NSW Cyber Security Policy

Document number:	Version number: 5.0

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 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* (the Policy) replaced the *NSW Digital Information Security Policy* on 1 February 2019. The Policy is reviewed annually and updated based on agency feedback and emerging cyber security threats and trends.

1.2 Purpose

This 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[2].

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 managed, owned or shared by the NSW public sector, and

---

[1] https://www.digital.nsw.gov.au/strategy
[2] Email policy@cyber.nsw.gov.au for a copy of the guidance documents

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

This policy is not mandatory for state owned corporations, local councils and 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.

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

1.4   Risk Based Implementation of the Policy

This policy is risk based and agencies must identify target maturity levels appropriate to their risks, including the type of information they hold and services they provide.

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

The Agency Head must sign off on any target maturity levels below a level 3 (and/or E8 level 0 or 1). Residual risks must be tracked and managed in the risk register with the Agency Head responsible for risk acceptance and the risk register being reviewed quarterly.

1.5   Assistance implementing the Policy

Cyber Security NSW may assist agencies with their implementation of 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 policy@cyber.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 below.

1.6   Exemptions and extensions

Exemptions to this policy and extensions to reporting will only be considered in exceptional circumstances. To seek an exemption or extension, 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.

Independent agencies may seek to raise exemption or extension requests directly to Cyber Security NSW, but are expected to still advise their parent cluster of the request.

Requests must be made in writing to Cyber Security NSW at policy@cyber.nsw.gov.au, **prior to 30th September.**

2. Reporting and Attestation

2.1   Reporting obligations

Cluster CISOs, and/or central cluster cyber security teams, are to coordinate Policy reporting across the entirety of their cluster.

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

By 31 October each year, agencies must submit the following to their cluster CISO or Cyber Security NSW:

1. Maturity reporting against all mandatory requirements in this policy and the Australian Cyber Security Centre (ACSC) Essential Eight for the previous financial year. The reporting template to be provided by Cyber Security NSW

2. Cyber security risks with a residual rating of high or extreme[3] and a list of the agencies' "crown jewels"

3. An attestation on cyber security to also be included in each agency's individual annual report. If your agency does not complete an annual report, an attestation must still be completed and signed-off by your Agency Head.

Agencies have an obligation to ensure reporting reflects an accurate and verifiable assessment of maturity as well as implementation of other requirements of this Policy. As such, agencies must:

- Compile and retain in accessible form, the artefacts that demonstrate the basis of their self-assessments

- Resolve discrepancies and inaccuracies identified in their reporting, including discrepancies between their reported level of maturity and the level they can demonstrate with evidence

- Refer to the Policy Guidance (see: Supplementary Documents) to support their assessments of maturity

- Ensure their attestations refer to any departures from the requirements of the Policy (see: Attestation).

2.2   Maturity reporting

Agencies must provide a yearly report for the previous financial year to their cluster CISO, or Cyber Security NSW, in a format provided by Cyber Security NSW by 31 October each year. Scores are to be provided for your agency's maturity against the mandatory requirements in this policy and the ACSC Essential Eight, as well as target maturity levels for next year. It is possible to have a response of "not applicable" with an appropriate explanation that is acceptable to your agency.

---

[3] 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

The reports will be summarised and provided to the relevant governance bodies including the Cyber Security Steering Group (CSSG), Secretaries Board, relevant Committees of Cabinet, 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.

2.3   Crown jewels and risk reporting

Agencies must provide a list of their crown jewels and high and extreme risks to their cluster CISO, or Cyber Security NSW, in a format provided by Cyber Security NSW, by 31 October each year. If an agency does not have any crown jewels or high and extreme risks, they can provide a response of "not applicable".

2.4   Attestation

Agencies must provide a signed annual attestation for the previous financial year to Cyber Security NSW by 31 October 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

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

3.   Mandatory Requirements

NOTE: Please use the Cyber Security Policy Maturity Model and Guidance in conjunction with these Mandatory Requirements when assessing maturity levels.

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, reporting and meeting the requirements of this policy.				
1.3	Develop, implement and maintain an approved cyber security plan that is integrated with your agency's business continuity arrangements.				
1.4	Include cyber security in their risk management framework and consider cyber security threats when performing risk assessments.				
1.5	Be accountable for the cyber risks of their ICT service providers with access to or holding of government information and systems and ensure these providers understand and comply with the cyber security requirements of the contract, including the applicable parts of this policy (Section 5.10) and any other relevant agency security policies.				

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 a demonstrable factor in decision-making and where cyber security risk management processes are understood and applied.					
2.4	Ensure that appropriate access controls and security screening processes are in place for people with privileged access or access to sensitive or classified information.					
2.5	Receive and/or provide information on security threats and intelligence with Cyber Security NSW and cooperate across NSW Government to enable management of government-wide cyber risk.					

	LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER

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).
3.2	Implement the ACSC Essential Eight.
3.3	Classify information[4] and systems according to their business value (i.e. the impact of loss of confidentiality, integrity or availability).
3.4	Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects. Any upgrades to existing systems must comply with your organisation's cyber risk tolerance.
3.5	Audit trail and activity logging records are determined, documented, implemented and reviewed for new ICT systems and enhancements.

	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	Exercise their cyber incident response plan at least every year.
4.3	Ensure that ICT systems and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.
4.4	Report cyber security incidents to their cluster CISO and/or Cyber Security NSW according to the *NSW Cyber Security Response Plan*. If relevant, ensure incident reporting is compliant with Federal reporting requirements.
4.5	Participate in whole-of-government cyber security exercises as required.

---

[4] https://www.digital.nsw.gov.au/policy/managing-data-information/information-classification-handling-and-labeling-guidelines

4. The Essential Eight

The ACSC recommends that organisations implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems. Please check the ACSC website for the latest version of the Essential Eight and maturity model[5].

The ACSC Essential Eight was refreshed on 12 July 2021. This update focused on using the maturity levels to counter the sophistication of different levels of adversary tradecraft and targeting, rather than being aligned to the intent of a mitigation strategy. The redefinition of a number of maturity levels will also strengthen a risk-based approach to implementation of the Essential Eight strategies. As the maturity model has been redefined and many requirements have changed, maturity assessments for the July 2021 model should not be directly compared to earlier versions of Essential Eight.

- FAQ: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq

- Essential Eight Maturity Model: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

- Definitions: https://www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-terminology

- ISM: https://www.cyber.gov.au/acsc/view-all-content/ism

Mitigation Strategy	What	Why
Application control	Checking programs against a pre-defined approved list and blocking all programs not on this list	So unapproved programs including malware are unable to start and preventing attackers from running programs which enable them to gain access or steal data
Patch applications	Apply security fixes/patches or mitigations (temporary workarounds) for programs within a timely manner (48 Hours for internet reachable applications). Do not use applications which are out-of-support and do not receive security fixes	Unpatched applications can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems
Configure MS Office macro settings	Only allow Office macros (automated commands) where there is a business requirement and restrict the type of commands a macro can execute. Also monitor usage of Macros.	Macros can be used to run automated malicious commands that could let an attacker download and install malware

---

[5] https://www.cyber.gov.au/acsc/view-all-content/essential-eight

User application hardening	Configure key programs (web browers, office, PDF software, etc) to apply settings that will make it more difficult for an attacker to successfully run commands to install malware	Default settings on key programs like web browsers may not be the most secure configuration. Making changes will help reduce the ability of a compromised/malicious website from successfully downloading and installing malware.
Restrict administrative privileges	Limit how accounts with the ability to administer and alter key system and security settings can be accessed and used.	Administrator accounts are 'the keys to the kingdom' and so controlling their use will make it more difficult for an attacker to identify and successfully gain access to one of these accounts which would give them significant control over systems
Patch operating systems	Apply security fixes/patches or temporary workarounds/mitigations for operating systems (e.g. Windows) within a timely manner (48 Hours for internet reachable applications). Do not use versions of an Operating system which are old and/or not receiving security fixes	Unpatched operating systems can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems
Multi-factor authentication	A method of validating the user logging in by using additional checks separate to a password such as a code from an SMS/Mobile application or fingerprint scan	Makes it significantly more difficult for adversaries to use stolen user credentials to facilitate further malicious activities
Regular backups	Regular backups of important new or changed data, software and configuration settings, stored disconnected and retained for at least three months. Test the restoration process when the backup capability is initially implemented, annually and whenever IT infrastructure changes.	To ensure information can be accessed following a cyber-security incident e.g. a ransomware incident).

5. Roles and Responsibilities

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

- 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 this policy or shared among multiple roles.

See guidance for more information[6].

5.1 Agency Heads

All Agency Heads[7] (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

- Determining their agency's risk appetite using the approved whole-of-government Internal Audit and Risk Management Policy[8]

- 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

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

---

[6] Email policy@cyber.nsw.gov.au for a copy of the guidance documents
[7] 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
[8] https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management

- 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

- Determining their agency's risk appetite using the approved whole-of-government Internal Audit and Risk Management Policy[9]

- 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

5.2   ICT & Digital Leadership Group (IDLG)

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

- Endorsing the Policy and any updates

- Ensuring the Policy's implementation across NSW Government

- Reviewing the summarised agency/cluster reports against the Policy's mandatory requirements

- Providing leadership, support and resources for the Policy and advocating organisational commitment to improving the cyber security culture of the agency/cluster

5.3   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

---

[9] https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management

- 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

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

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 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

- Implementing policies, procedures, practices and tools to ensure compliance with this policy

