# NSW Cyber Security Policy 2026–2027

July 2026

Cyber Security NSW

NSW GOVERNMENT

1

# Purpose

The NSW Cyber Security Policy outlines the mandatory cyber security requirements that all NSW Government departments and public service agencies must put in place to protect their systems, data and services. These requirements set the minimum standard to ensure agencies apply an integrated approach to prevent and respond to cyber security threats. The policy provides end-to-end traceability, linking obligations to implementation, reporting and assurance. This approach creates clear accountability, supports effective control environments, and ensures agencies maintain auditable evidence. This policy aims to:

- establish a consistent minimum standard for cyber security across the NSW Government
- ensure departments and agencies manage cyber security risks in line with risk-based practices
- support the confidentiality, integrity and availability of government services and information.

Non-compliance with this policy increases cyber risk and may cause harm to health and safety, critical services, privacy, and public trust, and may result in increased audit scrutiny.

2

# Scope

## 2.1 Organisations this policy covers

This policy applies to all NSW Government departments, public service agencies, statutory authorities, and NSW Government organisations that submit an annual report to a secretary of a lead department or portfolio, directly to a minister or directly to the Premier of NSW.

## 2.2 Systems this policy covers

This policy applies to:

- information, data and digital assets created and managed by the NSW public sector, including outsourced assets
- information and communications technology (ICT) systems managed, owned or shared by the NSW public sector, including cloud services
- operational technology (OT) and Internet of Things (IoT) devices that handle government data or government-held citizen data, or deliver government services.

Agencies must comply with this policy across all systems, services and environments they own, operate or rely on, including third-party and shared services.

In addition, agencies should consider the guidance in Section 9.1, which outlines other ways to apply this policy to emerging technologies, cloud environments, digital platforms, and other ICT systems beyond the mandatory scope. This proactive approach supports a more resilient and adaptive cyber security posture.

## 2.3 Excluded organisations

This policy is not mandatory for state-owned corporations, non-government organisations, local government, and universities. These entities may adopt this policy as a standard where appropriate.

3

# Mandatory requirements

The mandatory requirements are the minimum cyber security standard all NSW Government agencies must put in place. This standard contains management and governance practices for establishing an effective cyber security program, as well as key systems-based controls to improve cyber hygiene and help agencies better protect themselves against common threats.

These mandatory requirements incorporate the Australian Cyber Security Centre (ACSC) Essential Eight mitigation strategies (mandatory requirements 3.3 to 3.10). They also align with the Protective Security Policy Framework (PSPF) from the Department of Home Affairs and recognised standards and guidance, including ISO/IEC 27001/27002 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

More detailed requirements support these mandatory requirements and set out what organisations must do in practice. NSW Government agencies must ensure that documented implementation evidence supports each mandatory requirement, including relevant reporting and assurance artefacts, to demonstrate compliance.

## Mandatory requirement 1: Govern and identify

| Requirement number | Description |
|---|---|
| 1.1 | Allocate and perform roles and responsibilities for cyber security. |
| 1.2 | Have an executive-level governance committee with appropriate authority to make decisions about cyber security, including OT and IoT. |
| 1.3 | Ensure that the Audit and Risk Committee (ARC) receives regular briefings on cyber security risks, related issues and corrective actions. |
| 1.4 | Develop and maintain a cyber security strategy. |
| 1.5 | Develop and maintain formalised plans, policies and processes for cyber security practices. |
| 1.6 | Establish and maintain processes for asset inventory management and identify asset dependencies. |
| 1.7 | Assess and identify crown jewels and classify systems. |
| 1.8 | Govern the identification, retention and secure disposal of data. |
| 1.9 | Define risk tolerance and risk appetite and manage cyber security risks. |
| 1.10 | Identify and manage third-party service provider risks, including shared ICT services with other NSW Government agencies. |
| 1.11 | Establish and maintain vulnerability management processes. |
| 1.12 | Ensure the assessment of cyber security requirements and impacts as part of change management. |

