Department of Customer Service

NSW Cyber Security Policy 2023-2024

Version 6.0

NSW GOVERNMENT

Contents

1 Policy statement

1.1 Overview

Having strong cyber security capability and a culture of responsibility is an important component of the NSW Beyond Digital Strategy.[1] It enables the effective use of emerging technologies and ensures confidence in the services provided by the NSW 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.

Cyber security is becoming more important as cyber risks continue to evolve. Rapid technological change in the past decade has resulted in increased cyber connectivity and more dependency on cyber infrastructure.

The NSW Cyber Security Policy is reviewed annually and updated based on agency feedback and emerging cyber security threats and trends.

1.2 Purpose

The NSW Cyber Security Policy outlines the Mandatory Requirements to which all NSW Government agencies must adhere to. Each Mandatory Requirement is supported by detailed requirements. These detailed requirements are a baseline of minimum requirements expected of agencies. The policy aims to reduce impacts to confidentiality, integrity and availability of services and information, by ensuring cyber security risks to the information and systems of NSW Government departments and agencies are appropriately managed. This policy is designed to be read by Agency Heads and all Executives, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), or equivalent, and audit and risk teams.

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

1.3 Scope

The NSW Cyber Security Policy applies to all NSW Government departments and public service agencies, including statutory authorities, and all NSW Government entities that submit an annual report to a Secretary of a lead department or portfolio, direct to a Minister or direct to the Premier. In this policy, references to "lead portfolio departments" or "portfolios" mean the departments listed in Part 1, Schedule 1 of the *Government Sector Employment Act 2013*.[2] The term "agency" is used to refer to any or all NSW Government departments, public service agencies and statutory authorities. References to employees and contractors applies to people who have access to NSW Government systems and/or information and communications technology (ICT).

The NSW Cyber Security Policy applies to:

information, data and digital assets created and managed by the NSW public sector, including outsourced information, data and digital assets

ICT systems managed, owned or shared by the NSW public sector, including cloud services

operational technology (OT) and Internet of Things (IoT) devices that handle government data, government-held citizen data or provide government services.

The NSW Cyber Security Policy is not mandatory for state-owned corporations, non-government organisations, local government or universities. However, it is recommended for adoption by these organisations as a foundation of strong cyber security practice. Cyber Security NSW can work with these types of organisations to help implement the policy.

Local government can consider voluntary self-assessment against the Cyber Security Guidelines – Local Government[3]. These are foundational cyber security requirements for local government modelled off the NSW Cyber Security Policy. These guidelines will be updated annually, in accordance with the annual review of the NSW Cyber Security Policy.

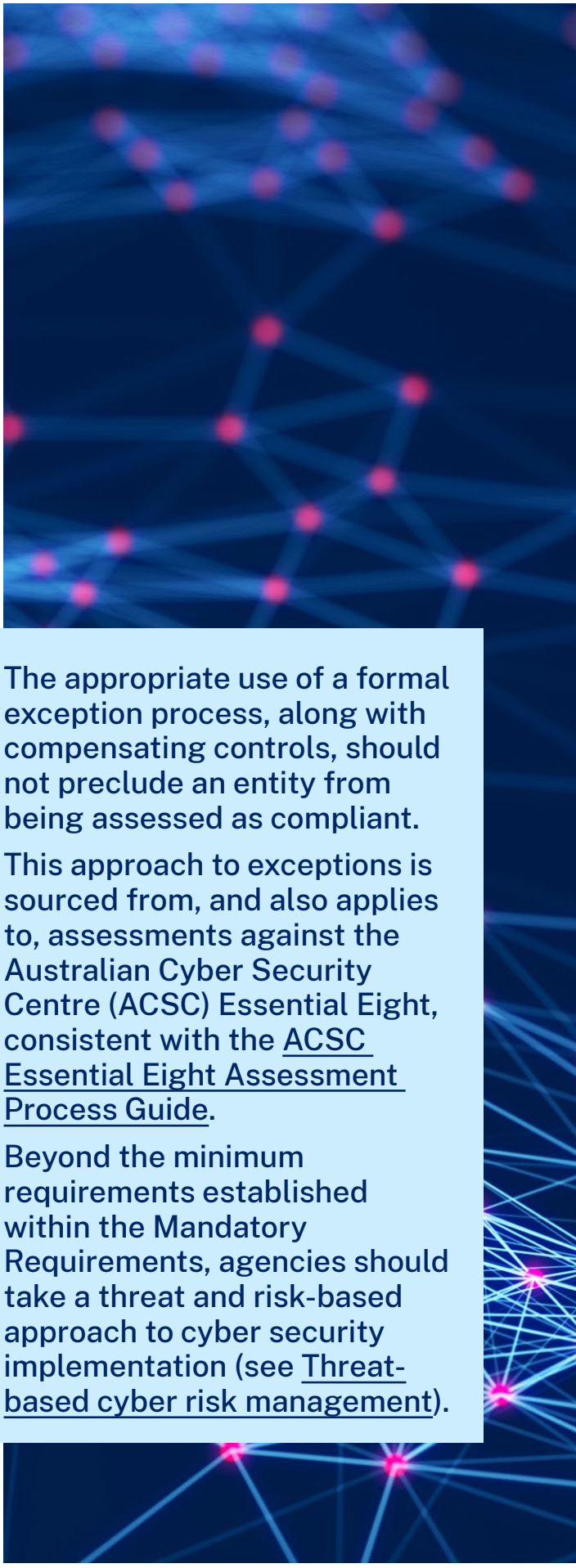
2 https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2013-040
3 https://www.olg.nsw.gov.au/council-circulars/22-39-release-of-cyber-security-guidelines-for-nsw-local-government/

