



Customer
Service

NSW Cyber Security Policy

Document number:

Version number: 4.0



1 Policy Statement

1.1 Overview

Strong cyber security is an important component of the NSW *Beyond Digital Strategy*, enabling the effective use of emerging technologies and ensuring confidence in the services provided by NSW 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. We have also had rapid technological change resulting in increased cyber connectivity and more dependency on cyber infrastructure.

The *NSW Cyber Security Policy* (the policy) replaced the *NSW Digital Information Security Policy* from 1 February 2019. New requirements of the policy include strengthening cyber security governance, identifying an agency's most valuable or operationally vital systems or information ("crown jewels"), strengthening cyber security controls, developing a cyber security culture across all staff, working across government to share security and threat intelligence and a whole of government approach to cyber incident response. The policy is reviewed annually and updated based on agency feedback and emerging cyber security threats.

Agencies must establish effective cyber security policies and procedures and embed cyber security into risk management practices and assurance processes. When cyber security risk management is done well, it reinforces organisational resilience, making entities aware of their risks and helps them make informed decisions in managing those risks. This should be complemented with meaningful training, communications and support across all levels of the agency.

1.2 Purpose

The policy outlines the mandatory requirements to which all NSW government departments and Public Service agencies must adhere, to ensure cyber security risks to their information and systems are appropriately managed. This policy is designed to be read by Agency Heads and all Executives, Chief Information Officers, Chief Information Security Officers (or equivalent) and Audit and Risk teams.

1.3 Scope

This 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 cluster, direct to a Minister, or direct to the Premier. In this policy, references to "lead cluster departments" or "clusters" mean the departments listed in Part 1, Schedule 1 of the *Government Sector Employment Act 2013*. The term "agency" is

used to refer to any or all NSW government departments, Public Service agencies and statutory authorities. Please see guidance for more information.

This policy applies to:

- Information, data and digital assets created and managed by the NSW public sector, including outsourced information, data and digital assets;
- information and communications technology (ICT) systems, and
- Operational Technology (OT) and Internet of Things (IoT) devices that handle government or citizen data or provide critical government services

This policy specifies 25 mandatory requirements that all agencies MUST implement.

Agencies must continually improve their cyber security program. Uplift of cyber security policy maturity should be approached through risk-based decision making to prioritise higher risks.

Agencies that provide critical or higher risk services and hold higher risk information should implement a wider range of controls and be aiming for broader coverage and higher maturity levels. Agencies implementing high risk projects must seek additional guidance, strategies and controls when implementing their security plan, including from supplementary sources mentioned in the useful links section.

This policy is not mandatory for state owned corporations, however it is recommended for adoption in state owned corporations, as well as local councils and universities as a foundation of strong practice.

For the purposes of this policy, references to employees and contractors only applies to people who have access to organisation systems and/or ICT.

1.4 Assistance implementing the Policy

Cyber Security NSW can assist agencies implementing the policy, with an FAQ document and guidelines on several cyber security topics. For copies of these documents or for advice regarding the policy please contact cybersecuritypolicy@customerservice.nsw.gov.au.

Agencies must identify their central cluster Chief Information Security Officer (CISO) and maintain contact with them throughout the policy reporting period, especially if they require assistance meeting the reporting and maturity requirements outlined.

1.5 Exemptions

Exemptions to this policy will only be considered in exceptional circumstances. To seek an exemption, contact your cluster CISO in the first instance. If the exemption request is deemed valid by your cluster CISO they will contact Cyber Security NSW on your behalf.

1.6 Summary of Your Agency's Reporting Obligations

Cluster CISOs, and/or central cluster cyber security teams, are to coordinate policy reporting across the entirety of their cluster. In April each year, Cluster CISOs are to provide Cyber Security NSW with an updated list of all agencies in their cluster and how they will be reporting, in a template provided by Cyber Security NSW.

- By 31 August each year, agency's must submit a report to their cluster CISO, or Cyber Security NSW, in a template provided by Cyber Security NSW, covering the following:
 1. Assessment against all mandatory requirements in this policy for the previous financial year
 2. A maturity assessment against the Australian Cyber Security Centre (ACSC) Essential 8¹
 3. Cyber security risks with a residual rating of high or extreme²
 4. A list of the agencies' "crown jewels"
- Agencies are to include an attestation on cyber security in their annual report and provide a copy to Cyber Security NSW by 31 August each year. 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.