## Mandatory requirement 2: Detect, respond and recover

| Requirement number | Description |
|---|---|
| 2.1 | Implement event logging and continuous monitoring to detect unusual activity. |
| 2.2 | Maintain a cyber incident response plan and use exercises and post-incident reviews to continuously improve the plan. |
| 2.3 | Report cyber incidents and provide information on threats to Cyber Security NSW. |
| 2.4 | Include cyber security in business continuity and disaster recovery planning. |

## Mandatory requirement 3: Protect

| Requirement number | Description |
|---|---|
| 3.1 | Conduct awareness activities, including mandatory cyber security awareness training. |
| 3.2 | Implement access controls to ensure authorised access only. |
| 3.3 | Patch applications (ACSC Essential Eight). |
| 3.4 | Patch operating systems (ACSC Essential Eight). |
| 3.5 | Implement multi-factor authentication (MFA) (ACSC Essential Eight). |
| 3.6 | Restrict administrative privileges (ACSC Essential Eight). |
| 3.7 | Implement application control (ACSC Essential Eight). |
| 3.8 | Securely configure Microsoft Office macro settings (ACSC Essential Eight). |
| 3.9 | Implement user application hardening (ACSC Essential Eight). |
| 3.10 | Maintain backups of important data, software and configuration settings (ACSC Essential Eight). |
| 3.11 | Establish and maintain secure configurations. |
| 3.12 | Define and implement data security controls. |
| 3.13 | Implement email security controls. |
| 3.14 | Implement controls for endpoint protection, including mobile devices. |
| 3.15 | Implement network security controls. |

4

# Essential Eight

The ACSC continues to maintain the Essential Eight as the baseline set of 8 mitigation strategies for protecting systems against common cyber threats. Mandatory requirements 3.3 to 3.10 embed the Maturity Level One Essential Eight controls for consistency and time-series metrics. Agencies must apply these controls in relevant ICT environments and use additional safeguards based on threats and risks identified through their cyber security risk management processes (see Threat-based cyber risk management in section 9.2). Cyber Security NSW reviews relevant ACSC updates annually and adjusts as necessary.

5

# Applying this policy based on risk

All mandatory requirements represent the minimum acceptable cyber security baseline; agencies still must meet these standards. Where full implementation is not achievable, a risk-based approach permits managed expectations through formal processes but does not remove or reduce an agency's underlying compliance obligations.

Agencies must document system-level exceptions to mandatory requirements and have an appropriate authority approve them through a formal process.

Exception documentation should include:

- detail, scope and reason for exceptions
- detail of compensating controls associated with exceptions, including:
  - detail, scope and reason for compensating controls
  - expected implementation lifetime of compensating controls
  - when agency will next review compensating controls
- system risk rating before and after implementing compensating controls
- any caveats placed on using the system due to exceptions
- acceptance by an appropriate authority of the remaining risk for the system
- when an appropriate authority will next consider the necessity of exceptions (noting exemptions should not be approved beyond one year).

Using a formal exceptions process and compensating controls should not preclude an organisation from being assessed as compliant. This approach to exceptions comes from, and applies to, assessments under the ACSC Essential Eight assessment process guide.

6

# Reporting and assurance

Agencies must show that they comply with each mandatory requirement through documented implementation evidence, assurance assessments, and formal attestation by an appropriate authority. Compliance cannot be assumed and agencies must maintain a continuous state of readiness to provide auditable evidence of their cyber security posture against all mandatory requirements.

## 6.1 Annual reporting requirements

Agencies must report their compliance with the mandatory requirements for the previous financial year and provide all other required reporting under this policy. They must report in line with the methods and templates in the reporting guidance.

Agencies must identify their portfolio chief information security officer (CISO) or senior cyber security lead and stay engaged with them throughout the reporting period to meet reporting requirements.

### By 30 June

Portfolio CISOs **must** provide Cyber Security NSW with:

- an updated list of agencies in the portfolio
- confirmation of each agency's reporting pathway (either through the portfolio CISO or directly to Cyber Security NSW).

### By 31 October

Each agency **must** provide Cyber Security NSW with the following reports:

- an assurance assessment against all mandatory requirements in the NSW Cyber Security Policy for the previous financial year.
- a list of all high and extreme remaining cyber security risks (or 'not applicable' if none), in the required format
- an assessment against all-of-government cyber security risks in the required format, following Cyber Security NSW guidance
- a crown jewel asset inventory (mandatory requirement 1.7) in the required format
- a cyber security attestation for the agency, including compliance with the NSW Cyber Security Policy.