1.4 Risk-based implementation of the NSW Cyber Security Policy

Whilst the NSW Cyber Security Policy applies across the entire agency and sets out minimum requirements for agencies, not all requirements can be uniformly implemented across the defined scope. For the scope of the Mandatory Requirements, agencies should ensure any use of exceptions for a system are documented and approved by an appropriate authority through a formal process.

Documentation for exceptions should include the following:

- detail, scope and justification for exceptions
- detail of compensating controls associated with exceptions, including:
  - detail, scope and justification for compensating controls
  - expected implementation lifetime of compensating controls
  - when compensating controls will next be reviewed
- system risk rating before and after the implementation of compensating controls
- any caveats placed on the use of the system as a result of exceptions
- acceptance by an appropriate authority of the residual risk for the system
- when the necessity of exceptions will next be considered by an appropriate authority (noting exceptions should not be approved beyond one year).



The appropriate use of a formal exception process, along with compensating controls, should not preclude an entity from being assessed as compliant.

This approach to exceptions is sourced from, and also applies to, assessments against the Australian Cyber Security Centre (ACSC) Essential Eight, consistent with the ACSC Essential Eight Assessment Process Guide.

Beyond the minimum requirements established within the Mandatory Requirements, agencies should take a threat and risk-based approach to cyber security implementation (see Threat-based cyber risk management).

1.5 Assistance implementing the NSW Cyber Security Policy

Cyber Security NSW can provide guidance documents and toolkits to assist agencies with implementation of the NSW Cyber Security Policy. For copies of these documents, or for advice regarding the policy, please contact info@cyber.nsw.gov.au

Agencies must identify their central portfolio CISO and maintain contact with them throughout the NSW Cyber Security Policy reporting period, especially if they require assistance meeting the reporting requirements outlined below.

1.6 Exemptions and extensions

Exemptions to the NSW Cyber Security Policy, and extensions to reporting, will only be considered in exceptional circumstances. To seek an exemption or extension, contact your portfolio CISO in the first instance. If the exemption or extension request is deemed valid by your portfolio CISO, they will contact Cyber Security NSW on your behalf.

Independent agencies may seek to raise an exemption or extension request directly with Cyber Security NSW but are expected to advise their portfolio CISO of the request.

Requests must be made in writing to Cyber Security NSW via info@cyber.nsw.gov.au, prior to 30 September.

2 Reporting and attestation

2.1 Reporting obligations

Portfolio CISOs, and/or central portfolio cyber security teams, are to coordinate NSW Cyber Security Policy reporting across their portfolio.

By 30 June each year, portfolio CISOs are to provide Cyber Security NSW with an updated list of all agencies in their portfolio, with confirmation of how they will be reporting, in a template provided by Cyber Security NSW.

By 31 October each year, Cyber Security NSW must be provided with a report for each agency, either via the portfolio CISO or directly to Cyber Security NSW. Reporting must include:

01

an assurance assessment against all Mandatory Requirements in the NSW Cyber Security Policy for the previous financial year

02

cyber security risks with a residual rating of high or extreme[4]

03

an attestation on cyber security.

