial implementation; however, it is highly recommended to select a reason from one of the five dropdown options in the "implementation status" section. Alternatively, provide an explanation in the "Comments" section detailing the reason for non-compliance and/or noting any compensating controls used.

Councils do not need to report their findings to Cyber Security NSW, however the self-assessment templates could be used to inform internal audit/risk and regular reporting to the Councils’ Audit Risk and Improvement Committee (ARIC), along with a continual monitoring process.

4. Threat-based cyber risk management

Each council has its own unique operational context that influences the threats and risks they are exposed to. Likewise, the business objectives and constraints of a council will also inform how risks are managed, and which mitigation strategies should be prioritised.

Using the cyber security risk management program established through the implementation of the Foundational Requirements, councils are best placed to manage key risks aligned to business objectives and risk appetite and making continuous improvements. This includes identification, prioritisation and implementation of additional controls beyond the Foundational Requirements.

Councils that provide critical or higher-risk services and hold higher-risk information should implement a wider range of controls and aim for broader coverage and effective implementation of those controls. Councils implementing projects with higher cyber security risks should seek additional guidance, strategies and controls when implementing their security strategy and plan, including from supplementary sources mentioned in Useful links.

As part of a risk-based approach to cyber security, Cyber Security NSW recommends councils update their risk management program for cyber security to incorporate consideration of key threats, including:

- establishing threat modelling processes to inform cyber security risk assessments.

- implementing appropriate mitigation strategies to address the identified threat and risk controls, with prioritisation aligned to the business objectives and organisational context of the council.
    - this may include consideration of:
        - ACSC Essential Eight controls at Level 2 and Level 3 maturity
        - zero-trust principles and related implementation strategies e.g., NIST SP800-207, CISA Zero Trust Maturity Model, etc
        - environment-specific mitigation strategies (including cloud, enterprise mobility, OT and IoT assets)
        - commonly used good practice control frameworks, e.g., ISO 27002:2022, Australian Signals Directorate (ASD) ISM, etc.
        - criticality of services provided by the council and sensitivity of information held or processed by the council.

Establishing effective threat modelling and risk management practices is an ongoing journey involving continuous improvement and will require effective implementation of multiple Foundational Requirements in order to support these practices. As such, councils that are not at a level of capability to begin establishing threat modelling processes should identify and assess the longer-term uplift required as part of their cyber security strategy development, to support threat-based risk management and to support the alignment with business objectives in risk management processes.

Cyber Security NSW provides optional threat modelling and reporting templates to assist councils in sharing information on key threats and risks. For copies of these templates, please contact advisory@cyber.nsw.gov.au. These resources are optional for councils to use and not a requirement for implementing the threat-based requirements.

5. The NSW Cyber Security Policy

The Guidelines are based on the NSW Cyber Security Policy (the Policy), which has been edited to better suit councils. The Policy outlines the mandatory requirements to which all NSW Government departments and Public Service agencies must adhere to ensure cyber security risks to their information and systems are appropriately managed.

Whilst the Policy is not mandatory for local government, it is recommended for adoption as a foundation of strong cyber security practice. Cyber Security NSW can work with councils to help implement the policy.

The NSW Cyber Security Policy can be viewed at: https://www.digital.nsw.gov.au/delivery/cyber-security/policies

6. Roles and Responsibilities

This section outlines the roles and responsibilities a council should allocate as part of their cyber security function:

- **Councils have flexibility to tailor roles to their organisational context**, but all responsibilities should be allocated and performed regardless of role title.
- A council may not have all the roles outlined below.
- These responsibilities can be allocated to roles not specifically named in this policy or shared among multiple roles.
- All councils must have an independent internal audit function that reports to the audit, risk and improvement committee and is consistent with current international standards for internal audit.[2]

To make it easier for councils to map these roles and responsibilities against their own organisational structure, they have been divided into sections: Director, Management, Operational.

6.1. Executive-level (or equivalent) roles and responsibilities

6.1.1. General Manager (GM) or Executive Officer (Joint Organisations)(EO)

The General Manager or Chief Executive Officer role is responsible for:

- appointing or assigning an appropriate staff member in the organisation with the authority to perform the duties outlined in the Guidelines
- ensuring their organisation develops, implements and maintains an effective cyber security strategy and/or plan
- determining their organisation's risk appetite using the approved whole-of-government Internal Audit and Risk Management Policy[3]

[2] https://www.olg.nsw.gov.au/wp-content/uploads/2023/12/Guidelines-for-Risk-Management-and-Internal-Audit-updated-November-2023.pdf
[3] Guidelines for Risk Management and Internal Audit for Local Government in NSW - Office of Local Government NSW

- should attend the Audit Risk and Improvement Committee (ARIC) meetings
- supporting the organisation's cyber security plan
- determining their organisation's risk appetite
- appropriately funding, resourcing and supporting cyber security initiatives, including training and awareness and continual improvement initiatives to support the Guidelines
- approving internal security policies as required.