¹ <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained>

² 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/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management>

2 Roles and Responsibilities

This section outlines the roles and responsibilities an agency should allocate as part of their cyber security function. An agency may not have all the roles outlined below. In these instances, the responsibilities must be allocated to another role at equivalent level within the organisation. Whilst agencies have flexibility to tailor these roles to their organisational context, all responsibilities must be allocated and performed. Those changed allocations of responsibilities should be clearly identified when reporting to Cyber Security NSW. See guidance for more information.

2.1 ICT & Digital Leadership Group (IDLG)

The IDLG is chaired by the Government Chief Information and Digital Officer (GCIDO) and is responsible for:

- Approving the policy and any updates
- Ensuring its implementation across NSW Government
- Reviewing the summarised agency/cluster reports against the policy's mandatory requirements

2.2 Agency Heads

The Secretary of a department is accountable for:

- Appointing or assigning an appropriate senior executive band officer in the agency or across the cluster, with the authority to perform the duties outlined in this policy – this person should be dedicated to security at least at the cluster level
- Appointing or assigning a senior executive band officer with authority for Industrial Automation and Control Systems (IACS) cyber security for the agency or cluster (if applicable)
- Ensuring all agencies in their cluster implement and maintain an effective cyber security program
- Supporting the agency's cyber security plan

All Agency Heads³ (e.g. Commissioners, Chief Executive Officers), including the Secretary of a department, are accountable for:

- Ensuring their agency complies with the requirements of this policy and timely reporting on compliance with the policy
- Ensuring their agency develops, implements and maintains an effective cyber security plan and/or information security plan

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

- Ensuring CISOs (or equivalent) and a senior executive band officer for IACS (if applicable) attend the agency's risk committee meetings as advisors or committee members
- Determining their agency's risk appetite using the approved whole-of-government Internal Audit and Risk Management Policy⁴
- Appropriately resourcing and supporting agency cyber security initiatives including training and awareness and continual improvement initiatives to support this policy
- Approving internal security policies as required

2.3 Chief Information Security Officers (CISO) or Chief Cyber Security Officers (CCSO)

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 incorporate these into the agency's current risk framework and processes
- Assessing and providing recommendations on any exemptions to agency or cluster information security policies and standards
- Attending agency or cluster risk committee meetings, when invited by the Audit and Risk Committee (ARC)
- Implementing policies, procedures, practices and tools to ensure compliance with this policy
- Investigating, responding to and reporting on cyber security events
- Reporting cyber incidents to the appropriate agency governance forum and Cyber Security NSW based on severity definitions provided by Cyber Security NSW
- Representing their agency on whole-of-government collaboration, advisory or steering groups established by Cyber Security NSW or cluster CISO
- Establishing training and awareness programs to increase employees' cyber security capability
- Building cyber incident response capability that links to agency incident management and the whole of government cyber response plan
- Collaborating with privacy, audit, information management and risk officers to protect agency information and systems
- For cluster CISOs, supporting agencies in their cluster to implement and maintain an effective cyber security program including via effective collaboration and/or governance forums
- Managing the budget and funding for the cyber security program

⁴ <https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management>

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

CIOs or COOs, or staff with CIO/COO responsibilities are accountable for:

- Working with CISOs and across their agency to implement this policy
- Implementing a cyber security 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
- Clarifying 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 position 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

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

Information Security Managers, Cyber Security Managers or Senior Responsible Officers are responsible for one or all of the following within their agency or cluster:

- Managing and coordinating the response to cyber security incidents, changing threats, and vulnerabilities
- Developing and maintaining cyber security procedures and guidelines
- Providing guidance on cyber security risks introduced from business and operational change
- Managing the life cycle of cyber security platforms including design, deployment, ongoing operation, and decommissioning
- Ensuring appropriate management of the availability, capacity and performance of cyber security hardware and applications
- Providing input and support to regulatory compliance and assurance activities and managing any resultant remedial activity
- Developing a metrics and assurance framework to measure the effectiveness of controls
- Providing day-to-day management and oversight of operational delivery

2.6 NSW Chief Cyber Security Officer (NSW CCSO)

The NSW CCSO is accountable for:

- Creating and implementing the NSW Government Cyber Security Strategy
- Building a cyber-aware culture across NSW Government

- Receiving, collating and reporting on high cyber risks and monitoring cyber security incident reports across 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 policy, capability and capacity
- Recommending and recording exemptions to any part of the NSW Government Cyber Security Policy
- Representing NSW Government on cross-jurisdictional matters relevant to cyber security
- Assisting agencies to share information on security threats and cooperate on security threats and intelligence to enable management of government-wide cyber risk
- Creating and implementing the NSW Government cyber incident response arrangements
- Coordinating the NSW Government response to significant cyber incidents and cyber crises