Agencies have an obligation to ensure reporting reflects an accurate and verifiable assessment of the Mandatory Requirements, as well as implementation of other requirements in the NSW Cyber Security Policy. As such, agencies must:

- compile and retain, in accessible form, evidence that demonstrates the basis of their assurance assessment
- resolve discrepancies and inaccuracies identified in their reporting, including discrepancies between their reported control implementation and scope, and what is demonstrable with evidence
- ensure their attestations refer to any departures from the requirements of the NSW Cyber Security Policy (see Attestation).

2.2 Mandatory Requirement reporting

By 31 October each year, Cyber Security NSW must be provided with a report for each agency, either via the portfolio CISO or directly to Cyber Security NSW. Agencies must complete an assurance assessment against the Mandatory Requirements in the NSW Cyber Security Policy. It is possible to have a response of “not applicable” with an explanation that is acceptable to your agency (see Exemptions and extensions).

4 As sourced from the agency’s risk register or equivalent and as required in TPP20-08 Internal Audit and Risk Management Policy for the NSW Public Sector: https://www.treasury.nsw.gov.au/documents/tpp20-08-internal-audit-and-risk-management-policy-general-government-sector

2.3 Risk reporting

By 31 October each year, Cyber Security NSW must be provided with a list of the high or extreme residual cyber risks for each agency, in a format provided by Cyber Security NSW. This list can be provided via the portfolio CISO or directly to Cyber Security NSW. If an agency does not have any high or extreme residual cyber risks, they can provide a response of "not applicable".

Residual risks must be tracked and managed in a risk register and reviewed in accordance with the agency's enterprise risk management framework. Risks exceeding the risk appetite and risk tolerance must be escalated to the Agency Head, or authorised officer who is responsible for risk acceptance.

As part of the threat-based risk management component of the NSW Cyber Security Policy, agencies are encouraged to also report on key threats identified by the agency, as well as associated risks and mitigations, using the provided template.

2.4 Attestation

Agencies must provide a signed annual attestation for the previous financial year to Cyber Security NSW by 31 October each year. If more than one agency is included in the attestation, a list of all the agencies should be detailed within the attestation itself.

The attestation should address:

- whether the agency has assessed its cyber security risks
- whether the agency has cyber security residual risks that exceed the agency's risk appetite
- whether the agency has adequately reported its cyber security assessment, in compliance with the NSW Cyber Security Policy
- in the case of machinery-of-government changes, the periods of time entities are responsible for respective controls
- whether cyber security is appropriately addressed at agency governance forums
- what the agency is doing to continuously improve the management of cyber security governance and resilience.

In the attestation, the Agency Head must sign off on any Mandatory Requirements that have been assessed as not met or partially met in the assurance assessment (noting that agencies are not expected to have fully met all Mandatory Requirements in the 2023-2024 financial year of NSW Cyber Security Policy reporting, as this reporting year is intended as a baseline only).

There is no expected format for the attestation, as long as the above requirements are explicitly addressed.

3 Mandatory Requirements

The Mandatory Requirements are a minimum baseline for NSW Government agencies to implement. The baseline contains a combination of management and governance practices required to establish an effective cyber security program, as well as key systems-based controls to improve cyber hygiene and help agencies better protect themselves against common threats. This includes incorporation of the ACSC Essential Eight mitigation strategies (Mandatory Requirements 3.3 – 3.10).

The Mandatory Requirements are supported by detailed requirements (see Detailed requirements), which further articulate specific expectations for the practices that are to be implemented and reported on using the assurance assessment.

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 and Risk Committee (ARC) 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 NSW Government agencies.
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.

4 Essential Eight

The ACSC has developed and published the Essential Eight strategies for mitigating cyber incidents. The Essential Eight are embedded in Mandatory Requirements 3.3 to 3.10. Agencies must implement the Essential Eight to applicable ICT environments with a minimum requirement of Level 1 maturity, as part of the baseline set in the Mandatory Requirements. 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 agency as part of the threat-based requirements (see Threat-based cyber risk management).