6.2. Director-level (or equivalent) roles and responsibilities

This is aligned with a structure of Council Executive Committees where a CIO/CISO typically reports to a Director and then on to the GM. If the CIO/CISO is a direct report to the GM this is not relevant but will demonstrate the difference in duties if this structure is adopted. However, this structure is not mandatory, and councils should assign these responsibilities where appropriate based on their specific organisational context

6.2.1. Director-level

- overseeing the implementation of a cyber security strategy in collaboration with the CIO/COO and CISO/CCSO
- reporting on progress and outcomes from the cyber security strategy and associated actions to the Executive Committee

6.2.2. Chief Information Security Officers (CISO) or Chief Cyber Security Officers (CCSO)

CISOs and CCSOs (or staff with these responsibilities) are responsible for:

- defining and implementing a cyber security strategy and/or plan for the protection of their organisation's information and systems
- developing a cyber security strategy, architecture and risk management process and incorporating these into the organisation's current risk framework and processes
- deciding on risk treatment strategies for cyber security within the council when the identified risk falls outside the acceptable risk tolerance
- reviewing and providing recommendations on any exemptions to organisation information security policies and standards

- investigating, responding to, and reporting on cyber security incidents to the appropriate council governance forum and Cyber Security NSW, based on severity definitions provided by Cyber Security NSW

6.2.3. Chief Information Officer (CIO) or Chief Operating Officer (COO)

CIOs or COOs (or staff with these responsibilities) are responsible for:

- ensuring the GM & Council are made aware of the strategy, and the resources required to implement the strategy
- working with staff across their council to implement these guidelines, including allocating sufficient resources and funding (in circumstances where this role holds appropriate financial delegations) to manage the identified cyber security risks under their remit
- implementing a cyber security strategy and/or 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
    - ensuring that all staff, including mayors, councillors, consultants, contractors and outsourced service providers, understand the cyber security requirements of their roles
- defining the scope of CIO or COO responsibilities for cyber security relating to assets such as information, building management systems and IACS
- supporting CISOs, CCSOs or equivalent positions with their responsibilities
- ensuring a secure-by-design approach for new initiatives and upgrades to existing systems, including legacy systems
- ensuring all staff and providers understand their role in building and maintaining secure systems.

6.3. Manager-level (or equivalent) roles and responsibilities

6.3.1. Information Security Manager, Cyber Security Manager or Senior Responsible Officer

Information Security Managers, Cyber Security Managers or Senior Responsible Officers (or staff with these responsibilities) are responsible for:

- managing and coordinating the response to cyber security incidents, changing threats and vulnerabilities
- developing and maintaining cyber security procedures and guidelines

- implementing and executing controls to mitigate risks
- providing guidance on cyber security risks introduced from business and operational change
- managing the life cycle of cyber security platforms
- 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.

6.4. Operational-level roles and responsibilities

6.4.1. Information Management Officer

Information management officers (or staff with these responsibilities) undertake information and records management activities to ensure all information and records are managed in accordance with the organisation's recordkeeping plan, policies, processes and procedures. They are responsible for:

- acting as a focal point within their organisation for all matters related to information management required to support cyber security, and
- ensuring that a cyber incident that involves information damage or loss is escalated and reported to the appropriate information management response team in your organisation

6.4.2. Privacy Officer

Councils should have a person who fulfills the role of Privacy Officer, as recommend by the Information and Privacy Commission NSW (IPC NSW).[4] The role is responsible for:

- acting as point of contact with IPC NSW, the public and within the council for all matters related to privacy and personal information
- ensuring that privacy considerations are integrated into the council's overall cyber security policies, procedures and processes
- assisting in identifying privacy impacts of new projects or proposed new legislation

[4] https://www.ipc.nsw.gov.au/privacy/agencies/role-privacy-contact-officers

- collaborating with the cyber security team in incident response planning
- coordinating the investigation of privacy incidents, determining the extent of the breach and coordinating notifications to affected individuals and regulatory authorities
- assessing and managing privacy complaints.

6.4.3. Internal Audit and Risk

The *Local Government (General) Regulation 2021* (NSW) (Part 9, Division 6A) requires each council to have an internal audit function by July 2024[5]

Consistent with the regulations and Local Government Act 1993 (the Act), Internal audit, and risk teams (or staff with these responsibilities) should identify activities to support the effective audit and risk management of the cyber security program at the council. The workplans should consider:

- validating that the cyber security strategy and plan meet the council's business goals and objectives, and ensuring the plan supports the council's cyber security strategy
- providing independent assurance regarding the effectiveness of cyber security controls
- conducting risk assessments to identify and evaluate potential cyber security threats and vulnerabilities
- integrating cyber security into the council's overall risk management framework and risk appetite
- meeting with the organisation CISO (or equivalent) to ensure cyber risk frameworks fit into the enterprise risk framework

6.4.4. Council staff

Council staff should contribute to an organisation's cyber security culture. Responsibilities include:

- practising secure password habits
- identifying and reporting cyber incidents and cyber threats
- completing cyber security awareness programmes and role-based training
- safeguarding classified information
- staying informed about cyber security best practices

[5] https://www.olg.nsw.gov.au/councils/governance/risk-management-audit-and-internal-controls

6.5. Other roles and responsibilities

6.5.1. Third-party service providers

Councils are responsible for managing cyber security requirements and risks posed by third-party service providers. The scope of a council's responsibility applies at a minimum to; a) ICT service providers (including third-party NSW Government shared service providers), and b) other third-party service providers which process or store an agency's sensitive information.

