Policy

Cyber Security Policy

Responsible Manager (Title)	Lead Analyst		
Adopted by Council	Date		Minutes
File Reference Number		Version 1.0	Review Due
Document(s) this policy Supersedes	Nil		
Community Plan Linkage	5.1 Leadership - A strong, accountable and representative government that engages broadly with the community in a genuine, respectful and meaningful way		

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 and Risk teams.

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

As the Guidelines are to be used for proof of cyber maturity and assurance for internal cyber security processes, there is no requirement to report maturity scores to Cyber Security NSW.

2 Introduction

Strong cyber security is an important component of the NSW Beyond Digital Strategy, enabling the effective use of emerging technologies and ensuring confidence in the services provided by NSW Local Government. 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 The NSW Cyber Security Policy

This Policy is based on the Guidelines which are informed by the NSW Cyber Security Policy (the Policy),The Guidelines have been edited to better suit Councils and have been revised for voluntary compliance. This 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.

The Policy is not mandatory for state owned corporations, Councils and universities. However, it is recommended for adoption by these organisations as a foundation of strong cyber security practice. Cyber Security NSW can provide guidance on implementation to these types of organisations.

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

4 Policy statement

Roles and Responsibilities

This section outlines the roles and responsibilities Council has as part of their cyber security function

4.1 General Manager and Director Corporate and Community

The General Manager and Director Corporate and Community are responsible for:

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

4.2 Lead Analyst

The Lead Analyst is responsible for:

- Defining and implementing a cyber security plan for the protection of their organisation's information and systems
- Developing a cyber security strategy, architecture and risk management process and incorporate these into the organisation's current risk framework and processes
- Assessing and providing recommendations on any exemptions to organisation information security policies and standards
- Attending risk committee meetings
- Implementing policies, procedures, practices and tools to assist with the implementation of the Guidelines
- Investigating, responding to and reporting on cyber security events

- Reporting cyber incidents to the General Manager and Cyber Security NSW, if appropriate
- Establishing training and awareness programs to increase employees' cyber security capability
- Building cyber incident response capability
- Collaborating with privacy, audit, information management and risk officers to protect organisation information and systems
- Managing the budget and funding for the cyber security program

4.3 Senior Responsible Officer – Coordinator Information Technology

The Senior Responsible Officer is responsible for:

- Working with the Lead Analyst and across their organisation to implement this policy
- Implementing a cyber security plan that includes consideration of threats, risks and vulnerabilities that impact the protection of the organisation's information and systems within the organisation's cyber security risk tolerance
- Ensuring that all staff, including consultants, contractors and outsourced service providers understand the cyber security requirements of their roles
- Clarifying the scope of their responsibilities for cyber security relating to assets such as information, building management systems and Industrial Automation and Control Systems (IACS)
- Assisting the Lead Analyst 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 system
- Managing and coordinating the response to cyber security incidents, changing threats and vulnerabilities
- Developing and maintaining cyber security procedures and guidelines
- Providing guidance on cyber security risks introduced from business and operational change
- Managing the life cycle of cyber security platforms including design, deployment, ongoing operation and decommissioning
- Ensuring appropriate management of the availability, capacity and performance of cyber security hardware and applications
- Providing input and support to regulatory compliance and assurance activities and managing any resultant remedial activity
- Developing a metrics and assurance framework to measure the effectiveness of controls
- Providing day-to-day management and oversight of operational delivery

4.4 Information Technology Security Officer

Information Technology Security Officer is responsible for:

- Acting as a focal point within their organisation for all matters related to information management that are required to support cyber security

- Ensuring that a cyber incident that involved damage or loss is escalated and reported to the appropriate information management response team in your organisation

4.5 Coordinator Governance & Risk Management

Coordinator Governance and Risk Management is responsible for:

- Providing assurance regarding the effectiveness of cyber security controls
- Meeting with the Lead Analyst and Senior Responsible Officer to ensure cyber risk frameworks fit into the Enterprise Risk Framework