The Mandatory Requirements aligned to the Essential Eight maturity level 1 in the NSW Cyber Security Policy are mapped to the controls taken from the December 2023 release of the Information Security Manual (ISM).[5] Agencies must report against these, per the Mandatory Requirements. Cyber Security NSW will review changes made on an annual basis for any adjustments to be incorporated for the next reporting period.

The Essential Eight controls are subject to annual review by the ACSC. Updates 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, agencies should assess changes and prioritise implementation of new or adjusted requirements as part of their risk management processes.

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

5 Threat-based cyber risk management

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

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

Agencies 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. Agencies implementing projects with higher cyber security risks must 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 agencies 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 agency
    - 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 agency and sensitivity of information held or processed by the agency.

Cyber Security NSW provides optional threat reporting templates to assist agencies in sharing information on key threats and risks. For copies of these templates, please contact info@cyber.nsw.gov.au.

Establishing effective threat modelling and risk management practices is an ongoing journey involving continuous improvement and will require effective implementation of multiple Mandatory Requirements in order to support these practices. As such, agencies 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 has threat modelling resources available to support agencies with establishing threat modelling in their entity. These resources are optional for agencies to use and not a requirement for implementing the threat-based requirements.

6 Roles and responsibilities

This section outlines the roles and responsibilities an agency should allocate as part of their cyber security function. Please note that:

agencies have flexibility to tailor these roles to their organisational context, but all responsibilities must be allocated and performed regardless of role title

an agency may not have all the roles outlined below

these responsibilities can be allocated to roles not specifically named in the NSW Cyber Security Policy or shared among multiple roles.

6.1 Agency Heads

All Agency Heads[6] (e.g. Commissioners, Chief Executive Officers), including the Secretary of a department, are accountable for:

- ensuring their agency complies with the requirements of the NSW Cyber Security Policy and timely reporting on compliance with the policy
- ensuring their agency develops, implements and maintains an effective cyber security strategy and plan
- determining their agency's risk appetite using the approved whole-of-government Internal Audit and Risk Management Policy[7]
- signing off on any Mandatory Requirements that have been assessed as not met or partially met in the assurance assessment
- appropriately funding, resourcing, prioritising and supporting agency cyber security initiatives, including training and awareness, and continual improvement initiatives to support the NSW Cyber Security Policy
- approving internal security policies as required.

The Secretary of a department is also accountable for:

- appointing or assigning an appropriate senior executive band officer in the agency or across the portfolio with the authority to perform the duties outlined in the NSW Cyber Security Policy – this person should be accountable for cyber security at least at the portfolio level
- appointing or assigning a senior executive band officer with authority for Industrial Automation and Control Systems (IACS) cyber security for the agency or portfolio, if applicable
- ensuring all agencies in their portfolio implement and maintain an effective cyber security program
- supporting the agency's cyber security strategy and plan.

6 The head of the agency listed in Part 2 or 3 of Schedule 1 of the *Government Sector Employment Act 2013*: https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2013-040

7 https://www.treasury.nsw.gov.au/documents/tpp20-08-internal-audit-and-risk-management-policy-general-government-sector

6.2 ICT & Digital Leadership Group (IDLG)

The IDLG is chaired by the NSW Government Chief Information and Digital Officer (GCIDO) and is attended by the CIOs in the NSW Government. The IDLG is responsible for:

- endorsing the NSW Cyber Security Policy and any updates
- ensuring the implementation of the NSW Cyber Security Policy across the NSW Government
- reviewing the summarised agency/portfolio reports against the NSW Cyber Security Policy's Mandatory Requirements
- providing leadership, support and resources for the NSW Cyber Security Policy and advocating organisational commitment to improving the cyber security culture of the agency/portfolio.

6.3 NSW Chief Cyber Security Officer (NSW CCSO)

The NSW CCSO is accountable for:

- creating and implementing the NSW Cyber Security Strategy
- building a cyber-aware culture across the NSW Government
- reporting on consolidated agency compliance and maturity
- chairing the NSW Government Cyber Security Steering Group (CSSG)
- consulting with agencies and providing advice and assistance to the NSW Government on cyber security, including improvements to the NSW Cyber Security Policy, capability and capacity
- recommending and recording exemptions to any part of the NSW Cyber Security Policy
- representing the NSW Government on cross-jurisdictional matters relevant to cyber security
- assisting agencies in sharing information on security threats and cooperating on security threats and intelligence to enable management of government-wide cyber risk
- receiving, collating and reporting on high cyber risks and monitoring cyber incident reports across the NSW Government
- creating and implementing the NSW Government cyber incident response arrangements
- coordinating the NSW Government response to significant cyber incidents and cyber crises.