Foundational Requirement 1.10 sets out minimum expectations for third-party security risk management including detailed requirements (see Section 8 Detailed Requirements) for use of contract clauses, monitoring and enforcement for in-scope third-party service providers.

Council responsibilities include:

- ensuring third-party risks are considered in enterprise risk management processes
- conducting regular management of third-party risks through ongoing risk-based reviews to verify compliance with contractual agreements and security measures
- establishing and maintaining a comprehensive inventory of all external third-party service providers engaged
- ensuring responsibilities in contracts extend to meeting cyber security requirements by defining risk-based tolerances and processes to manage when a third-party fails to comply with the agreed security requirements in contracts (e.g. break clauses) and offboarding if non-compliance continues
- dependent on the risks associated with a particular product or service, councils may consider including the following in new procurement processes and contracts
    - accountability for suspected or actual security incidents or breaches to any data, systems infrastructure or processes used in its arrangement, and ensuring incidents are reported immediately, enabling timely protective measures
    - documenting controls and data segmentation in contracts or service level agreements with the provider, relative to the data classification of the information and systems that are to be covered and the service being provided
    - requiring access control processes safeguarding council data by limiting access to authorised individuals
    - prioritising security for users accessing sensitive data, including mandating multi-factor authentication, significantly reducing unauthorised access risks

- data sovereignty upon contractual negotiations, including data hosting locations and locations of support services offered by the third-party service provider
- privacy provisions when third-party service providers capture, hold or process personal information
- where privileged access to systems is required to perform services, third-party service providers will be required to follow documented council processes for requesting access each time it is required, and councils should consider revoking access whenever it is not in use.
- as part of the off-boarding process, ensuring data retention and data destruction time frames are clearly defined at the end of the contract agreement, and consistent with relevant legislation and applicable directives (e.g. Local Government Records GA39)

Existing contracts may not have appropriate contractual mechanisms to enable councils to effectively exercise their responsibilities in relation to this section. Where this is the case, the council may be subject to increased risks through the inability to require or contractually enforce requirements related to cyber security (e.g. incident notification, obligations for implementation of appropriate security protections to protect services and customer data, termination of contracts due to security considerations and/or appropriate assurance of the performance of security obligations in the contract). For legacy contracts, councils are expected to take a risk-based approach to managing these third-party services. This includes ensuring that the relevant risks and mitigation strategies are appropriately documented, managed (and where required, escalated) in line with the council's risk management framework.

Where councils require third-party service providers to assist with their implementation of the Guidelines, councils should ensure they have the following in place to protect government systems outsourced to them or that they have access to.

- Foundational Requirement 1.10.1 – Establish and maintain an inventory of third-party service providers, including ICT service providers.
- Foundational Requirement 1.10.2 – Ensure there is a contractually supported process for third-party service providers to notify the agency of suspected or actual security incidents, as well as data breaches (noting this will vary based on risk profile and risk appetite).
- Foundational Requirement 1.10.3 – Have processes to monitor and assess adherence of third-party service providers to cyber security requirements, including using assurance reports, audits, test results or other forms of evaluations.
- Foundational Requirement 1.10.4 – Include clauses in contracts with third-party service providers for cyber security requirements and break clauses associated with failure to meet security requirements.

- Foundational Requirement 3.2.1 – Establish a process for granting, maintaining and revoking access for agency systems, applications and information to ensure authorised access only.
- Foundational Requirement 3.5.2 – Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their entity's sensitive data.
- Foundational Requirement 3.5.3 – Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their entity's non-sensitive data.
- Foundational Requirement 3.5.5 – Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their entity's sensitive customer data.

This does not prevent other contractual obligations being imposed.

6.5.2. Audit Risk and Improvement Committee

The Local Government Act (section 428A) requires each council to establish an audit, risk and improvement committee that is appropriate for the council's size, risk profile, operational complexity, resources, and its ability to attract suitably qualified committee members.

Consistent with the obligations set out in the legislation and regulations, as well as the Risk Management obligations on the ARIC (see: Core Requirement 2 from the OLG Guidelines for Risk Management and Internal Audit for Local Government in NSW), the Audit, Risk & Improvement committee should ensure that they review the management of cyber security risks which could include through the monitoring implementation of the foundational requirements of the Local Government Guidelines.

Each audit, risk and improvement committee should provide independent advice to the council on cyber security risks, issues, & concerns. This advice should be informed by the council's internal audit and risk management activities as well as information and advice provided by council staff, relevant external bodies and other subject matter experts.

The exact nature of each audit, risk and improvement committee's role and the specific activities it reviews relating to cyber security risks on behalf of a council under section 428A of the Act will vary depending on the council's needs, risks and business functions.

7. Foundational Requirements

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

Councils should adopt the Foundational Requirements (as well as the supporting practices described in Section 8 Detailed Requirements) as part of their cyber security strategy and/or plan.