2.7 Information Management Officer

A cluster or agency should have a person or persons who fulfil the role of Information Management Officer as part of their role and are responsible for:

- Acting as a focal point within their agency for all matters related to information management that are required to support cyber security
- Ensuring that a cyber incident that involves information damage or loss is escalated and reported to the appropriate information management response team in your agency

2.8 Internal Audit

Agency Internal Audit teams are responsible for:

- Validating that the cyber security 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 this policy and cyber security controls
- Providing assurance regarding the effectiveness of cyber security controls

2.9 Risk

Agency Risk teams are responsible for:

- Assisting to ensure the risk framework is applied in assessing cyber security risks and with setting of risk appetite
- Assisting the agency CISO in analysing cyber security risks

- Meeting with cluster CISO to ensure cyber risk frameworks fit into the Enterprise Risk framework

2.10 3rd party ICT providers













Agencies are responsible under the cyber security policy for managing cyber security requirements including contract clauses as well as monitoring and enforcement for 3rd party ICT providers.

Where agencies require 3rd party vendors to comply with the policy, agencies should ensure vendors have the following in place to protect outsourced government systems:

- Mandatory Requirement 1.5: The ICT provider has a process that is followed to notify the agency quickly of any suspected or actual security incidents and follows reasonable direction from the agency arising from incident investigations (noting this will vary based on risk profile and risk appetite).
- Mandatory Requirement 2.1: The ICT provider ensures that their staff understand and implement the cyber security requirements of the contract.
- Mandatory Requirement 3.1: Any 'Crown Jewel' systems must be covered in the scope of an Information Security Management System (ISMS) or Cyber Security framework
- Mandatory Requirement 3.4: Cyber Security requirements are built into the early stages of projects and the system development life cycle (SDLC) including agile projects.
- Mandatory Requirement 3.5: Ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data, including processes for internal fraud detection.

This does not prevent other contractual obligations being imposed.

3 Mandatory Requirements

 LEAD	 PREPARE	 PREVENT	 DETECT	 RESPOND	 RECOVER
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	Develop, implement and maintain an approved cyber security plan that is integrated with your agency's business continuity arrangements. This must include consideration of cyber security threats, risks and vulnerabilities that impact the protection of the agency's information, ICT assets and services.				
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 and ensure the providers understand and comply with the cyber security requirements of the contract including the applicable parts of this policy (Section 2.10) 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.				
 LEAD	 PREPARE	 PREVENT	 DETECT	 RESPOND	 RECOVER
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 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 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.



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), Cyber Security Management System (CSMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as an agency’s “crown jewels”. The ISMS, CSMS or CSF should be compliant with, or modelled on, one or more recognised ICT,OT or IoT standard (see guideline for more information).
3.2	Implement the ACSC Essential 8 ⁵ .
3.3	Classify information ⁶ and systems according to their business value (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the requirements of the <i>NSW Government Information Classification Labelling and Handling Guidelines</i> and <ul style="list-style-type: none"> ○ assign overall responsibility for information asset protection and 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. Any upgrades to existing systems must incorporate appropriate controls to ensure the solution remains within the organisation’s cyber risk tolerance.
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.

⁵ Strategies to Mitigate Cyber Security Incidents: <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained>

⁶ <https://www.digital.nsw.gov.au/policy/managing-data-information/information-classification-handling-and-labeling-guidelines>

	 LEAD	 PREPARE	 PREVENT	 DETECT	 RESPOND	 RECOVER
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 and the NSW Government Cyber Incident Response Plan.					
4.2	Test their cyber incident response plan at least every year and involve their senior executives responsible for the management of media and external communications.					
4.3	Deploy monitoring processes and tools to allow for adequate incident identification and response. Ensure monitoring and scanning actions from advisories and alerts issued by Cyber Security NSW and/or clusters are undertaken in the advised time period.					
4.4	Report cyber security incidents to their Cluster CISO and/or Cyber Security NSW according to the NSW Cyber Security Response Plan.					
4.5	Participate in whole of government cyber security exercises as required.					
	 LEAD	 PREPARE	 PREVENT	 DETECT	 RESPOND	 RECOVER
5	Agencies must report against the requirements outlined in this policy and other cyber security measures for the previous financial year. 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 ⁷ , in the format provided by Cyber Security NSW by 31 August.					

