



NSW Cyber Security Policy

Document number:

Version number: 1.1



1 Policy Statement

1.1 Overview

Strong cyber security is an important component of the *NSW Digital Government Strategy*. 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 risks have continued to evolve in recent years and rapid technological change has resulted in increased cyber connectivity and more dependency on cyber infrastructure.

The word “systems” in this policy refers to: software, hardware, 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.

The *NSW Cyber Security Policy* (the policy) replaces the NSW Digital Information Security Policy 2015 and is part of the action plan outlined in the 2018 NSW Cyber Security Strategy. Key improvements include strengthening cyber security governance, identifying an Agency’s most valuable or operationally vital systems or information (also called the “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.

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 underpins organisational resilience because entities know their risks, make informed decisions in managing those risks, identify opportunities and continuously improve. This is reinforced 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 managed. This policy is designed to be read by Agency Heads, Chief Information Officers, Chief Information Security Officers (or equivalent), Audit and Risk teams and all Executives.

1.3 Scope

This policy applies to all NSW Government Departments and Public Service Agencies (*Government Sector Employment Act 2013* Schedule 1 Public Service agencies). In this policy, references to “lead cluster Departments” or “clusters” mean the Departments listed in Part 1, Schedule 1. The term “Agency” is used to refer to any or all NSW Government Departments and Public Service Agencies.

This policy applies to:

- information and communications technology (ICT) systems, and
- industrial automation and control systems (IACS) that handle government or citizen data or provide critical government services

This policy mandates a number of requirements that are a minimum that all agencies must implement. There is flexibility in some of the requirements to make an informed, risk-based decision on the type and number of controls that are implemented by an Agency.

Agencies that provide 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.

In accordance with Premier’s Memorandum M1999-19 *Applicability of Memoranda and Circulars to State Owned Corporations*, this policy does not apply to State Owned Corporations. This policy is however recommended for adoption in State Owned Corporations, as well as local councils and universities.

1.4 Exemptions

Exemptions to any part of this policy may be sought by Agency heads from the Government Chief Information and Digital Officer (GCIDO) who will be advised by the Government Chief Information Security Officer (GCISO). Please contact cybersecurity@finance.nsw.gov.au.

1.5 Summary of Your Agency’s Reporting Obligations

- By 31 August each year, submit a report to your Agency head and GCISO, in a template provided by GCISO, covering the following:
 1. Assessment against all mandatory requirements in this policy for the previous financial year, including a maturity assessment against the Australian Cyber Security Centre (ACSC) Essential 8¹
 2. Cyber security risks with a residual rating of high or extreme²

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

3. A list of the Agency's "crown jewels"

- Include an attestation on cyber security in your annual report and provide a copy to GCISO

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

ICT & Digital Leadership Group (IDLG)

The IDLG, chaired by the Government Chief Information and Digital Officer (GCIDO), 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

Agency heads

The head of each NSW Agency is accountable for:

- Ensuring their Agency complies with the requirements of this policy and reporting on compliance with the policy
- Ensuring their Agency develops, implements and maintains an effective information and cyber security plan
- 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 IACS cyber security for the Agency or Cluster (if applicable)
- 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 tolerance for security risks using the approved whole-of-government Internal Audit and Risk Management Policy³
- Appropriately resourcing and supporting Agency cyber security initiatives including training and awareness and continual improvement initiatives to support this policy
- For cluster Secretaries, ensuring all agencies in their cluster implement and maintain an effective cyber security program

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

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

³ <https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management>

- 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
- Ensuring all staff and providers understand their role in building and maintaining secure systems

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

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

- Assisting with defining and implementing a cyber security plan for the protection of the Agency's information and systems
- 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 the GCISO based on severity definitions provided by the GCISO
- Representing their Agency on whole-of-government collaboration, advisory or steering groups established by the GCISO 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

Government Chief Information Security Officer (GCISO)

The GCISO 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

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

Internal Audit

Agency Internal Audit teams are accountable for:

- On a risk basis, regularly reviewing their Agency's adherence to this policy and cyber security controls
- Assisting the Agency CISO in analysing internal controls and developing the cyber security plan

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 and developing the cyber security plan

3 Mandatory Requirements

|  LEAD |  PRFPARF |  PRVFNT |  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 IACS 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 and assets, and services and initiatives to improve. | | | | |
| 1.4 | Conduct cyber security risk assessments and include identified 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 |  PRFPARF |  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, 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 and running exercises such as simulations. | | | | |
| 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 the GCISO 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 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, <u>or</u> • An annual, independent review or audit of the management system and/or the effectiveness of the controls covered by the management system <u>or</u> • An annual, independent review or audit of reporting against the mandatory requirements in this policy |
| 3.2 | <p>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 | <p>Classify information⁵ and systems according to their importance (i.e. the impact of loss of confidentiality, integrity or availability) and</p> <ul style="list-style-type: none"> ○ assign ownership ○ implement controls according to their classification and relevant laws |

⁴ Strategies to Mitigate Cyber Security Incidents:

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

⁵ <https://arp.nsw.gov.au/dfsi-2015-01-nsw-government-information-classification-labelling-and-handling-guidelines>

| | |
|--|---|
| | <p>and regulations</p> <ul style="list-style-type: none"> ○ Identify the Agency’s “crown jewels” and report them to GCISO as per mandatory requirement 5.3. |
| 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-between; align-items: center; 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: #90ee90; padding: 5px;"> DETECT</div> <div style="background-color: #ffa500; padding: 5px;"> RESPOND</div> <div style="background-color: #ff6347; 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, 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 the GCISO 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-between; align-items: center; 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: #90ee90; padding: 5px;"> DETECT</div> <div style="background-color: #ffa500; padding: 5px;"> RESPOND</div> <div style="background-color: #ff6347; 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 by 31 August to the GCISO and their Agency Head on compliance with this policy in the format provided by the GCISO. |

| | |
|------------|--|
| 5.2 | Ensure cyber security risks with a residual rating of high or extreme ⁶ are reported to the GCISO. |
| 5.3 | Ensure the Agency's "crown jewels" are identified and reported to the GCISO. |
| 5.4 | Provide an attestation on cyber security in annual reports as outlined in section 4 and provide a copy to the GCISO. |

⁶ 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 the GCISO on their compliance with this policy in a format provided by the GCISO by 31 August each year. This will largely be a maturity-based assessment on the items listed as mandatory requirements including 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

Cyber security must be addressed in Agency annual reports or in Department annual reports if the Agency does not have a dedicated annual report. 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) is in place or an alternative independent review or audit has been undertaken

The template below is a suggestion only and should be updated to reflect the appropriate wording for the Agency’s situation. The attestation must also be provided to the GCISO.

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.

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

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

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

An independent review/audit/certification of the Agency's ISMS or effectiveness of controls or reporting against the mandatory requirements of the NSW Cyber Security Policy was undertaken by [*review or audit provider*] and found to be adequate or being properly addressed in a timely manner.

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/dfsi-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> |

6 Glossary

| Item | Definition |
|---|--|
| Agency Heads | Agency or Department Head, Chief Executive, or General Manager of any NSW government public service agency. |
| 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 ten groups into which NSW Government agencies are organised to enhance coordination and provision of related services and policy development. |
| 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. |
| 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) |
| GCISO | Government Chief Information Security Officer |
| 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. |
| 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. |
| 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. |
| 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. |

| Item | Definition |
|-------------------------|---|
| 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 |