Agency reports must be accurate, based on evidence and verifiable. Agencies must keep this evidence and provide it to Cyber Security NSW on request. They must also find and fix any discrepancies between what they report and what is in place, including scope.

Reported risks must match the agency's enterprise risk management framework and its approved risk appetite.

## 6.2 Attestation

Agencies must submit a signed annual attestation for the previous financial year. If the attestation covers multiple agencies, it must list all of them.

The attestation **must** clearly confirm that:

- the agency has appropriate oversight and governance for cyber security
- the agency has assessed its cyber security risks
- the agency tracks and reviews remaining risks against its risk appetite at least every quarter
- the agency head has approved any mandatory requirements that are partially met, not met, or not applicable, with documented reasons and any compensating controls.

Agencies should take advantage of internal audit functions or ARC oversight of the attestation before submission.

## 6.3 Information sharing

Agencies may share information with other NSW Government organisations to support coordinated cyber security responses and reduce duplicate data collection. This can include nominated organisations, such as Insurance & Care NSW (icare), where appropriate.

When sharing information, agencies **must**:

- approve the sharing
- document it with formal agreements, such as memoranda of understanding (MOU)
- use established coordination channels, such as the NSW Government Cyber Security Steering Group (CSSG).

7

# Variations to reporting requirements

## 7.1 Exemptions and extensions

Cyber Security NSW will consider exemptions and extensions only in exceptional circumstances and only for one reporting year.

Agencies must request an exemption if they cannot meet the annual reporting requirements of section 6.1 of this policy.

Agencies must request an extension if they cannot submit their report by 31 October of each year.

They must submit all requests in writing to Cyber Security NSW at info@cyber.nsw.gov.au before 31 October in line with the reporting guidance.

## 7.2 Treatment of ‘not applicable’ responses

Agencies may assess mandatory requirements as not applicable to their operations. They must clearly explain each ‘not applicable’ response in their attestation letter, including any compensating controls where relevant. They do not need to submit a formal exemption request.

If agencies are unsure whether a requirement applies, they must consult their portfolio CISO and seek clarity from Cyber Security NSW if needed.

8

# Roles and governance

This section sets out the minimum cyber security roles and responsibilities that agencies must assign and carry out under mandatory requirements 1.1 to 1.3. It also sets out the governance arrangements agencies must put in place under mandatory requirements 1.10, 3.2 and 3.5. Agencies do not need to use the exact role names or titles outlined in this section. These roles and responsibilities apply at both the agency and portfolio level, as described in section 2.1.

## 8.1 Accountable authorities

### 8.1.1 Agency heads

Agency heads, including commissioners, chief executive officers and department secretaries, are responsible for:

- ensuring their agency complies with the NSW Cyber Security Policy, including timely and accurate reporting
- ensuring the agency develops, implements and maintains an effective cyber security strategy and supporting plans
- setting the agency's cyber security risk appetite in line with the approved all of government Internal Audit and Risk Management Policy
- approving and formally acknowledging any mandatory requirements assessed as partially met, not met or not applicable through the assurance assessment process
- ensuring the agency adequately funds, resources and prioritises cyber security, including training, awareness and ongoing improvement
- approving internal cyber security policies, standards and frameworks as required
- ensuring the chief information officers (CIOs), or a delegate, participates in and carries out responsibilities in the ICT and Digital Leadership Group (IDLG)
- ensuring internal audit provides assurance on compliance with this policy
- ensuring risk management functions support effective cyber security risk management.

In addition, department secretaries:

- appoint a senior executive, within the agency or across the portfolio, with the authority and accountability to carry out the cyber security responsibilities in this policy, including at the portfolio level
- appoint a senior executive responsible for industrial automation and control systems (IACS) cyber security for the agency or portfolio, where needed
- ensure portfolio CISOs, chief security officers (CSOs) or equivalent senior executives provide effective oversight and support to help agencies meet their policy and reporting obligations
- ensure all agencies in the portfolio put in place and maintain an effective cyber security program in line with this policy
- support the development and delivery of agency and portfolio cyber security strategies and plans.