⁷ As sourced from the agency's risk register or equivalent and as required in TPP15-03 Internal Audit and Risk Management Policy for the NSW Public Sector: <https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management>

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.

4 Compliance Reporting and Attestation

Compliance reporting

Agencies must provide a yearly report for the previous financial year to their cluster CISO, or Cyber Security NSW, on their compliance with this policy in a format provided by Cyber Security NSW by 31 August each year. This will largely be a maturity-based assessment on the items listed as mandatory requirements as well as the ACSC Essential 8. It is possible to have a response of “not applicable” with an appropriate explanation that is acceptable to your agency.

The reports will be summarised and provided to the relevant governance bodies including the Cyber Security Steering Group (CSSG), Secretaries Board, Delivery and Performance Committee of Cabinet (DaPCo), Cyber Security Senior Officers Group (CSSOG) and the ICT and Digital Leadership Group (IDLG) and used to identify common themes and areas for improvement across NSW Government.

Annual attestation

Agencies must provide a signed annual attestation for the previous financial year to Cyber Security NSW by 31 August each year. This same attestation must be provided in agency annual reports or in department annual reports, if applicable. 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. 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 the following items:

- the agency has assessed its cyber security risks
- cyber security is appropriately addressed at agency governance forums
- the agency has a cyber incident response plan, it is integrated with the security components of business continuity arrangements, and has been tested over the previous 12 months (involving senior business executives)
- confirmation of the agency’s Information Security Management System/s (ISMS), Cyber Security Management Framework/s and/or Cyber Security Framework (CSF) including certifications or independent assessment where available
- what the agency is doing to continuously improve the management of cyber security governance and resilience

Example attestation

The following attestation is a suggestion only and can be adapted to accurately reflect the circumstances of the agency or cluster.

Cyber Security Annual Attestation Statement for the 20XX-20XX Financial Year for [Department or Statutory Body]

I, *[name of Department Head or Governing Board of the Statutory Body]*, am of the opinion that *[name of Department or Statutory Body]* have managed cyber security risks in a manner consistent with the Mandatory Requirements set out in the NSW Government Cyber Security Policy.

Governance is in place to manage the cyber security maturity and initiatives of [*name of Department or Statutory Body*].

Risks to the information and systems of [*name of Department or Statutory Body*] have been assessed and are managed.

There exists a current cyber incident response plan for [*name of Department or Statutory Body*] which has been tested during the reporting period.

[*name of Department or Statutory Body*] has an Information Security Management System (ISMS), Cyber Security Management System (CSMS) or Cyber Security Framework (CSF) in place.

[*name of Department or Statutory Body*] is doing the following to continuously improve the management of cyber security governance and resilience:

This attestation covers the following agencies: [*list of agencies*]

See guidance documents for more information and/or email the Cyber Security NSW Policy team (cybersecuritypolicy@customerservice.nsw.gov.au)

5 Useful Links

Issuer	Reference	Document Name
NSW Government	https://www.legislation.nsw.gov.au/#/view/act/1989/134	<i>State Owned Corporations Act 1989</i>
	https://www.legislation.nsw.gov.au/#/view/act/1998/17	<i>State Records Act 1998</i>
	https://www.legislation.nsw.gov.au/view/html/inforce/current/act-1998-133	<i>Privacy and Personal Information Protection Act 1998</i>
	https://www.legislation.nsw.gov.au/#/view/act/2002/71	<i>Health Records and Information Privacy Act 2002</i>
	https://www.legislation.nsw.gov.au/#/view/act/2009/52	<i>Government Information (Public Access) Act 2009</i>
	https://www.legislation.nsw.gov.au/view/html/inforce/current/act-2013-040	<i>Government Sector Employment Act 2013</i>
	https://www.legislation.nsw.gov.au/#/view/act/2015/60/full	<i>Data Sharing (Government Sector) Act 2015</i>
	https://www.nsw.gov.au/improving-nsw/projects-and-initiatives/nsw-state-infrastructure-strategy/	<i>The NSW State Infrastructure Strategy 2018-2038</i>
	https://www.emergency.nsw.gov.au/Documents/plans/sub-plans/cyber-security-incident-sub-plan.pdf	<i>NSW Government Incident Emergency Sub Plan</i>
	https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management	<i>Internal Audit and Risk Management Policy for the General Government Sector (TPP20-08)</i>
Department of Customer Service	https://www.digital.nsw.gov.au/policy/managing-data-information/information-classification-handling-and-labeling-guidelines	<i>NSW Government Information Classification, Labelling and Handling Guidelines</i>
	https://www.digital.nsw.gov.au/sites/default/files/NSW%20Cyber%20Security%20Strategy%202018.pdf	<i>NSW Government Cyber Security Strategy</i>
	https://www.digital.nsw.gov.au/support-services/data-information/managing-data-information	<i>Managing data and information, 2013</i>

