Cyber security

Policy

Approved by Council: 19/02/2025

To set out the mandatory requirements for management of cyber security risks to information and systems.

Policy statement

To ensure Council's Information and Communication Technology ('ICT') systems are fit-for-the-future, Council has adopted a hybrid operating model known as a 'cloud first' strategy. This strategy will reduce the risks associated with on-premise systems and better promote achievementof Council's business objectives.

A robust and mature cyber security program is critical to the achievement of Council's business objectives. Council's cyber security program consists of a number of mandatory requirements and has been informed by and is modelled on the NSW Government Cyber Security policy which is recommended as a foundation of strong practice for local councils.

This policy applies to all systems, people and processes that constitute the Council's information systems including, but not limited to, councillors, employees, ICT service providers, contractors, and all other parties with access to Council's ICT systems.

Mandatory requirement 1

LEAD	*By implementing cyber security planning and governance.*

1.1 Adopt and maintain an Information Security Incident and Data Breach Response Plan that integrates with Council's Business Continuity Plan.

1.2 Develop and implement Security procedures that support the objectives of this Policy; to be reviewed annually.

1.3 Develop and maintain an ICT Risk Register which will include cyber security risks.

1.4 Ensure cyber security minimum requirements are documented and built into procurement governance including requirements for bespoke ICT systems and assets.

1.5 Require third party ICT service providers, as a condition of engagement, to adhere to requirements for, among other things, the reporting and investigation of any suspectedor actual security incident.

1.6 Consider cyber security threats when performing risk assessments and include 'high'and 'extreme' risks in Council's overall risk management framework.

Mandatory requirement 2

PREPARE	*By promoting organisation-wide cyber security culture and accountability.*

2.1 Implement regular cyber security education for all employees and contractors, including

roles and responsibilities outlined in this policy, and expectations on reporting of cyber security risks.

2.2 Ensure that third party ICT service providers understand and implement Council's cyber security requirements as a condition of contract.

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 approval and screening processes are appropriate and consistently used to govern and regulate access to Council systems and information using the principle 'minimum access required to do the job'. This includes the timely removal of access when no longer required or when employment is terminated.

2.5 Share information on security threats and intelligence with Cyber Security NSW and cooperate across NSW Government to enable management of government-wide cyber risk.

Mandatory requirement 3

PREVENT	*By safeguarding information and systems*

3.1 Ensure all devices, ICT systems and physical assets are secured in accordancewith the Security procedures.

3.2 Undertake the design, development, deployment, and maintenance of new ICT systems, or enhancements to existing ICT systems or decommissioning of ICT systems, in accordance with the Security procedures and in consultation with theICT Manager.

3.3 Ensure all new ICT systems, or enhancements to existing ICT systems, comply with national standards and any relevant international standards where appropriate.

3.4 Implement Security Incident Management Response procedures.

3.5 Ensure ICT systems have the capability to produce an audit trail and activity logging to enable the assessment of the integrity of data and fraud detection.

Mandatory requirement 4

DETECT, RESPOND, RECOVER	*By improving business resilience and the ability to rapidly detect and respond to Cyber Incidents or Cyber Crisis.*

4.1 Test the Cyber Incident Response Plan annually and report results to the Leadership Team and other relevant stakeholders, as required.

4.2 Deploy monitoring processes and tools to allow for adequate incident identification and response.

4.3 Report confirmed Cyber Incidents or Cyber Crisis to Cyber Security NSW.

4.4 Evaluate effectiveness of Cyber Incident Response Plan following a Cyber Incident or Cyber Crisis and identify and implement improvements.

4.5 Maintain a register of Cyber Incidents and Cyber Crisis to allow identification ofpatterns and trends and high-risk areas that need targeted risk treatment.

Mandatory requirement 5

REPORT	*By reporting against the requirements outlined in the policy and other cyber security measures for the previous financial year.*

5.1 Provide status updates on control measures implemented for any cyber security risks classified as 'moderate', 'high', 'extreme' to each meeting of Council's ARIC.