# 8.2 Delivery roles

## 8.2.1 NSW Chief Cyber Security Officer (NSW CCSO)

The NSW Chief Cyber Security Officer (NSW CCSO) is responsible for:

- creating and implementing the NSW Government Cyber Security Strategy
- building and promoting a cyber-aware culture across the NSW Government
- reporting on consolidated agency compliance, maturity and systemic risk
- chairing the NSW Government CSSG
- consulting with agencies and providing advice, guidance and help on cyber security matters, including policy, capability and capacity improvements
- recommending and formally recording exemptions to the NSW Cyber Security Policy
- representing the NSW Government on cross-jurisdictional cyber security matters
- supporting agencies to share cyber threat information and to collaborate on threat intelligence to manage whole of government cyber risk
- receiving, analysing and reporting on high cyber risks, and monitoring cyber incident reporting across the NSW Government
- creating and implementing NSW Government cyber incident response arrangements
- coordinating the NSW Government response to major cyber incidents and cyber emergencies.

## 8.2.2 CISOs and CSOs

All CISOs, CSOs and staff with equivalent responsibilities are responsible for:

- setting and implementing a cyber security strategy, architecture and risk management approach to protect information and systems
- developing and maintaining a cyber security plan that aligns with the agency's risk management framework
- recommending how to treat cyber security risks that exceed the agency's risk appetite
- implementing policies, procedures, practices and technologies to comply with the NSW Cyber Security Policy
- reviewing and providing recommendations on exemptions to agency or portfolio information security policies and standards, where needed
- coordinating and submitting NSW Cyber Security Policy reporting, ensuring it is accurate, complete and on time
- investigating, responding to and reporting cyber incidents to agency governance forums and Cyber Security NSW, in line with severity levels and reporting requirements
- maintaining evidence for assurance assessments and making it available as required
- ensuring agencies using shared services have appropriate agreements, such as MOUs, in place, including requirements to meet cyber security standards and comply with the NSW Cyber Security Policy
- reporting all cyber incidents to Cyber Security NSW through the Cyber Portal within 24 hours of detection and classification
- working with portfolio CISOs or CSOs, where needed, to support coordinated risk management, incident response and compliance across the portfolio.

Portfolio CISOs, CSOs and staff with equivalent responsibilities also:

- manage the portfolio cyber security budget and allocate resources to address risks and improvement priorities
- apply for and coordinate access to relevant programs, initiatives or funding (for example, the Digital Restart Fund or ACSC uplift programs)
- support agencies in the portfolio to put in place and maintain effective cyber security strategies and programs, including through governance forums, collaboration, resourcing and budgeting advice, and guidance on compliance and reporting
- ensure agencies using portfolio-level shared services have appropriate agreements in place that require compliance with cyber security standards and the NSW Cyber Security Policy.

### 8.2.3 CIOs and chief operating officers (COOs)

CIOs, COOs and staff with equivalent responsibilities are responsible for:

- working with CISOs, CSOs and business leaders to implement the NSW Cyber Security Policy, including allocating enough resources and funding to manage cyber risks in their areas
- ensuring clear ownership of systems and data, and maintaining accountability for related cyber security risks and controls
- putting in place and supporting a cyber security strategy and plan that addresses threats, risks and vulnerabilities, and aligns with the agency's risk tolerance
- ensuring all staff, including consultants, contractors and service providers, understand and follow the cyber security requirements for their roles
- defining and maintaining the scope of their cyber security responsibilities across agency assets, including information, ICT systems, building management systems and IACS, where relevant
- supporting CISOs, CSOs or equivalent roles to deliver the agency's cyber security responsibilities
- ensuring a secure-by-design approach for new initiatives, major changes and system upgrades, including legacy systems
- ensuring staff and providers understand their role in building, operating and maintaining secure systems.