Issuer	Reference	Document Name
	https://arp.nsw.gov.au/dcs-2020-05-cyber-security-nsw-directive-practice-requirements-for-nsw-government	<i>DCS-2020-05 Cyber Security NSW directive – Practice Requirements for NSW Government</i>
	https://arp.nsw.gov.au/dcs-2020-02-nsw-cyber-security-policy/	<i>DCS-2020-02 NSW Cyber Security Policy</i>
Information and Privacy Commission NSW	https://www.ipc.nsw.gov.au/data-breach-guidance	<i>Guidance on Data Breaches, May 2018</i>
NSW Audit Office	https://www.audit.nsw.gov.au/our-work/reports/detecting-and-responding-to-cyber-security-incidents-	<i>Detecting and responding to cyber security incidents</i>
NSW Treasury	https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management/risk	<i>Risk management toolkit</i>
NSW Department of Premier and Cabinet	https://arp.nsw.gov.au/m1999-19-applicability-memoranda-and-circulars-state-owned-corporations-socs	<i>Memorandum M1999-19 Applicability of Memoranda and Circulars to State Owned Corporations.</i>
State Archives and Records Authority of NSW	https://www.records.nsw.gov.au/recordkeeping/rules/standards/records-management	<i>Standard on Records Management, 2018</i>
	https://www.records.nsw.gov.au/recordkeeping/advice/using-cloud-computing-services	<i>Using cloud computing services: implications for information and records management, 2015</i>
	https://www.records.nsw.gov.au/recordkeeping/advice/storage-and-preservation/service-providers-outside-nsw	<i>Storage of State records with service providers outside of NSW, 2015</i>
Australian Government – Home Affairs	https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018	<i>Security of Critical Infrastructure Act 2018</i>
	https://cybersecuritystrategy.homeaffairs.gov.au/	<i>Australia's Cyber Security Strategy, 2020</i>
Australian Government - Attorney-General's Department	https://www.protectivesecurity.gov.au/Pages/default.aspx	<i>The Protective Security Policy Framework</i>
	https://www.protectivesecurity.gov.au/resources/Pages/relevant-australian-and-international-standards.aspx	<i>Relevant Australian and international standards</i>

Issuer	Reference	Document Name
Australian Government - Australian Signals Directorate	https://acsc.gov.au/infosec/ism	<i>Information Security Manual</i>
Australian Government – Office of the Australian Information Commissioner	https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/	<i>Australian privacy Principles guidelines, 2014</i>
International Organization for Standardization	https://www.iso.org/standard/50038.html	<i>ISO 22301 Societal Security – Business continuity management systems – Requirements</i>
	https://www.iso.org/standard/44374.html	<i>ISO 27031 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity</i>
	https://www.iso.org/standard/44375.html	<i>ISO 27032 Information technology – Security techniques – Guidelines for cybersecurity</i>
National Institute of Standards and Technology	https://www.nist.gov/cyberframework	<i>Framework for Improving Critical Infrastructure Cybersecurity</i>
New Zealand National Cyber Security Centre	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Intro-Nov-2019.pdf	<i>Introduction: Cyber security governance</i>
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-1-Nov-2019.pdf	<i>Step One: Building a culture of cyber resilience</i>
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-2-Nov-2019.pdf	<i>Step Two: Establishing roles and responsibilities</i>
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-3-Nov-2019.pdf	<i>Step Three: Holistic risk management</i>
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-4-Nov-2019.pdf	<i>Step Four: Cyber security collaboration</i>
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-5-Nov-2019.pdf	<i>Step Five: Create a cyber security programme</i>
	https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-6-Nov-2019.pdf	<i>Step Six: Measuring resilience</i>

Issuer	Reference	Document Name
--------	-----------	---------------

6 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 <i>Government Sector Employment Act 2013</i>
Access Control	The process of granting or denying requests for access to systems, applications and information. Can also refer to the process of granting or denying requests for access to facilities
ACSC	Australian Cyber Security Centre
Application Whitelisting	An approach in which only an explicitly defined set of applications are permitted to execute on a system
Audit Log	A chronological record of system activities including records of system access and operations performed
Audit Trail	A chronological record that reconstructs the sequence of activities surrounding, or leading to, a specific operation, procedure or event
Authentication	Verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system
Authorisation	The process of defining or verifying permission for a specific identity or device to access or use resources in a system
Business Continuity Plan	A business continuity plan is a document that outlines how an organisation can ensure it's critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period.
Breach (data)	An incident that results in unauthorised access to, modification or disruption of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms
Breach (security)	When data is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Also referred to as a 'Data Spill'
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Classification	The categorisation of systems and information according to the expected impact if it was to be compromised
Cluster (also lead cluster department or department)	Officially defined as Departments in <i>Government Sector Employment Act 2013</i> Schedule 1 clusters are the eight 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 1 st July 2019).

