Appendix two – Cyber Security Policy mandatory requirements

Version three of the NSW Cyber Security Policy was in effect for the 2020 reporting period. The below is a list of the 25 mandatory requirements that were in effect at the time of this audit.

Requirement 1	**Agencies must implement cyber security planning and governance. Agencies must:**
1.1	Allocate roles and responsibilities as detailed in this policy.
1.2	Ensure there is a governance committee at the executive level (dedicated or shared) to be accountable for cyber security including risks, plans and meeting the requirements of this policy. Agencies need to consider governance of ICT systems and OT to ensure no gaps in cyber security related to items such as video surveillance, alarms, life safety and building management systems that use automated or remotely controlled or monitored assets including industrial Internet of Things (IoT) devices.
1.3	Have an approved cyber security plan to manage the agency's cyber security risks, integrated with business continuity arrangements. This must include consideration of threats, risks and vulnerabilities that impact the protection of the agency's information, ICT assets and services.
1.4	Consider cyber security threats when performing risk assessments and include high and critical risks in the agency's overall risk management framework.
1.5	Be accountable for the cyber risks of their ICT service providers and ensure the providers comply with the applicable parts of this policy and any other relevant agency security policies. This must include providers notifying the agency quickly of any suspected or actual security incidents and following reasonable direction from the agency arising from incident investigations.

Requirement 2	**Agencies must build and support a cyber security culture across their agency and NSW Government more broadly. Agencies must:**
2.1	Implement regular cyber security education for all employees and contractors, and ensure that outsourced ICT service providers understand and implement the cyber security requirements of the contract.
2.2	Increase awareness of cyber security risk across all staff including the need to report cyber security risk.
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 people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when they no longer need to have access, or their 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.

Requirement 3	Agencies must manage cyber security risks to safeguard and secure their information and systems. Agencies must:
3.1	Implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as an agency's 'crown jewels'. The ISMS or CSF should be compliant with, or modelled on, one or more recognised ICT/OT standard (see guideline for more information).
3.2	Implement the ACSC Essential 8.
3.3	Classify information and systems according to their importance (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the requirements of the NSW Government Information Classification Labelling and Handling Guidelines and: • assign ownership • implement controls according to their classification and relevant laws and regulations • identify the agency's 'crown jewels' and report them to Cyber Security NSW as per mandatory requirement 5.4.
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.
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.

Requirement 4	Agencies must improve their resilience including their ability to rapidly detect cyber incidents and respond appropriately. Agencies must:
4.1	Have a current cyber incident response plan that integrates with the agency incident management process, the NSW Government Cyber Incident Response Plan.
4.2	Test their cyber incident response plan at least every year, and involve their senior business and IT executives, functional area coordinators (if applicable), as well as media and communication teams.
4.3	Deploy monitoring processes and tools to allow for adequate incident identification and response.
4.4	Report cyber security incidents to Cyber Security NSW according to the NSW Cyber Security Response Plan.
4.5	Participate in whole-of-government cyber security exercises as required.

Requirement 5	Agencies must report against the requirements outlined in this policy and other cyber security measures. Agencies must:
5.1	Report annually to their cluster CISO, or Cyber Security NSW, their compliance with the mandatory requirements in this policy, in the format provided by Cyber Security NSW. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.
5.2	Report annually to their cluster CISO, or Cyber Security NSW, their maturity against the ACSC Essential 8, in the format provided by Cyber Security NSW. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.
5.3	Report annually to their cluster CISO, or Cyber Security NSW, the agency's cyber security risks with a residual rating of high or extreme, in the format provided by Cyber Security NSW by 31 August.
5.4	Report annually to their cluster CISO, or Cyber Security NSW, the agency's 'crown jewels'. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.
5.5	Provide a signed attestation to Cyber Security NSW by 31 August each year and include a copy of your attestation in your annual report, as outlined in section 4. If your agency does not complete an annual report, an attestation must still be completed and signed off by your agency head and submitted to your cluster CISO.