- Investigating, responding to and reporting on cyber security events

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

- Reporting cyber incidents to the appropriate agency governance forum and Cyber Security NSW based on severity definitions provided by Cyber Security NSW

- 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

- Applying for relevant programs/funding (eg. DRF, ACSC uplift programs)

5.5 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 an 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

5.6 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

5.7 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

5.8 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

5.9 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 the cluster CISO to ensure cyber risk frameworks fit into the Enterprise Risk Framework

5.10 3rd party ICT providers

Agencies are responsible under the cyber security Policy for managing cyber security requirements. This includes contract clauses, monitoring and enforcement for 3rd party ICT providers and the ICT security of non-government organisations holding and/or accessing government systems[10].

Where agencies require 3rd party organisations to comply with the Policy, agencies should ensure they have the following in place to protect government systems outsourced to them or that they may have access to:

- Mandatory Requirement 1.5: The third-party organisation 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 third-party organisation 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.

---

[10] https://buy.nsw.gov.au/resources/ICT-Purchasing-Framework

6. Useful links

Issuer	Reference	Document Name
NSW Government	https://www.legislation.nsw.gov.au/#/view/act/1989/134	*State Owned Corporations Act 1989*
	https://www.legislation.nsw.gov.au/#/view/act/1998/17	*State Records Act 1998*
	https://www.legislation.nsw.gov.au/view/html/inforce/current/act-1998-133	*Privacy and Personal Information Protection Act 1998*
	https://www.legislation.nsw.gov.au/#/view/act/2002/71	*Health Records and Information Privacy Act 2002*
	https://www.legislation.nsw.gov.au/#/view/act/2009/52	*Government Information (Public Access) Act 2009*
	https://www.legislation.nsw.gov.au/view/html/inforce/current/act-2013-040	*Government Sector Employment Act 2013*
	https://www.legislation.nsw.gov.au/#/view/act/2015/60/full	*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.emergency.nsw.gov.au/Documents/plans/sub-plans/cyber-security-incident-sub-plan.pdf	*NSW Government Incident Emergency Sub Plan*
	https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management	*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://www.digital.nsw.gov.au/Policy/managing-data-information/information-classification-handling-and-labeling-guidelines	*NSW Government Information Classification, Labelling and Handling Guidelines*
	https://www.digital.nsw.gov.au/transformation/cyber-security/cyber-security-strategy	*2021 NSW Cyber Security Strategy*
	https://www.digital.nsw.gov.au/support-services/data-information/managing-data-information	*Managing data and information, 2013*
	https://arp.nsw.gov.au/dcs-2020-05-cyber-security-nsw-directive-practice-requirements-for-nsw-government	*DCS-2020-05 Cyber Security NSW directive – Practice Requirements for NSW Government*

	https://arp.nsw.gov.au/dcs-2021-02-nsw-cyber-security-policy/	*DCS-2021-02 NSW Cyber Security Policy*
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/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.*
State Archives and Records Authority of NSW	https://www.records.nsw.gov.au/recordkeeping/rules/standards/records-management	*Standard on Records Management, 2018*
	https://www.records.nsw.gov.au/recordkeeping/advice/using-cloud-computing-services	*Using cloud computing services: implications for information and records management, 2015*
	https://www.records.nsw.gov.au/recordkeeping/advice/storage-and-preservation/service-providers-outside-nsw	*Storage of State records with service providers outside of NSW, 2015*
Australian Government – Home Affairs	https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018	*Security of Critical Infrastructure Act 2018*
	https://cybersecuritystrategy.homeaffairs.gov.au/	*Australia's Cyber Security Strategy, 2020*
Australian Government - Attorney-General's Department	https://www.protectivesecurity.gov.au/about	*The Protective Security Policy Framework*
	https://www.protectivesecurity.gov.au/resources/Pages/relevant-australian-and-international-standards.aspx	*Relevant Australian and international standards*
Australian Government - Australian Signals Directorate	https://acsc.gov.au/infosec/ism	*Information Security Manual*
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.iso.org/standard/50038.html	*ISO 22301 Societal Security – Business continuity management systems – Requirements*

	https://www.iso.org/standard/44374.html	*ISO 27031 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*
	https://www.iso.org/standard/44375.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*
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*

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 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
Availability	Making information consistently and readily accessible for authorised parties
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 *Government Sector Employment Act 2013* 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 1st 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
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
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

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

Item	Definition
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 *NSW Chief Cyber Security Officer* in May 2019
Operational Technology (OT)	Operational technology 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 any at least any chosen file or database
Patching	The action of updating, fixing, or improving a computer program
Position of Trust	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 Positions of trust can include, but are not limited to, an organisation's Chief Information Security Officer and their delegates, administrators or privileged users
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), 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
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

Item	Definition
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)
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
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
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