Foundational Requirements 3.3 – 3.10 are aligned to the Australian Cyber Security Centre's Essential Eight strategies to mitigate cyber security incidents. More information is provided in Section 9 The Essential Eight)

1. Govern and identify	
1.1	Allocate and perform roles and responsibilities for cyber security.
1.2	Have an executive-level governance committee with appropriate authority to make decisions about cyber security, including OT/IoT.
1.3	Ensure that the Audit Risk and Improvement Committee (ARIC) is briefed regularly on cyber security risks, related issues and corrective actions.
1.4	Develop and maintain a cyber security strategy.
1.5	Develop and maintain formalised plans, policies and processes for cyber security practices.
1.6	Establish and maintain processes for asset inventory management and identify asset dependencies.
1.7	Assess and identify Crown Jewels and classify systems.
1.8	Govern the identification, retention and secure disposal of data.
1.9	Define risk tolerance and risk appetite and manage cyber security risks.
1.10	Identify and manage third-party service provider risks, including shared ICT services supplied by other councils.
1.11	Establish and maintain vulnerability management processes.
1.12	Ensure cyber security requirements and impacts are assessed as part of change management processes.

2. Detect, respond and recover	
2.1	Implement event logging and continuous monitoring to detect anomalous activity.
2.2	Maintain a cyber incident response plan and use exercises and post-incident reviews to continuously improve the plan.
2.3	Report cyber incidents and provide information on threats to Cyber Security NSW.
2.4	Include cyber security in business continuity and disaster recovery planning.

3. Protect	
3.1	Conduct awareness activities, including mandatory cyber security awareness training.
3.2	Implement access controls to ensure only authorised access.
3.3	Patch applications (ACSC Essential Eight).
3.4	Patch operating systems (ACSC Essential Eight).
3.5	Implement multi-factor authentication (ACSC Essential Eight).
3.6	Restrict administrative privileges (ACSC Essential Eight).
3.7	Implement application control (ACSC Essential Eight).
3.8	Securely configure Microsoft Office macro settings (ACSC Essential Eight).
3.9	Implement user application hardening (ACSC Essential Eight).
3.10	Maintain backups of important data, software and configuration settings (ACSC Essential Eight).
3.11	Establish and maintain secure configurations.
3.12	Define and implement data security controls.
3.13	Implement email security controls.
3.14	Implement controls for endpoint protection, including mobile devices.
3.15	Implement network security controls.

8. Detailed Requirements

Outlined below are detailed requirements aligned to the NSW state reporting process that focus on further enhancing planning and governance, cyber security culture, safeguarding information and systems, strengthening resilience against attacks and improved reporting. These requirements build on the Foundational requirements to allow a more in-depth view of the council's cyber security posture.

Councils should adopt the Foundational Requirements (as well as the supporting practices described in this section) as part of their cyber security strategy and/or plan.

1. Govern and identify	
1.1.1	Has the council formalised roles and responsibilities for cyber security based on the local government guidelines
1.1.2	Has the council identified any additional roles and responsibilities for cyber security outside Has the council identified any additional roles and responsibilities for cyber security and reviewed these according to their organisational needs
1.2.1	Is there a governance committee at the executive level which meets at least quarterly, with appropriate authority to make decisions about cyber security
1.2.2	Does the terms of reference of the governance committee cover ICT, OT and IoT Systems?
1.3.1	Is cyber security a standing item on the Audit, Risk & Improvement Committee agenda
1.4.1	Does the council have a current approved cyber security strategy that aligns to the entity's strategic business objectives and captures key threats, risks, vulnerabilities, actions and initiatives to make improvements and address any gaps
1.5.1	Is the cyber security program supported by plans, policies, standards and processes to manage cyber security risks?
1.6.1	Does the council maintain asset inventories for ICT, OT, IoT, network and software
1.6.3	Does the council have a formal process for replacing end of support assets and software?
1.6.3	Does the council have a formal process for secure disposal of ICT assets?
1.7.1	Does the council have a framework for identifying Crown Jewel assets which has been used to identify crown jewels?
1.8.1	Has the council identified any data assets which are sensitive?
1.8.2	Has the council identified and formalised data retention requirements within a policy?
1.8.3	Does the council have a process for secure disposal of data and associated assets based on the type & sensitivity of the data?
1.9.1	Does the council have approved risk appetite statements for cyber security risks and defined risk tolerance
1.9.2	Does the council identify, assess and manage cyber security risks across the organisation
1.9.3	Are cyber security risks exceeding risk appetite or risk tolerance escalated according to the council's risk management framework
1.10.1	Does the council maintain an inventory of third party service providers