6.4 Chief Information Security Officers (CISOs) or Chief Cyber Security Officers (CCSOs)

All CISOs and CCSOs, or staff with those responsibilities, are responsible for:

- defining and implementing a cyber security plan for the protection of the agency's information and systems
- developing a cyber security strategy, architecture and risk management process, and incorporating these into the agency's current risk framework and processes
- deciding on risk treatment strategies for cyber security within the agency when the identified risk falls outside the acceptable risk tolerance
- implementing policies, procedures, practices and tools to ensure compliance with the NSW Cyber Security Policy
- reviewing and providing recommendations on any exemptions to agency or portfolio information security policies and standards
- NSW Cyber Security Policy reporting
- investigating, responding to and reporting on cyber security incidents to the appropriate agency governance forum and Cyber Security NSW, based on severity definitions provided by Cyber Security NSW

Portfolio CISOs and CCSOs, or staff with those responsibilities, are responsible for:

- supporting agencies in their portfolio to implement and maintain an effective cyber security strategy and program (e.g. via effective collaboration and/or governance forums, advice on budgeting and resourcing and so forth)
- managing the portfolio level cyber security budget (where applicable), and ensuring that resources are allocated to address cyber security needs
- applying for relevant programs/funding, e.g. Digital Restart Fund, ACSC uplift programs etc.

6.5 Chief Information Officer (CIO) or Chief Operating Officer (COO)

CIOs or COOs, or staff with those responsibilities, are accountable for:

- working with CISOs and across their agency to implement the NSW Cyber Security Policy, including allocating sufficient resources and funding to manage the identified cyber security risks under their remit
- implementing a cyber security strategy and plan that includes consideration of threats, risks and vulnerabilities that impact the protection of the agency's information and systems within the agency's cyber security risk tolerance
- ensuring that all staff, including 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
- assisting 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.

6.6 Information Security Manager, Cyber Security Manager or Senior Responsible Officer

Information Security Managers, Cyber Security Managers or Senior Responsible Officers are responsible for the following within their agency or portfolio:

- managing and coordinating the response to cyber 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 lifecycle 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.

6.7 Information Management Officer

A portfolio or agency should have a person or persons who fulfil the role of Information Management Officer. The Information Management Officer undertakes information and records management activities to ensure all information and records are managed in accordance with the agency's recordkeeping plan, policies, processes and procedures. They are responsible for:

- acting as a focal point within their agency 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 their agency.

6.8 Privacy Officer

Agencies should have a person who fulfils the role of Privacy Officer, as recommend by the Information and Privacy Commission NSW (IPC NSW).[8] The role is responsible for:

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

8 https://www.ipc.nsw.gov.au/privacy/agencies/role-privacy-contact-officers

6.9 Internal audit

Agency internal audit teams are responsible for:

- validating that the cyber security strategy and plan meets the agency's business goals and objectives, and ensuring the plan supports the agency's cyber security strategy
- regularly reviewing their agency's adherence to the NSW Cyber Security Policy and cyber security controls
- providing assurance regarding the effectiveness of cyber security controls
- reporting results of audit and assurance activities to the Audit and Risk Committee and Agency Head, as required.

6.10 Risk

Agency risk teams are responsible for:

- aligning cyber security with organisational goals and objectives
- conducting risk assessments to identify and evaluate potential cyber security threats and vulnerabilities
- managing cyber security risks within an agency and those associated with third-party service providers
- integrating cyber security into the agency's overall risk management framework and risk appetite
- meeting with the portfolio CISO to ensure cyber risk frameworks are aligned with the enterprise risk framework.

6.11 Agency staff

Agency staff should contribute to an agency'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.

6.12 Third-party service providers

Agencies are responsible for managing cyber security requirements and risks posed by third-party service providers. The scope of this 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.

Mandatory Requirement 1.10 sets out minimum expectations for third-party security risk management including detailed requirements for use of contract clauses, monitoring and enforcement for in-scope third-party service providers.