### 8.2.4 Information security managers, cyber security managers and senior responsible officers

Within their agency or portfolio, information security managers, cyber security managers and senior responsible officers are responsible for:

- managing and coordinating responses to cyber incidents, emerging threats and vulnerabilities
- developing, maintaining and putting cyber security procedures, standards and guidelines into practice
- implementing and operating controls to reduce cyber security risks
- advising on cyber security risks from business activities, operational changes and technology initiatives
- managing the lifecycle of cyber security tools and capabilities, from design to decommissioning
- ensuring cyber security technologies and services perform reliably and meet availability and capacity needs
- supporting regulatory compliance, assurance and audit activities, and coordinating and managing any necessary fixes
- developing and maintaining metrics and checks to monitor how well cyber security controls work
- managing day to day cyber security operations and service delivery.

### 8.2.5 Information management officers

Information management officers manage information and records so the agency handles them in line with its recordkeeping plan, policies and procedures. Agencies should assign one or more people to this role.

Information management officers are responsible for:

- acting as the main contact in the agency for information management matters that support cyber security, including protecting, handling and managing information throughout its lifecycle
- ensuring the agency promptly escalates and reports cyber incidents that involve information damage, loss or unauthorised access to the right teams.

### 8.2.6 Privacy officers

Privacy officers ensure the agency builds strong privacy protections into its operations and cyber security practices. Agencies should assign a person to this role, as recommended by the Information and Privacy Commission (IPC) NSW.

Privacy officers are responsible for:

- acting as the main point of contact for privacy matters within the agency, with the public and with IPC NSW
- ensuring the agency builds privacy into its cyber security policies and procedures
- helping identify and manage privacy impacts in new projects, systems, services and proposed legislation
- working with cyber security teams to plan for incident response involving personal information
- coordinating the investigation of privacy incidents, including assessing breaches and managing notifications to affected individuals and regulators
- managing and responding to privacy complaints in line with legal and policy requirements.

### 8.2.7 Agency staff

Agency staff support and contribute to the agency's cyber security culture. Their responsibilities include:

- following good cyber hygiene practices, including using strong passwords and secure authentication
- identifying and promptly reporting suspected or actual cyber incidents and threats
- completing required cyber security awareness and role based training
- protecting classified, sensitive and official information in line with agency policies
- staying up to date with cyber security responsibilities and best practices for their role.

# 8.3 Oversight functions

## 8.3.1 Internal audit

Agency internal audit teams give the agency head independent assurance that the agency effectively manages risks by reviewing the design of controls and how well they work.

They are responsible for:

- checking that the agency's cyber security strategy and plan align with business objectives
- regularly reviewing how well the agency follows the NSW Cyber Security Policy and implements cyber security controls
- providing independent assurance on the effectiveness of cyber security governance, risk management and controls
- reporting audit and assurance results to the ARC and the agency head, as required.

## 8.3.2 Risk

Risk teams lead and coordinate the agency's approach to risk management. They are responsible for:

- aligning cyber security risk management with the agency's goals and priorities
- carrying out risk assessments to identify and evaluate cyber threats and vulnerabilities
- managing cyber security risks, including risks from third-party service providers and shared services
- integrating cyber security risks into the agency's risk management framework and risk appetite
- working with the portfolio CISO or CSO, where relevant, to align cyber risk approaches across the agency and portfolio.

# 8.4 Governance arrangements

## 8.4.1 IDLG

The NSW Government Chief Information and Digital Officer (GCIDO) chairs the IDLG, which includes CIOs from across the NSW Government. The IDLG is responsible for:

- endorsing the NSW Cyber Security Policy and any updates
- overseeing and supporting consistent implementation of the policy across the NSW Government
- reviewing consolidated agency and portfolio reporting against the policy's mandatory requirements
- providing leadership, advocacy and support to strengthen cyber security capability and culture across agencies and portfolios
- promoting ongoing improvement in cyber security governance, resilience and risk management.

### 8.4.2 Managing third-party service providers

Agencies must manage cyber security risks from third-party service providers. At a minimum, this includes:

- ICT service providers, including NSW Government shared service providers
- other providers that process or store the agency's sensitive information.

Agencies **must**:

- set clear security requirements in contracts, monitor compliance and enforce agreed obligations
- identify and manage third-party cyber security risks through enterprise risk management processes
- carry out ongoing risk-based reviews of third-party compliance with contractual and security requirements
- maintain a complete and up-to-date list of all third-party service providers
- include clear responsibilities in contracts, define acceptable risk levels and set out how to respond if a provider does not meet security requirements (for example, break clauses or offboarding)
- ensure they meet all relevant mandatory requirements when third-party providers support the agency's implementation of this policy.