1.10.2	Do contracts with third party providers (ICT providers and service providers handling/storing sensitive data) include contractual requirements to notify the council of suspected or actual cyber security incidents and data breaches?
1.10.3	Does the council have a process to monitor adherence of third party service providers to the cyber security requirements of the contract?
1.10.4	Does the council have cyber security clauses in contracts with third party service providers
1.11.1	Does the council have a vulnerability management process to identify and triage technical vulnerabilities
1.11.2	Does the council's vulnerability management process also include reviewing and actioning alerts from Cyber Security NSW?
1.12.1	Does the council assess cyber security requirements in IT and enterprise changement management processes?
1.12.2	Does the council manage changes to any cyber security controls through a change control process
1.12.3	Does the council conduct testing of cyber security controls and secure configurations after significant changes
2. Detect, respond and recover	
2.1.1	Does the council have processes for logging and monitoring critical security events based on identified risks
2.2.1	Does the council have and maintain a cyber incident response plan
2.2.2	Does the council exercise the cyber incident response plan annually
2.2.3	Does the council perform post-incident reviews and action findings from those reviews such as updating plans and processes
2.2.3	Does the council have a cyber security incident register
2.3.2	Does the council report all cyber security incidents to Cyber Security NSW
2.4.1	Does the council's business continuity and disaster recovery plans consider cyber incident scenarios
2.4.2	Does the council's business continuity and disaster recovery plans consider continuity of cyber security operations in a BC/DR event?
3. Protect	
3.1.1	Is cyber security awareness training mandated for all staff, annually and at onboarding
3.1.2	Does the council have a program of cyber awareness activites outside of mandatory training to maintain awareness of cyber risks
3.1.3	Does the council perform phishing simulations for all staff on a periodic basis
3.1.4	Does the council have mandatory additional training for users in high risks roles focused on additional cyber risks related to those roles?

3.2.1	Does the council have access control processes to ensure only authorised access is granted to council systems?
3.2.2	Does the council remove access within a defined period of an employee's termination/change of role?
3.2.3	Does the council conduct routine user access reviews to ensure accesses are removed when no longer needed?
3.3 E8 ML1	Does the council patch applications (ACSC Essential Eight)? - 3.3.1 An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. - 3.3.2 A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. - 3.3.3 A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. - 3.3.4 A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products. - 3.3.5 Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. - 3.3.6 Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. - 3.3.7 Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products are applied within two weeks of release. - 3.3.8 Online services that are no longer supported by vendors are removed. - 3.3.9 Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player and security products that are no longer supported by vendors are removed.
3.4 E8 ML1	Does the council patch operating systems (ACSC Essential Eight)? - 3.4.1 An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. - 3.4.2 A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. - 3.4.3 A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices. - 3.4.4 A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices. - 3.4.5 Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. - 3.4.6 Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. - 3.4.7 Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.

	- 3.4.8 Operating systems that are no longer supported by vendors are replaced.
3.5 E8 ML1	Does the council implement multi-factor authentication (ACSC Essential Eight)? - 3.5.1 Multi-factor authentication is used to authenticate users to their entity's online services that process, store or communicate their entity's sensitive data. - 3.5.2 Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their entity's sensitive data. - 3.5.3 Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their entity's non-sensitive data. - 3.5.4 Multi-factor authentication is used to authenticate users to their entity's online customer services that process, store or communicate their entity's sensitive customer data. - 3.5.5 Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their entity's sensitive customer data. - 3.5.6 Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. - 3.5.7 Multi-factor authentication uses: something users have and something users know; or something users have that is unlocked by something users know or are.
3.6 E8 ML1	Does the council restrict administrative privileges (ACSC Essential Eight)? - 3.6.1 Requests for privileged access to systems, applications and data repositories are validated when first requested. - 3.6.2 Privileged accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. - 3.6.3 Privileged users are assigned a dedicated privileged account to be used solely for duties requiring privileged access. - 3.6.4 Privileged accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties. - 3.6.5 Privileged users use separate privileged and unprivileged operating environments. - 3.6.6 Unprivileged accounts cannot login to privileged operating environments. - 3.6.7 Privileged accounts (excluding local administrator accounts) cannot login to unprivileged operating environments.
3.7 E8 ML1	Does the council implement application control (ACSC Essential Eight)? - 3.7.1 Application control is implemented on workstations. - 3.7.2 Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. - 3.7.3 Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
3.8 E8 ML1	Does the council securely configure Microsoft Office macro settings (ACSC Essential Eight)? - 3.8.1 Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. - 3.8.2 Microsoft Office macros in files originating from the internet are blocked. - 3.8.3 Microsoft Office macro antivirus scanning is enabled. - 3.8.4 Microsoft Office macro security settings cannot be changed by users.

3.9 E8 ML1	Does the council implement user application hardening (ACSC Essential Eight)? - 3.9.1 Web browsers do not process Java from the internet. - 3.9.2 Web browsers do not process web advertisements from the internet. - 3.9.3 Internet Explorer 11 is disabled or removed. - 3.9.4 Web browser security settings cannot be changed by users.
3.10 E8 ML1	Does the council maintain backups of important data, software and configuration settings (ACSC Essential Eight)? - 3.10.1 Backups of data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. - 3.10.2 Backups of data, software and configuration settings are synchronised to enable restoration to a common point in time. - 3.10.3 Backups of data, software and configuration settings are retained in a secure and resilient manner. - 3.10.4 Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. - 3.10.5 Unprivileged accounts cannot access backups belonging to other accounts. - 3.10.6 Unprivileged accounts are prevented from modifying and deleting backups.
3.11.1	Does the council ensure unnecessary accounts, components, services are disabled or removed from relevant systems
3.11.2	Does the council ensure that default accounts or credentials for operating systems, including pre-configured accounts, are disabled or changed
3.11.3	Does the council have a process for ensuing that only authorised people are allowed to change the security settings of operating systems
3.12.1	Does council have a process for ensuring that all data imported manually is scanned for malicious and active content
3.12.2	Does the council have a processes for data encryption
3.13.1	Does the council have email anti-spoofing measures, including use of domain based message authentication, reporting and conformance (DMARC), Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) in place
3.13.2	Has the council implemented email content filtering
3.14.1	Has the council implemented antivirus software on all endpoints and servers.
3.14.2	Has the council implemented software firewalls on all endpoints and servers.
3.14.3	Does the council have a Mobile Device Management (MDM) solution for all mobile devices used by staff
3.15.1	Does the council utilise network segmentation to segregate critical servers, services and data
3.15.2	Does the council ensure default accounts or credentials are changed for all network devices
3.15.3	Does the council have a network access control policy

