Appendix four – Cyber Security Guidelines – Local Government foundational requirements

This table includes the foundational requirements in the December 2022 version of the Cyber Security NSW Cyber Security Guidelines – Local Government as these were the relevant requirements during the audit period. Cyber Security NSW's website contains the latest Guidelines and requirements.

Lead

1	**Councils should implement cyber security planning and governance. Councils should:**
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.

Prepare

2	**Councils should build and support a cyber security culture across their organisation. Councils should:**
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.

Prevent

3	**Councils should 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.

Detect, respond, recover

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.

Source: Cyber Security Guidelines – Local Government, December 2022.