Agency 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, agencies may consider including the following in new procurement processes and contracts, in accordance with NSW Government's ICT Purchasing Framework[9]:
    - accountability for suspected or actual security incidents or breaches to any data, systems infrastructure or processes used in its arrangement, and ensuring all 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 agency data confidentiality, integrity and availability 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 agency processes for requesting access each time it is required, and agencies should consider revoking access whenever it is not in use

9 https://info.buy.nsw.gov.au/resources/ICT-Purchasing-Framework

Existing contracts may not have appropriate contractual mechanisms to enable agencies to effectively exercise their responsibilities in relation to this section. Where this is the case, the agency 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, agencies 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 agency's risk management framework.

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

- Mandatory Requirement 1.10.1 – Establish and maintain an inventory of third-party service providers, including ICT service providers.
- Mandatory 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).
- Mandatory 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.
- Mandatory 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.
- Mandatory Requirement 3.2.1 – Establish a process for granting, maintaining and revoking access for agency systems, applications and information to ensure authorised access only.
- Mandatory 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.
- Mandatory 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.
- Mandatory 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.

6.13 NSW Government shared service providers

Any departments, agencies or statutory authorities that provide services covered by the NSW Cyber Security Policy must provide reporting information to entities using their services to ensure accountability and enable effective third-party risk management. Responsibilities include reporting:

- security to all affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities, in the shared service provider's implementation of the NSW Cyber Security Policy, and
- any Mandatory Requirements that are not met or partially met, considering compensating controls.

7 Useful links

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*
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-2021-02-nsw-cyber-security-Policy/	*DCS-2021-02 NSW Cyber Security Policy*

Reference	Document Name
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 – Department of 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*

Reference	Document Name
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.oaic.gov.au/privacy/australian-privacy-principles-guidelines/	*ISO 22301 Societal Security – Business continuity management systems – Requirements*
https://www.iso.org/standard/75106.html	*ISO 27031 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*
https://www.iso.org/standard/44374.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*
https://www.nist.gov/publications/zero-trust-architecture	*NIST Special Publication 800-207 – Zero Trust Architecture*
Cybersecurity & Infrastructure Security Agency	
https://www.cisa.gov/zero-trust-maturity-model	*Zero Trust Maturity Model*
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*

8 Glossary

Item	Definition
Agency Heads	a) In the case of a Department – the Secretary of the Department, or b) in any other case – the head of the agency listed in Part 2 or 3 of Schedule 1 of the Government Sector Employment Act 2013.
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.
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.

Item	Definition
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.
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 – 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.
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.
Full backup	Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Item	Definition
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.
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
NSW Government shared service providers	Any departments, agencies or statutory authorities that provide services to entities covered by the NSW Cyber Security Policy.
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.
Portfolio **(also lead portfolio department or department)**	Officially defined as departments in Government Sector Employment Act 2013 Schedule 1, portfolios are the eleven groups into which NSW Government agencies are organised to enhance coordination and provision of related services and policy development. This reflects the machinery-of-government changes effective in 2023.

Item	Definition
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.
Public service agency	Section 3 of the Government Sector Employment Act defines a public service agency as: • a department (listed in Part 1 of Schedule 1 to the Act) • a public service executive agency (being an agency related to a department) • a separate public service agency.
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)
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.

9 Detailed requirements

Mandatory Requirement	Detailed Requirement
1.1 Allocate and perform roles and responsibilities for cyber security.	1.1.1 Ensure the roles and responsibilities set out in the NSW Cyber Security Policy are assigned and performed.
	1.1.2 Define and allocate additional roles and responsibilities for cyber security, and review these according to organisational need.
1.2 Have an executive-level governance committee with appropriate authority to make decisions about cyber security, including OT/IoT.	1.2.1 Have a governance committee (shared or dedicated) at the executive level that: -has appropriate delegations/seniority to make decisions on cyber security matters -meets at least quarterly -ensures that the Agency Head, as the ultimate authority for cyber security, is regularly briefed on cyber security risks, related issues and corrective actions.
	1.2.2 Ensure the committee has an agreed terms of reference with accountability for cyber security governance over information security, as well as the cyber security of ICT, OT and IoT systems.
	1.2.3 Ensure the Agency Head has ultimate accountability for the cyber security of the agency.
1.3 Ensure that the Audit and Risk Committee (ARC) is briefed regularly on cyber security risks, related issues and corrective actions.	1.3.1 Ensure cyber security is a standing item on the agenda at the department or agency audit and risk committees, including risks, related issues and corrective actions.
1.4 Develop and maintain a cyber security strategy.	1.4.1 Develop and maintain a 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.
	1.4.2 The cyber security strategy is endorsed by the Agency Head.
1.5 Develop and maintain formalised plans, policies and processes for cyber security practices.	1.5.1 Develop and maintain plans, policies and processes for managing cyber security risks based on organisational context, the agency's cyber security strategy, and NSW Cyber Security Policy requirements.
1.6 Establish and maintain processes for asset inventory management and identify asset dependencies.	1.6.1 Establish and maintain inventories for enterprise ICT (including cloud), software, OT, IoT and network assets.
	1.6.2 Establish and maintain processes for periodically reconciling accuracy and completeness of asset inventories.
	1.6.3 Establish and maintain processes for managing the lifecycles of assets and software, including risk-managed disposal and replacement of end-of-support assets and software.
	1.6.4 Identify and document external upstream and downstream dependencies of enterprise ICT (including cloud), OT and IoT assets, covering at least Crown Jewel assets.