### 8.4.3 Managing NSW Government shared service providers

Departments, agencies and statutory bodies that provide shared services under the NSW Cyber Security Policy must provide relevant reporting information to the organisations that use those services. This reporting supports accountability and helps manage third party cyber security risks across government.

Shared service providers **must report to affected organisations**:

- any cyber security risks, incidents or vulnerabilities that could impact the organisation's security or obligations
- any mandatory requirements that are partially met, not met, not applicable or managed by a third-party, including details of any compensating controls.

# Advisory guidance

This section provides non-mandatory guidance to help agencies with reporting, assurance and implementation of the policy. Although agencies must implement the mandatory requirements as the minimum standard for compliance, this guidance supports agencies to extend consistent cyber security practices beyond core systems, recognising that evolving technology requires a considered and adaptive approach.

## 9.1 Additional ways to apply this policy

Where appropriate, agencies may also apply the NSW Cyber Security Policy to:

- other ICT systems, including:
  - cloud-hosted and cloud-native environments
  - digital platforms, enterprise applications and automation
  - end-user and enterprise mobility environments
- third-party and shared service environments that store, process or transmit agency information
- emerging and evolving technology risks, including:
  - risks from automation and autonomous systems
  - risks from reliance on external providers and supply chains
  - cryptographic risks, including those linked to advances in quantum computing.

### 9.1.1 Application to artificial intelligence (AI)

Agencies may apply the mandatory requirements to AI systems and AI-enabled services that process, generate or analyse government information. This includes systems developed in-house and third-party tools.

Agencies may apply existing controls based on risk, including:

- managing risks from AI vendors and service providers
- controlling access to AI tools and services
- protecting data from unauthorised use, disclosure or leakage through AI systems
- logging and monitoring AI system use and outputs, where relevant
- managing changes to AI systems and updates, including risks from third party providers.

Agencies should also ensure that, where they use cryptographic controls, providers can move to quantum-resistant methods as standards evolve, particularly for sensitive or long-lived data.

## 9.2 Threat-based cyber risk management

Agencies face different cyber threats depending on their services, information and operations. They must manage cyber security risks based on these threats, in line with their business objectives, risk appetite and service criticality.

Agencies should use the mandatory requirements to identify, assess and prioritise cyber risks. They should apply additional controls where risks or potential impacts are higher.

Agencies that deliver critical services, handle sensitive or high value information, or run high-risk projects must apply stronger controls. This includes building additional safeguards into system design, major programs and transformation initiatives.

As part of a threat based approach, agencies should:

- focus on the threats, attack patterns and exposures most relevant to their environment
- use threat modelling or similar methods to inform risk assessments and prioritise controls
- implement controls that match the level of risk, including stronger protections where needed (for example, higher Essential Eight maturity; zero trust principles; and controls for cloud, mobility, OT and IoT
- align controls with recognised frameworks, such as the Australian Signals Directorate information security manual, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001, ISO/IEC 27002:2022 and ISO/IEC 62443.
- consider service criticality and information sensitivity when deciding how much control coverage is necessary.

Agencies should share information on key threats and risks with Cyber Security NSW through approved channels, such as the NSW Cyber Security Cyber Portal, to support coordinated risk management across government.

Threat-based risk management is ongoing and supports continuous improvement. Agencies with less maturity should identify longer term improvements through their cyber security strategies and plans. Cyber Security NSW provides optional resources to support this work.

The ACSC updates the Essential Eight and its guidance to reflect changes in the threat environment and lessons from cyber incidents. Agencies should monitor these updates and prioritise any new or changed requirements as part of their ongoing risk management.

## 9.3 Application to quantum technologies and cryptographic risk

Agencies may consider risks from quantum computing where systems use cryptographic controls to protect government information, particularly for sensitive or long lived data.

