



NSW Cyber Security Policy

Document number:

Version number: 3.0 **SUPERSEDED BY V4.0**

SUPERSEDED



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.

This policy applies to:

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

This policy mandates a number of requirements all agencies **MUST** implement. There is flexibility to make an informed, risk-based decision on the type and number of controls that are implemented by an agency as part of its Information Security Management System or Cyber Security Framework.

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. It is recommended that agencies seek additional guidance, strategies and controls 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.

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 agency's "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.

SUPERSEDED

¹ https://acsc.gov.au/publications/protect/Essential_Eight_Explained.pdf

² 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>

2 Roles and Responsibilities

Each agency should have someone performing each of the following roles:

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
- 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

³ The head of the agency listed in Part 2 or 3 of Schedule 1 of the *Government Sector Employment Act 2013*

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

- Appropriately resourcing and supporting agency cyber security initiatives including training and awareness and continual improvement initiatives to support this policy

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 as an advisor or member
- 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.

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 or Cyber Security Manager

Information Security Managers or Cyber Security Managers 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 accountable 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 dealt with in the proper manner and reported to the State Archives and Records Authority

2.8 Internal Audit

Agency Internal Audit teams are accountable 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 Vendors/3rd parties

Vendors/3rd parties are responsible for:

- Complying with the NSW Cyber Security Policy minimum standards
- Complying with all relevant whole-of-government security requirements, including all security-related controls/clauses in procurement contracts

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	Have an approved cyber security plan to manage the agency's cyber security risks, integrated with business continuity arrangements. This must include consideration of threats, risks and vulnerabilities that impact the protection of the agency's information, ICT assets and services.				
1.4	Consider cyber security threats when performing risk assessments and include high and critical risks in the agency's overall risk management framework.				
1.5	Be accountable for the cyber risks of their ICT service providers and ensure the providers comply with the applicable parts of this policy and any other relevant agency security policies. This must include providers notifying the agency quickly of any suspected or actual security incidents and following reasonable direction from the agency arising from incident investigations.				
 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 education for all employees and contractors, and ensure that outsourced ICT service providers understand and implement the cyber security requirements of the contract.				
2.2	Increase awareness of cyber security risk across all staff including the need to report cyber security 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	<p>Implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as an agency's "crown jewels". The ISMS or CSF should be compliant with, or modelled on, one or more recognised ICT/OT standard (see guideline for more information).</p> <p>2019 version - Implement an Information Security Management System (ISMS) or Cyber Security Management System (CSMS) that is compliant with recognised standards such as ISO/IEC27001 or ISA/IEC62443 (for IACS) and implement the relevant controls based on their requirements and risk appetite.</p> <p>At a Cluster or Agency level, there must be:</p> <ul style="list-style-type: none"> • ISO27001 certification of the ISMS with scope at least covering systems identified as an Agency's "crown jewels" and including annual surveillance audits, or • An annual, independent review or audit of the management system and/or the effectiveness of the controls covered by the management system or • An annual, independent review or audit of reporting against the mandatory requirements in this policy
3.2	<p>Implement the ACSC Essential 8⁵.</p> <p>2019 Version - Implement and report against the ACSC Essential 8:4</p> <ul style="list-style-type: none"> • the Agency's current maturity levels for each control • the Agency's target maturity levels and target date for each control, based on the Agency's risk tolerance.
3.3	Classify information ⁶ and systems according to their importance (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the

⁵ Strategies to Mitigate Cyber Security Incidents: https://acsc.gov.au/publications/protect/Essential_Eight_Explained.pdf

⁶ <https://arp.nsw.gov.au/dfsi-2015-01-nsw-government-information-classification-labelling-and-handling-guidelines>

	<p>requirements of the <i>NSW Government Information Classification Labelling and Handling Guidelines</i> and</p> <ul style="list-style-type: none"> ○ assign ownership ○ implement controls according to their classification and relevant laws and regulations ○ identify the agency's "crown jewels" and report them to Cyber Security NSW as per mandatory requirement 5.4.
3.4	Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects.
3.5	Ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including processes for internal fraud detection.
<div style="display: flex; justify-content: space-around; text-align: center;"> <div style="background-color: #cccccc; padding: 5px;"> LEAD</div> <div style="background-color: #add8e6; padding: 5px;"> PREPARE</div> <div style="background-color: #90ee90; padding: 5px;"> PREVENT</div> <div style="background-color: #32cd32; padding: 5px;"> DETECT</div> <div style="background-color: #ffa500; padding: 5px;"> RESPOND</div> <div style="background-color: #ff0000; padding: 5px;"> RECOVER</div> </div>	
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 business and IT executives, functional area coordinators (if applicable), as well as media and communication teams.
4.3	Deploy monitoring processes and tools to allow for adequate incident identification and response.
4.4	Report cyber security incidents to Cyber Security NSW according to the NSW Cyber Security Response Plan.
4.5	Participate in whole of government cyber security exercises as required.
<div style="display: flex; justify-content: space-around; text-align: center;"> <div style="background-color: #cccccc; padding: 5px;"> LEAD</div> <div style="background-color: #add8e6; padding: 5px;"> PREPARE</div> <div style="background-color: #90ee90; padding: 5px;"> PREVENT</div> <div style="background-color: #32cd32; padding: 5px;"> DETECT</div> <div style="background-color: #ffa500; padding: 5px;"> RESPOND</div> <div style="background-color: #ff0000; padding: 5px;"> RECOVER</div> </div>	
5	Agencies must report against the requirements outlined in this policy and other cyber security measures. Agencies must:
5.1	Report annually to their cluster CISO, or Cyber Security NSW, their compliance with the mandatory requirements in this policy, in the format