Mandatory Requirement	Detailed Requirement
1.7 Assess and identify Crown Jewels and classify systems.	1.7.1 Implement a Crown Jewel identification framework and identify Crown Jewel assets.
	1.7.2 Classify systems and information for business value, mission criticality and sensitivity (as defined in the NSW Information Handling & Classification Guidelines).
1.8 Govern the identification, retention and secure disposal of data.	1.8.1 Establish and maintain inventories for data assets covering at least Official: Sensitive classification (as defined in the NSW Information Handling & Classification Guidelines).
	1.8.2 Define data retention requirements (with reference to any applicable legislative and policy requirements) for: categories of data, including minimum and maximum retention timeframes; and, for at least Crown Jewels, conduct periodic reconciliation of data assets against data retention requirements.
	1.8.3 Establish and maintain processes for secure disposal of data and associated assets in accordance with the type of data and its information classification.
1.9 Define risk tolerance, risk appetite and manage cyber security risks.	1.9.1 Define risk appetite and risk tolerance for cyber risks and have the cyber risk appetite approved by the Secretary or relevant Agency Head.
	1.9.2 Ensure cyber security risks in all areas of the agency are identified, assessed, managed, documented and reported as part of (or consistent with) the agency's enterprise risk management framework.
	1.9.3 Ensure the Agency Head or authorised officer has formally approved applicable residual risks where NSW Cyber Security Policy Mandatory Requirements are not implemented and in line with agency's risk management acceptance criteria.
	1.9.4 Escalate unmitigated cyber risks exceeding risk appetite or risk tolerance to delegates in line with the agency's risk management framework or acceptance criteria.
1.10 Identify and manage third-party service provider risks, including shared ICT services supplied by other NSW Government agencies.	1.10.1 Establish and maintain an inventory of third-party service providers including ICT service providers.
	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.
	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.
	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.

Mandatory Requirement	Detailed Requirement
1.11 Establish and maintain vulnerability management processes.	1.11.1 Establish and maintain a vulnerability management process for the identification and triage of technical vulnerabilities.
	1.11.2 Assess alerts from Cyber Security NSW and action alerts applicable to the agency's systems, consistent with the agency's vulnerability management processes.
1.12 Ensure cyber security requirements and impacts are assessed as part of change management processes.	1.12 1 Ensure cyber security requirements are assessed within IT and enterprise change management processes, including impacts to implement and maintain any required cyber security controls.
	1.12.2 Manage changes to cyber security technical controls through enterprise IT change management processes.
	1.12.3 Test applicable cyber security controls and secure configurations upon completion of a significant change and update relevant documentation.
2.1 Implement event logging and continuous monitoring to detect anomalous activity.	2.1.1 Implement and maintain processes to log and monitor critical security events aligning to the threats and risks identified for the organisation, and act on relevant anomalies.
2.2 Maintain a cyber incident response plan and use exercises and post incident reviews to continuously improve the plan	2.2.1 Develop and maintain a cyber incident response plan.
	2.2.2 Exercise the cyber incident response plan at least annually.
	2.2.3 Perform post-incident reviews where results are used to update existing processes and templates.
	2.2.4 Develop and maintain a cyber incident register.
2.3 Report cyber incidents and provide information on threats to Cyber Security NSW.	2.3.1 Establish and maintain agency's incident management procedures. Have a defined workflow that indicates when and where information and intelligence should be shared, which includes reporting of cyber event information to Cyber Security NSW.
	2.3.2 Report all cyber incidents to Cyber Security NSW.
2.4 Include cyber security in business continuity and disaster recovery planning.	2.4.1 Include cyber incident scenarios in business continuity and disaster recovery plans.
	2.4.2 Include continuity of cyber security operations in business continuity and disaster recovery plans.
3.1 Conduct awareness activities, including mandatory awareness training.	3.1.1 Define cyber security awareness training requirements for all staff regarding evolving threats, compliance obligations and secure workplace practices.
	3.1.2 Mandate completion of cyber security awareness training for employees and contractors, both annually and when onboarding.
	3.1.3 Conduct continuous user education regarding evolving threats, compliance obligations and secure workplace practices through awareness activities (outside mandatory training) that align with the defined training plan and cyber risk appetite of the entity.
	3.1.4 Conduct regular phishing simulations.
	3.1.5 Define cyber security awareness training for high-risk roles, including privileged users, finance/HR teams, executives, etc.
	3.1.6 Mandate completion for employees and contractors in high-risk roles both annually and when onboarding.