5.2 Report suspected or actual Cyber Incident or Cyber Crisis to the first ARIC meeting following the breach or after becoming aware of the suspected breach.

5.3 Provide statistical reporting on Cyber Incidents or Cyber Crisis concerning Council to ARIC annually.

5.4 Provide reporting to the Leadership Team and ARIC (as required) regarding non-conformance with this policy and Security procedures.

1. ROLES AND RESPONSIBILITIES

- **Council staff, Councillors, contractors/consultants and service providers** are responsible for:
  - Managing the risk associated with ICT systems and information and ensuring compliance with policies, standards, procedures, and guidelines.
  - Reporting non-conformance with this policy and/or suspected or actual Cyber Incidents or Cyber Crisis immediately to the ICT Manager.
- **Audit Risk and Improvement Committee** is responsible for overseeing and advising the General Manager and the governing body of:
  - Appropriateness and/or effectiveness of internal controls, processes and procedures for the risk Council faces in relation to cyber security.
  - Compliance, or otherwise, of stakeholders with Council's policy and procedures for managing cyber security risk including reporting requirements.
  - Trends or patterns evidenced in the occurrence(s) of Cyber Incidents or CyberCrisis.
- **ICT Manager** is responsible for:
  - Overseeing the implementation, adherence to and review of this policy.
  - Defining and implementing an Information Security Incident and Data Breach Response Plan.
  - Developing a cyber security strategy, architecture, and risk management processand incorporating these, with the assistance of the Enterprise Risk Coordinator, into Council's current risk management framework and processes.
  - Assessing and providing recommendations on any exemptions to this policy and Security procedures.
  - Attending ARIC meetings to assist in meeting reporting requirements, as required.
  - Taking the lead in investigating, responding to and reporting on suspected or actual

Cyber Incidents and Cyber Crisis.
- Reporting Cyber Incidents and Cyber Crisis to Cyber Security NSW and ARIC.
- Representing Council on whole-of-government collaboration, advisory or steering groups established by Cyber Security NSW.
- Establishing training and awareness programs to increase employee cyber security capability.
- Maintaining the register of Cyber Incidents or Cyber Crisis.

- **Risk and Assurance Specialist** is responsible for:
  - Assisting the ICT Manager in analysing cyber security risks.
  - Ensuring the effectiveness of cyber security controls are reviewed as part of a Council-wide program.

2. DEFINITIONS

ARIC - Audit, Risk and Improvement Committee.

Cyber Incident - moderate or higher impact to services, information, assets, reputation or relationships. Public visibility of impacts through service degradation or public disclosure of information/systems breaches, with economic impacts.

Cyber Crisis – major disruption 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.

ICT - Information and Communications Technology, 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.

Security Procedures - Council's internal cyber security procedures including both functional and assurance requirements within a product, system, process or technology environment.

Contact officer
ICT Manager.

Related documents

Policies
Code of Conduct
Privacy Management
Risk Management

Procedures
D24/17946 - IT Acceptable Use Standard
D23/29642 – Data Breach Plan
D23/7704 – Information and ICT Systems – Access and Use

Legislation
Privacy and Personal Information Protection Act 1998 (NSW)
Health Records and Information Privacy Act 2002 (NSW)
Government Information (Public Access) Act 2009 (NSW
State Records Act 1998 (NSW)

Other

Australian Cyber Security Centre (ACSC) Essential 8:
https://www.cyber.gov.au/publications/essential-eight-explained

NSW Government Digital – 'Mandatory 25' Requirements for Cyber Security:
https://www.digital.nsw.gov.au/policy/cyber-security-policy/mandatory-requirements

File No.: CM: D20/2822		Next review date: 4 years	
Version	Purpose and description	Date adopted by Council	Resolution No.
1.0	Initial draft 14/09/2020		
2.0	Draft reviewed 27/01/2021		
3.0	Final review 30/08/2021		
4.0	Adopted Council meeting	20/10/2021	54/21
4.1	Policy transferred to a new template	07/02/2025	
5.0	Adopted Council meeting	19/02/2025	08/25