9. The Essential Eight

The ACSC has developed and published the Essential Eight strategies for mitigating cyber incidents. The Essential Eight are embedded in **Foundational Requirements 3.3 to 3.10**. Councils are recommended to implement the Essential Eight to applicable ICT environments with a minimum requirement of Level 1 maturity, as part of the baseline set in the Guidelines. Mitigation strategies for Level 2 and Level 3 maturity should then be considered alongside other mitigation strategies based on the threats and risks identified by the council as part of the threat-based requirements (see Threat-based cyber risk management).

The Foundational Requirements aligned to the Essential Eight maturity level 1[6] in the Guidelines are mapped to the controls taken from the December 2023 release of the Information Security Manual (ISM).[7] The Essential Eight controls are subject to annual review by the ACSC, noting the ACSC have conducted an annual review of the Essential Eight Maturity Model and decided that they won't be releasing an update for 2024Updates to the Essential Eight are often guided by changes in the threat environment and informed by evidence, including information about incidents observed by the ACSC. As such, councils should assess changes and prioritise implementation of new or adjusted requirements as part of their risk management processes.

10. Glossary

Item	Definition
Access control	The process of granting or denying requests for access to systems, applications and information. Can also refer to the process of granting or denying requests for access to facilities.
ACSC	Australian Cyber Security Centre
Application control	An approach in which only an explicitly defined set of applications are allowed to run on systems.
Audit log	A chronological record of system activities including records of system access and operations performed.
Audit trail	A chronological record that reconstructs the sequence of activities surrounding, or leading to, a specific operation, procedure or event.
Authentication	Verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system.
Authorisation	The process of defining or verifying permission for a specific identity or device to access or use resources in a system.
Availability	The assurance that systems and information are accessible and useable by authorised entities when required.
Breach (data)	When data is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

[6] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

[7] https://www.cyber.gov.au/sites/default/files/2023-12/Information%20Security%20Manual%20%28December%202023%29.pdf

Item	Definition
Breach (security)	A cyber incident that results in unauthorised access to data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.
Business Continuity Plan	A business continuity plan is a document that outlines how an organisation can ensure its critical business functions will: continue to operate despite serious incidents or disasters that might otherwise have interrupted them; or will be recovered to an operational state within a reasonably short period.
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Classification	The categorisation of systems and information according to the expected impact if it was to be compromised.
Critical infrastructure	Physical facilities, supply chains and ICT networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect its ability to conduct national defence and ensure national security.
Crown Jewels	The most valuable or operationally vital systems or information in an organisation.
CSF	Cyber Security Framework
CSMS	A Cyber Security Management System is a management system focused on cyber security of control systems rather than information
Classification	The categorisation of systems and information according to the expected impact if it was to be compromised.
Cyber attack	A deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity. Note: There are multiple global definitions of what constitutes a cyber attack.
Cybercrime	Crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It includes crimes where computers facilitate an existing offence, such as online fraud or online child sex offences.
Cyber crisis	Major disruptions to services and operations, with genuine risks to critical infrastructure and services that pose risks to the safety of citizens and businesses. These often result in intense media interest as well as large demands on resources and critical services.
Cyber event	An identified occurrence of a system, service or network state indicating a possible breach of security policy or failure of safeguards.
Cyber incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
Cyber incident response plan	A plan for responding to cyber incidents.

Item	Definition
Cyber security	Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them.
Disaster recovery plan	Outlines an organisation's recovery strategy for how they are going to respond to a disaster.
Essential Eight	The eight essential mitigation strategies that the ASD recommends organisations implement as a baseline to make it much harder for malicious actors to compromise their systems and data.
Exercise- Tabletop	Also known as a tabletop exercise, a discussion exercise has participants discuss a hypothetical cyber incident and propose approaches for remediation and recovery, while referencing the organisation's cyber incident response plan and associated processes. Discussion exercises are led by a facilitator who guides exercise engagement and ensures participant discussion remains focused through the use of prompting questions. Discussion exercises are suitable for reviewing and evaluating cyber incident response processes.
Exercise- Functional (Simulation)	Functional Exercises take place in a simulated operational environment where participants perform their roles and responsibilities during a cyber incident. Functional Exercises allow an organisation to test their equipment, software, hardware, and communication during a cyber incident. Forensic artefacts and simulated attacks can be introduced by the control team so that participants can test their ability to detect and respond to threats. Functional Exercises are suitable for testing crisis communication and cooperation, in addition to evaluating the organisation's cyber incident response processes.
Full Backup	Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.
General Manager	A general manager's role to implement council decisions and carry out functions imposed by legislation (Local Government Act 1993).
IACS	Industrial Automation and Control Systems, also referred to as Industrial Control System (ICS), include "control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e. electricity, gas and water), pipelines and petroleum production and distribution facilities, and other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets". (IEC/TS 62443-1-1 Ed 1.0)
ICT	Information and communications technology, also referred to as information technology (IT), includes software, hardware, network, infrastructure, devices and systems that enable the digital use and management of information and the interaction between people in a digital environment.
Incident response plan	A plan for responding to cyber incidents.