Item	Definition
Critical infrastructure	Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security. (Security of Critical Infrastructure Act 2018)
Crown jewels	The most valuable or operationally vital systems or information in an organisation.
CSF	Cyber Security Framework
CSMS	A Cyber Security Management System is a management system focused on cyber security of control systems rather than information.
Cyber attack	A deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity
Cyber crime	Crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It also includes crimes where computers facilitate an existing offence, such as online fraud or online child sex offences
Cyber crisis	Major disruptions to services and operations, with genuine risks to critical infrastructure and services, with risks to the safety of citizens and businesses. Intense media interest, large demands on resources and critical services.
Cyber event	An identified occurrence of a system, service or network state indicating a possible breach of security policy or failure of safeguards
Cyber incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it
Cyber Incident Response Plan	A plan for responding to cyber security incidents
Cyber security	Measures used to protect the confidentiality, integrity and availability of systems and information
Disaster Recovery Plan	Outlines an organisation's recovery strategy for how they are going to respond to a disaster
Essential Eight	The Essential Eight are eight essential mitigation strategies that organisations are recommended to implement as a baseline to make it much harder for adversaries to compromise systems
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.
ISMS	An Information Security Management System “consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation’s information security to achieve business objectives”. (ISO/IEC 27000:2018)
Incident Response Plan	A plan for responding to cyber security incidents
Information security	The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability
IoT	The network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to connect to the internet and collect and exchange data
Macro	An instruction that causes the execution of a predefined sequence of instructions
Multi-factor authentication	A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are)
NSW CCSO	NSW Chief Cyber Security Officer – Note: The NSW whole-of-government cyber function was renamed ‘Cyber Security NSW’, and the ‘Government Chief Information Security Officer’ was renamed <i>NSW Chief Cyber Security Officer</i> in May 2019.
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 any at least any chosen file or database
Patching	The action of updating, fixing, or improving a computer program

Item	Definition
Position of Trust	<p>A position that involves duties that require a higher level of assurance than that provided by normal employment screening. In some organisations additional screening may be required</p> <p>Positions of trust can include, but are not limited to, an organisation's Chief Information Security Officer and their delegates, administrators or privileged users</p>
Privileged User	<p>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</p> <p>A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications</p>
Public Service agency	<p>Section 3 of the <i>Government Sector Employment Act</i> defines a Public Service agency as:</p> <ul style="list-style-type: none"> • a Department (listed in Part 1 of Schedule 1 to the Act), or • a Public Service executive agency (being an agency related to a Department), or • a separate Public Service agency.
Red Team	<p>Ethical hackers that provide penetration testing to ensure the security of an organisation's information systems</p>
Remote Access	<p>Access to a system that originates from outside an organisation's network and enters the network through a gateway, including over the internet</p>
Risk appetite	<p>"Amount and type of risk that an organisation is willing to pursue or retain." (ISO/Guide 73:2009)</p>
Risk tolerance	<p>"Organisation's or stakeholder's readiness to bear the risk, after risk treatment, in order to achieve its objectives." (ISO/Guide 73:2009)</p>
SDLC	<p>The System Development Life Cycle is the "scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal". (NIST SP 800-137)</p>
Secure-by-design	<p>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.</p>
Significant cyber incident	<p>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.</p>
State owned corporation	<p>Commercial businesses owned by the NSW Government: Essential Energy, Forestry Corporation of NSW, Hunter Water, Port Authority of NSW, Sydney Water, Landcom, Water NSW</p>

Item	Definition
Supply Chain	Supply chain is a system of organisations, people, activities, information, and resources involved in supplying a product or service to a consumer
Systems	Software, hardware, data, communications, networks and includes specialised systems such as industrial and automation control systems, telephone switching and PABX systems, building management systems and internet connected devices
Whitelisting	Authorising only approved applications for use within organisations in order to protect systems from potentially harmful applications