Agencies may apply existing controls based on risk, including:

- identifying systems and data that rely on cryptographic protections and assessing their exposure to future quantum risks
- planning for transition to quantum resistant cryptographic approaches in line with Australian Signals Directorate (ASD) guidance
- considering data longevity, system dependencies and business impact when prioritising transition activities
- ensuring third party providers that use cryptographic controls can support future transition to quantum resistant methods.

## 9.4 Additional third-party service provider management

Agencies must manage cyber security risks from third-party service providers. This includes ICT providers (such as NSW Government shared service providers) and those that process or store the agency's sensitive information, as defined in mandatory requirement 1.10.

The following practices help strengthen third-party risk management:

- clearly define responsibilities for cyber security incidents or data breaches, including immediate notification and cooperation during response
- apply security controls based on data classification, and ensure data is properly separated
- consider data sovereignty, including where data is hosted and supported
- meet privacy obligations when collecting, holding or processing personal information
- control and monitor privileged access.

## 9.5 Help implementing the NSW Cyber Security Policy

Cyber Security NSW provides guidance and toolkits to help agencies implement the NSW Cyber Security Policy. For copies or advice, please contact info@cyber.nsw.gov.au

10

# Useful links

| Issuer | Reference | Document |
|---|---|---|
| **NSW Government** | https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1989-134 | *State Owned Corporations Act 1989* |
| | https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-017 | *State Records Act 1998* |
| | https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-133 | *Privacy and Personal Information Protection Act 1998* |
| | https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2002-071 | *Health Records and Information Privacy Act 2002* |
| | https://www.legislation.nsw.gov.au/#/view/act/2009/52 | *Government Information (Public Access) Act 2009* |
| | https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2013-040 | *Government Sector Employment Act 2013* |
| | https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2015-060 | *Data Sharing (Government Sector) Act 2015* |
| | https://www.infrastructure.nsw.gov.au/sis-2018/ | State infrastructure strategy 2018 |
| | https://www.nsw.gov.au/rescue-and-emergency-management/sub-plans/cyber-security | Cyber security emergency sub plan |
| | https://arp.nsw.gov.au/tpp20-08-internal-audit-and-risk-management-policy-for-the-general-government-sector/ | TPP20-08 Internal Audit and Risk Management Policy for the General Government Sector |
| **NSW Department of Customer Service** | https://data.nsw.gov.au/nsw-government-information-classification-labelling-and-handling-guidelines | NSW Government Information Classification, Labelling and Handling Guidelines |
| | https://www.digital.nsw.gov.au/delivery/cyber-security/2026-2028-nsw-government-cyber-security-strategy | 2026–2028 NSW Government Cyber Security Strategy |
| | https://www.digital.nsw.gov.au/policy/data-strategy | Data Strategy |
| | https://www.digital.nsw.gov.au/delivery/cyber-security/policies | Cyber Security NSW Circulars |
| | https://www.digital.nsw.gov.au/policy/artificial-intelligence/ai-governance-assurance-and-frameworks/nsw-ai-assessment-framework | Office for AI – AI Assessment Framework |

| Issuer | Reference | Document |
|---|---|---|
| **IPC NSW** | https://www.ipc.nsw.gov.au/guide-mandatory-notification-data-breach-scheme-guide-managing-data-breaches-accordance-ppip-act | Guide – Mandatory Notification of Data Breach Scheme: Guide to managing data breaches in accordance with the *PPIP Act* |
| **Audit Office of NSW** | https://www.audit.nsw.gov.au/our-work/reports/detecting-and-responding-to-cyber-security-incidents- | Detecting and responding to cyber security incidents |
| **NSW Treasury** | https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management/risk | Risk management toolkit |
| **NSW Department of Premier and Cabinet** | https://arp.nsw.gov.au/m1999-19-applicability-memoranda-and-circulars-state-owned-corporations-socs | Memorandum M1999-19 Applicability of Memoranda and Circulars to State Owned Corporations (SOCs) |
| **State Records NSW** | https://www.nsw.gov.au/nsw-government/recordkeeping/policies-and-standards/standard-on-records-management | Standard on records management |
| | https://www.nsw.gov.au/nsw-government/recordkeeping/secure-and-store/using-cloud-computing-services | Cloud computing: implications for records management |
| | https://www.nsw.gov.au/nsw-government/recordkeeping/secure-and-store/taking-or-sending-records-out-of-nsw | Guidance on taking or sending records out of NSW |
| **Australian Government Department of Home Affairs** | https://www.legislation.gov.au/C2018A00029/latest/text | *Security of Critical Infrastructure Act 2018* |
| | https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy | Cyber security strategy |
| **Australian Government Attorney-General's Department** | https://www.protectivesecurity.gov.au/ | The Protective Security Policy Framework |
| | https://www.protectivesecurity.gov.au/resources/australian-government-and-international-resources | Australian Government and international resources |