	provided by Cyber Security NSW. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.
5.2	Report annually to their cluster CISO, or Cyber Security NSW, their maturity against the ACSC Essential 8, in the format provided by Cyber Security NSW. Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.
5.3	Report annually to their cluster CISO, or Cyber Security NSW, the agency's cyber security risks with a residual rating of high or extreme ⁷ , in the format provided by Cyber Security NSW by 31 August.
5.4	Report annually to their cluster CISO, or Cyber Security NSW, the agency's "crown jewels". Cluster CISOs must provide all reports to Cyber Security NSW by 31 August.
5.5	Provide a signed attestation to Cyber Security NSW by 31 August each year and include a copy of your attestation in your annual report, as outlined in section 4. If your agency does not complete an annual report, an attestation must still be completed and signed off by your agency head and submitted to your cluster CISO.

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>

4 Compliance Reporting and Attestation

Compliance reporting

Agencies must provide a yearly report 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 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 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)
- certification of the agency’s Information Security Management System (ISMS) or confirmation of the agency’s Cyber Security Framework (CSF)
- what the agency is doing to continuously improve the management of cyber security governance and resilience

The template below is a suggestion only and should be updated to reflect the appropriate wording for the agency’s situation.

Annual attestation template

The following attestation 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) 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*]

SUPERSEDED

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/act/2009/52	<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://legislation.nsw.gov.au/#/view/act/2013/40	<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>
Department of Finance, Services and Innovation	https://arp.nsw.gov.au/dfs/2015-01-nsw-government-information-classification-labelling-and-handling-guidelines	NSW Government Information Classification, Labelling and Handling Guidelines (2015)
	https://www.digital.nsw.gov.au/policy/cyber-security	<i>NSW Government Cyber Security Strategy</i>
	https://www.digital.nsw.gov.au/sites/default/files/Digital%20Information%20Security%20Policy%202015.pdf	<i>NSW Digital Information Security Policy (2015)</i>
	https://www.digital.nsw.gov.au/support-services/data-information/managing-data-information	<i>Managing data and information, 2013</i>
Information and Privacy Commission NSW	https://www.ipc.nsw.gov.au/data-breach-guidance	Guidance on Data Breaches, May 2018
NSW Audit Office	https://www.audit.nsw.gov.au/publications/latest-reports/detecting-and-responding-to-cyber-security-incidents	<i>Detecting and responding to cyber security incidents</i>

Issuer	Reference	Document Name
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, 2016</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>
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/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf	<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>

Issuer	Reference	Document Name
	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>

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>
ACSC	Australian Cyber Security Centre
CIO	Chief Information Officer
CISO	Chief Information Security Officer
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).
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	
CSMS	A Cyber Security Management System is a management system focused on cyber security of control systems rather than information.
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 incident	Moderate or higher impact to services, information, assets, reputation or relationships. Public visibility of impacts through service degradation or public disclosure of information/systems breaches, with economic impacts.
Cyber security	All measures used to protect systems, and information processed, stored or communicated on such systems, from compromise of confidentiality, integrity and availability. (emerging Australian Government 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)

Item	Definition
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)
IoT	The Internet of Things (IoT) refers to the inter-connection of many devices and objects utilising internet protocols that can occur with or without the active involvement of individuals using the devices. The IoT is the aggregation of many machine-to-machine (M2M) connections.
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.
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	Ethical hackers that provide penetration testing to ensure the security of an organisation’s information systems
Risk appetite	“Amount and type of risk that an organisation is willing to pursue or retain.” (ISO/Guide 73:2009)
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)
SDLC	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)
Secure-by-design	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.

Item	Definition
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, Port Authority of NSW, Sydney Water, Landcom, Water NSW
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

SUPERSEDED