4.6 Other roles and responsibilities

3rd party ICT providers

Councils are responsible under the Guidelines for managing cyber security requirements. This includes contract clauses, monitoring and enforcement for 3rd party ICT providers and the ICT security of non-government organisations holding and/or accessing government systems[2]. Council should ensure that 3rd party ICT providers have the following in place to protect government systems outsourced to them or that they may have access to:

- Foundational Requirement 1.5: The third-party organisation has a process that is followed to notify the Council quickly of any suspected or actual security incidents and follows reasonable direction from the Council arising from incident investigations (noting this will vary based on risk profile and risk appetite).
- Foundational Requirement 2.1: The third-party organisation ensures that their staff understand and implement the cyber security requirements of the contract.
- Foundational Requirement 3.1: Any 'Crown Jewel' systems must be covered in the scope of an Information Security Management System (ISMS) or Cyber Security Framework
- Foundational Requirement 3.4: Cyber security requirements are built into the early stages of projects and the system development life cycle (SDLC),including agile projects.
- Foundational Requirement 3.5: Ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data, including processes for internal fraud detection. This does not prevent other contractual obligations being imposed.

5 Foundational Requirements

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

1	Council will implement cyber security planning and governance. Council will
1.1	Allocate roles and responsibilities as detailed in the Guidelines.

1.2	Ensure there is a governance committee at the executive level or equivalent (dedicated or shared) to be accountable for cyber security including risks, plans, reporting and meeting the requirements of the Guidelines.
1.3	Develop, implement and maintain an approved cyber security plan that is integrated with your organisation's business continuity arrangements.
1.4	Include cyber security in their risk management framework and consider cyber security threats when performing risk assessments.
1.5	Be accountable for the cyber risks of their ICT service providers with access to or holding of government information and systems and ensure these providers understand and comply with the cyber security requirements of the contract, including the applicable parts of the Guidelines and any other relevant organisational security policies.
2	**Council will build and support a cyber security culture across their organisation. Council will:**
2.1	Implement regular cyber security awareness training for all employees, contractors and outsourced ICT service providers.
2.2	Increase awareness of cyber security risk across all staff including the need to report cyber security risks.
2.3	Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied.
2.4	Ensure that appropriate access controls and security screening processes are in place for people with privileged access or access to sensitive or classified information.
2.5	Receive and/or provide information on security threats and intelligence with Cyber Security NSW and cooperate with NSW Government to enable management of government-wide cyber risk.
3	**Councils will manage cyber security risks to safeguard and secure their information and systems. Councils should:**
3.1	Implement an Information Security Management System (ISMS), Cyber Security Management System (CSMS) or Cyber Security Framework (CSF).
3.2	Implement the ACSC Essential Eight.
3.3	Classify information and systems according to their business value (i.e. the impact of loss of confidentiality, integrity or availability).
3.4	Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects. Any upgrades to existing systems must comply with your organisation's cyber risk tolerance.

3.5	Audit trail and activity logging records are determined, documented, implemented and reviewed for new ICT systems and enhancements.
4	**Councils should improve their resilience including their ability to rapidly detect cyber incidents and respond appropriately. Councils should:**
4.1	Have a current cyber incident response plan that integrates with the agency incident management process and the *NSW Government Cyber Incident Response Plan*.
4.2	Exercise their cyber incident response plan at least every year.
4.3	Ensure that ICT systems and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.
4.4	Report cyber security incidents to their CISO and/or Cyber Security NSW. If relevant, ensure incident reporting is compliant with Federal reporting requirements.