Item	Definition
Information security	The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.
Internet of Things (IoT)	The network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors and network connectivity, which enables these objects to connect to the internet and collect and exchange data.
ISMS	An information security management system "consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives". (ISO/IEC 27000:2018)
Macro	An instruction that causes the execution of a predefined sequence of instructions.
Multi-factor authentication	A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).
NSW CCSO	NSW Chief Cyber Security Officer
Operational technology (OT)	OT is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.
PABX	A Private Automatic Branch Exchange is an automatic telephone switching system within a private enterprise.
Partial backup	A partial restoration would be anything less than a full restoration. The expectation would be at least any chosen file or database.
Patching	The action of updating, fixing or improving a computer program.
Position of Trust	A position that involves duties that require a higher level of assurance than that provided by normal employment screening. In some organisations additional screening may be required Positions of trust can include, but are not limited to, an organisation's Chief Information Security Officer and their delegates, administrators or privileged users
Privileged user	A user who can alter or circumvent a system's security measures. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security measures. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.
Red Team	Ethical hackers that provide penetration testing to ensure the security of an organisation's information systems
Remote access	Access to a system that originates from outside an organisation's network and enters the network through a gateway, including over the internet.

Item	Definition
Risk appetite	“Amount and type of risk that an organisation is willing to pursue or retain.” (ISO/Guide 73:2009)
Risk, inherent	The current risk level given the existing set of controls rather than the hypothetical notion of an absence of any controls.
Risk, residual	The rating of the current risk that remains after application of existing mitigating controls and/or other existing risk treatment.
Risk tolerance	Organisation’s or stakeholder’s readiness to bear the risk, after risk treatment, in order to achieve its objectives.” (ISO/Guide 73:2009)
SDLC	The System Development Life Cycle is the “scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal”. (NIST SP 800-137)
Secure-by-design principles	An approach to software and hardware development that tries to minimise vulnerabilities by designing from the foundation to be secure and taking malicious practices for granted.
Significant cyber incident	Significant impact to services, information, assets, NSW Government reputation, relationships and disruption to activities of NSW business and/or citizens. Multiple NSW Government agencies, their operations and/or services impacted. May involve a series of incidents having cumulative impacts.
State owned corporation	Commercial businesses owned by the NSW Government: Essential Energy, Forestry Corporation of NSW, Hunter Water, Landcom, Port Authority of NSW, Sydney Water, Transport Asset Holding Entity of NSW (TAHE), Water NSW.
Supply chain	A system of organisations, people, activities, information and resources involved in supplying a product or service to a consumer.
Systems	Software, hardware, data, communications, networks and specialised systems, such as industrial and automation control systems, telephone switching and PABX systems, building management systems and internet connected devices.
Whitelisting	Authorising only approved applications for use within organisations in order to protect systems from potentially harmful applications

11. Useful links

Issuer	Reference	Document Name
NSW Government	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1989-134	*State Owned Corporations Act 1989*
	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-017	*State Records Act 1998*
	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-133	*Privacy and Personal Information Protection Act 1998*
	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2002-071	*Health Records and Information Privacy Act 2002*
	https://www.legislation.nsw.gov.au/#/view/act/2009/52	*Government Information (Public Access) Act 2009*
	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2013-040	*Government Sector Employment Act 2013*
	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2015-060	*Data Sharing (Government Sector) Act 2015*
	https://www.nsw.gov.au/improving-nsw/projects-and-initiatives/nsw-state-infrastructure-strategy/	*The NSW State Infrastructure Strategy 2018-2038*
	https://www.nsw.gov.au/rescue-and-emergency-management/sub-plans/cyber-security	*NSW Government Incident Emergency Sub Plan*
	https://www.treasury.nsw.gov.au/documents/tpp20-08-internal-audit-and-risk-management-policy-general-government-sector	*Internal Audit and Risk Management Policy for the General Government Sector (TPP20-08)*
	https://www.digital.nsw.gov.au/policy/internet-things-iot	*NSW Government Internet of Things (IoT) Policy*
NSW Government - Office of Local Government	https://www.legislation.nsw.gov.au/view/html/inforce/current/act-1993-030	*Local Government Act,1993*
	https://www5.austlii.edu.au/au/legis/nsw/consol_act/lga1993182/s428a.html	*Local Government Act, 1993 - Sect 428a*
	https://www.olg.nsw.gov.au/wp-content/uploads/2023/12/Local-Government-General-Amendment-Audit-Risk-and-Improvement-Committees-Regulation-2023.pdf	*Local Government (General) Amendment (Audit, Risk and Improvement Committees) Regulation, 2023*
NSW Government - Department of Customer Service	https://data.nsw.gov.au/nsw-government-information-classification-labelling-and-handling-guidelines	*NSW Government Information Classification, Labelling and Handling Guidelines*
	https://www.digital.nsw.gov.au/delivery/cyber-security/strategies/nsw-cyber-security-strategy	*2021 NSW Cyber Security Strategy*