Mandatory Requirement	Detailed Requirement
3.2 Implement access controls to ensure only authorised access.	3.2.1 Establish a process for granting, maintaining and revoking access for agency systems, applications and information to ensure only authorised access.
	3.2.2 Remove access within a defined period of an employee's termination or the employee no longer needing access to the information or system.
	3.2.3 Conduct routine user access reviews to ensure that access is being removed for terminated staff, inactive accounts and for privileges no longer required upon a role change.
	3.2.4 Establish a continuous improvement process to address identified access control gaps.
3.3 Patch applications (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.

Mandatory Requirement	Detailed Requirement
3.4 Patch operating systems (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 Implement multi-factor authentication (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.

Mandatory Requirement	Detailed Requirement
3.6 Restrict administrative privileges **(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 Implement application control **(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 Securely configure Microsoft Office macro settings **(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 Implement user application hardening **(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.

Mandatory Requirement	Detailed Requirement
3.10 Maintain backups of important data, software and configuration settings (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 Establish and maintain secure configurations.	3.11.1 Unneeded accounts, components, services and functionality of all relevant system categories (e.g. operating systems, application systems, database management systems, etc.) are disabled or removed.
	3.11.2 Default accounts or credentials for operating systems, including pre-configured accounts, are changed.
	3.11.3 Only authorised users are permitted access to modify settings for the security functionality of operating systems.
3.12 Define and implement data security controls.	3.12.1 When manually importing data to systems, the data is scanned for malicious and active content.
	3.12.2 Data at rest is encrypted using an ASD-approved cryptographic algorithm.
	3.12.3 All data communicated over network infrastructure is encrypted.
3.13 Implement email security controls.	3.13.1 Employ email anti-spoofing measures, including use of domain-based message authentication, reporting and conformance (DMARC), Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).
	3.13.2 Email content filtering is implemented to filter potentially harmful content in email bodies and attachments.
	3.13.3 Emails arriving via an external connection where the email source address uses an internal domain, or internal subdomain, are blocked at the email gateway.

Mandatory Requirement	Detailed Requirement
3.14 Implement controls for endpoint protection, including mobile devices.	3.14.1 Antivirus software is implemented on endpoints and servers.
	3.14.2 A software firewall is implemented on endpoints and servers to restrict inbound and outbound network connections to an approved set of applications and services.
	3.14.3 Mobile devices used by staff to access government systems have enforced separation of work data from personal data.
3.15 Implement network security controls.	3.15.1 Networks are segregated into network zones according to the criticality of servers, services and data.
	3.15.2 Default accounts or credentials for network devices, including pre-configured accounts, are changed.
	3.15.3 Prevent connections to or from known malicious endpoints, using a Protective Domain Name System (PDNS) service or other security mechanism.
	3.15.4 Network access controls are implemented to limit network traffic within and between network segments to only those required for business purposes.

Department of Customer Service

2/24 Rawson Place
Haymarket NSW 2000

Office hours:
Monday to Friday
9am - 5pm

E: info@cyber.nsw.gov.au

NSW GOVERNMENT