6 The Essential Eight

The ACSC recommends that organisations implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems. Please check the ACSC website for the latest version of the Essential Eight and maturity model· https://www.cyber.gov.au/acsc/view-all-content/essential-eight

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

Mitigation Strategy	What	Why
Application control	Checking programs against a pre-defined approved list and blocking all programs not on this list	So unapproved programs including malware are unable to start and preventing attackers from running programs which enable them to gain access or steal data

Patch applications	Apply security fixes/patches or mitigations (temporary workarounds) for programs within a timely manner (48 Hours for internet reachable applications). Do not use applications which are out-of-support and do not receive security fixes	Unpatched applications can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems
Configure MS Office macro settings	Only allow Office macros (automated commands) where there is a business requirement and restrict the type of commands a macro can execute. Also monitor usage of Macros.	Macros can be used to run automated malicious commands that could let an attacker download and install malware
User application hardening	Configure key programs (web browers, office, PDF software, etc) to apply settings that will make it more difficult for an attacker to successfully run commands to install malware	Default settings on key programs like web browsers may not be the most secure configuration. Making changes will help reduce the ability of a compromised/malicious website from successfully downloading and installing malware.
Restrict administrative privileges	Limit how accounts with the ability to administer and alter key system and security settings can be accessed and used.	Administrator accounts are 'the keys to the kingdom' and so controlling their use will make it more difficult for an attacker to identify and successfully gain access to one of these accounts which would give them significant control over systems
Patch operating systems	Apply security fixes/patches or temporary workarounds/mitigations for operating systems (e.g. Windows) within a timely manner (48 Hours for internet reachable applications). Do not use versions of an Operating system which are old and/or not receiving security fixes	Unpatched operating systems can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems
Multi-factor authentication	A method of validating the user logging in by using additional checks separate to a password such as a code from an SMS/Mobile application or fingerprint scan	Unpatched operating systems can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems

Regular backups	Regular backups of important new or changed data, software and configuration settings, stored disconnected and retained for at least three months. Test the restoration process when the backup capability is initially implemented, annually and whenever IT infrastructure changes.	To ensure information can be accessed following a cyber-security incident e.g. a ransomware incident).

7 Definition/Glossary

Item	Definition
General Manager	A general manager's role to implement Council decisions and carry out functions imposed by legislation (Local Government Act 1993).
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 Whitelisting	An approach in which only an explicitly defined set of applications are permitted to execute on a system
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	Making information consistently and readily accessible for authorised parties
Business Continuity Plan	A business continuity plan is a document that outlines how an organisation can ensure it's critical business functions will either 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
Breach (data)	An incident that results in unauthorised access to, modification or disruption of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms

Breach (security)	When data is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Also referred to as a 'Data Spill'
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	Those physical facilities, supply chains, information technologies and communication 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 Australia's ability to conduct national defense and ensure national security. (Security of Critical Infrastructure Act 2018)
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
Cyber crime	Crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It also 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, with risks to the safety of citizens and businesses. Intense media interest, 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 security incidents

Cyber security	Measures used to protect the confidentiality, integrity and availability of systems and information
Disaster Recovery Plan	Outlines an organisation's recovery strategy for how they are going to respond to a disaster
Essential Eight	The Essential Eight are eight essential mitigation strategies that organisations are recommended to implement as a baseline to make it much harder for adversaries to compromise systems
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
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

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)
Incident Response Plan	A plan for responding to cyber security incidents
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
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
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 – Note: The NSW whole-of-government cyber function was renamed 'Cyber Security NSW', and the '*Government Chief Information Security Officer'* was renamed *NSW Chief Cyber Security Officer* in May 2019
Operational Technology	Operational technology is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events
Partial Backup	A partial restoration would be anything less than a full restoration. The expectation would be any 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
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	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, Port Authority of NSW, Sydney Water, Landcom, Water NSW
Supply Chain	Supply chain is 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 includes 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

8 Relevant Legislation, Policies, Procedures and other useful information

Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)
https://www.legislation.nsw.gov.au/view/html/inforce/current/act-1998-133

Health Records and Information Privacy Act 2002 (HRIP Act)
https://www.legislation.nsw.gov.au/#/view/act/2002/71

NSW Government Information Classification, Labelling and Handling Guidelines 2020
https://www.digital.nsw.gov.au/policy/managing-data-information/information-classification- handling-and-labeling-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/Pages/default.aspx

Information Security Manual https://acsc.gov.au/infosec/ism