	https://www.digital.nsw.gov.au/policy/data-strategy	*Data Strategy*
	https://arp.nsw.gov.au/dcs-2020-02-nsw-cyber-security-Policy/	*DCS-2020-02 NSW Cyber Security Policy*
IPC NSW	https://www.ipc.nsw.gov.au/data-breach-guidance-nsw-agencies	*Data breach guidance for NSW agencies, September 2020*
Audit Office of NSW	https://www.audit.nsw.gov.au/our-work/reports/detecting-and-responding-to-cyber-security-incidents-	*Detecting and responding to cyber security incidents*
NSW Treasury	https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management/risk	*Risk management toolkit*
NSW Department of Premier and Cabinet	https://arp.nsw.gov.au/m1999-19-applicability-memoranda-and-circulars-state-owned-corporations-socs	*Memorandum M1999-19 Applicability of Memoranda and Circulars to State Owned Corporations (SOCs)*
State Archives and Records Authority of NSW	https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/standard-records-management	*Standard on Records Management, 2018*
	https://staterecords.nsw.gov.au/recordkeeping/using-cloud-computing-services-implications-information-and-records-management	*Using cloud computing services: implications for information and records management, 2015*
	https://staterecords.nsw.gov.au/recordkeeping/storage-state-records-service-providers-outside-nsw	*Storage of State records with service providers outside of NSW, 2015*
Australian Government – Home Affairs	https://www.legislation.gov.au/Details/C2022C00160	*Security of Critical Infrastructure Act 2018*
	https://cybersecuritystrategy.homeaffairs.gov.au/	*Australia's Cyber Security Strategy, 2023*
Australian Government - Attorney-General's Department	https://www.protectivesecurity.gov.au/	*The Protective Security Policy Framework*
	https://www.protectivesecurity.gov.au/resources/australian-government-and-international-resources	*Australian Government and international resources*
Australian Government – ASD	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism	*Information Security Manual*
Australian Government – Office of the Australian Information Commissioner	https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/	*Australian Privacy Principles Guidelines, 2014*
International Organization for Standardization	https://www.iso.org/standard/75106.html	*ISO 22301 Societal Security – Business continuity management systems – Requirements*

	https://www.iso.org/standard/44374.html	*ISO 27031 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*
	https://www.iso.org/standard/76070.html	*ISO 27032 Information technology – Security techniques – Guidelines for cybersecurity*
National Institute of Standards and Technology	https://www.nist.gov/cyberframework	*Framework for Improving Critical Infrastructure Cybersecurity*
New Zealand National Cyber Security Centre	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Intro-Nov-2019.pdf	*Introduction: Cyber security governance*
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-1-Nov-2019.pdf	*Step One: Building a culture of cyber resilience*
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-2-Nov-2019.pdf	*Step Two: Establishing roles and responsibilities*
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-3-Nov-2019.pdf	*Step Three: Holistic risk management*
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-4-Nov-2019.pdf	*Step Four: Cyber security collaboration*
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-5-Nov-2019.pdf	*Step Five: Create a cyber security programme*
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-6-Nov-2019.pdf	*Step Six: Measuring resilience*

12. Relevant Legislation, Policies and Procedures

Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)

https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-133

Health Records and Information Privacy Act 2002 (HRIP Act)

https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071

NSW Government Information Classification, Labelling and Handling Guidelines 2020

https://data.nsw.gov.au/nsw-government-information-classification-labelling-and-handling-guidelines

NSW Cyber Security Policy (the Policy)

https://www.digital.nsw.gov.au/policy/cyber-security-policy

Australia's Cyber Security Strategy

https://cybersecuritystrategy.homeaffairs.gov.au/

The Protective Security Policy Framework

https://www.protectivesecurity.gov.au/

Information Security Manual

https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

13. Document version control

Version	Status	Date	Comments
0.1	Draft	30/3/2024	Initial Draft
0.2	First revised draft	26/6/2024	Peer Review Document Updates
0.3	Second revised draft	2/7/2024	Draft for Director level review
0.4	Consultation Draft	17/7/2024	Incorporated Director feedback. Draft for OLG consultation
0.5	SAT Team changes	23/8/2024	Incorporated team feedback
0.6	Changes to align with NSW Cyber Security Policy assurance	5/10/2024	Changes to the self-assessment and guidelines
0.7	Draft for Council Feedback	14/10/2024	Sent for Council Feedback

0.8	Revised Draft for Council Feedback	6/12/2024	Incorporated Council Feedback
0.9	Final Draft for CSNSW ELT Approval	9/12/20024	ELT Approval
1.0	Approval	24/01/2025	Approved

For more information, please contact Cyber Security NSW: info@cyber.nsw.gov.au