| Issuer | Reference | Document |
|---|---|---|
| **Australian Government ASD** | https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism | Information security manual |
| | https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography | Planning for post-quantum cryptography |
| **Australian Government Office of the Australian Information Commissioner** | https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/ | Australian Privacy Principles guidelines |
| **ISO** | https://www.iso.org/standard/75106.html | ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements |
| | https://www.iso.org/standard/44374.html | ISO 27031:2025 Cybersecurity – Information and communication technology readiness for business continuity |
| | https://www.iso.org/standard/76070.html | ISO/IEC 27032:2023 Cybersecurity – Guidelines for Internet security |
| **National Institute of Standards and Technology** | https://www.nist.gov/cyberframework | Cybersecurity Framework |
| **New Zealand National Cyber Security Centre** | https://www.ncsc.govt.nz/assets/guidance/Documents/charting-your-course-governance-full-nov-2019.pdf | Cyber Security Governance |

11

# Glossary

| Item | Definition |
|---|---|
| **Access control** | The process of deciding who can access systems, applications, information and physical spaces. |
| **Agency head** | The person in charge of an agency. For departments, this is the secretary of the department; for any other cases, it's the head of the agency listed in Part 2 or 3 of Schedule 1 of the Government Sector Employment Act 2013. |
| **All-of-government (AoG)** | NSW Government-wide activities and reporting that apply across agencies and portfolios. |
| **Application control** | An approach that allows only approved applications to run on systems. |
| **Artificial intelligence (AI)** | The ability of computer systems to perform tasks that usually require human intelligence, such as learning, reasoning and making decisions. |
| **Assurance assessment** | An evidence-based assessment to support reporting and the agency head's attestation. |
| **Attestation** | A formal, signed declaration in which an organisation confirms that it has assessed its cyber security against relevant requirements for a specific reporting period, that the results are accurate and complete, and that it has identified, acknowledged and accepted any areas of non-compliance. |
| **Audit log** | A time-ordered record of system activities, including who accessed the system and what they did. |
| **Audit trail** | A time-ordered record that shows the steps leading to, or surrounding, a specific event or action. |
| **Authentication** | Verifying that a user, device or system is who or what they claim to be before allowing access to resources in a system. |
| **Authorisation** | Defining what a user, device or system is allowed to access or do. |
| **Availability** | Making sure authorised users can access systems and information when necessary. |
| **Business continuity plan** | A document that explains how an organisation will keep critical services running during an incident, or restore them quickly. |
| **Classification** | Grouping systems and information based on the impact if they are compromised. |

| Item | Definition |
|---|---|
| **Critical infrastructure** | Physical facilities, supply chains and ICT networks that are essential. If they fail for a long time, they can significantly harm society, the economy or national security. |
| **Crown jewels** | An organisation's most important systems or most valuable information. |
| **Cyber attack** | A deliberate attempt to disrupt, damage or gain unauthorised access to systems, networks or data. Note that multiple global definitions of 'cyber attack' exist. |
| **Cyber event** | Something that happens in a system or network that may indicate a policy breach or controls failure but does not compromise information or systems. |
| **Cyber incident** | An unwanted or unexpected event that could affect the security or availability of systems or the information they handle. |
| **Cyber incident response plan** | A plan that explains how the organisation will respond to cyber incidents. |
| **Cyber security** | Measures that protect systems, devices and information from unauthorised access, damage or disruption. |
| **Cybercrime** | Crime that targets computers or uses them to commit offences, such as hacking, malware attacks and online fraud. |
| **Data breach** | When data is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. |
| **Disaster recovery plan** | A plan that explains how the organisation will restore systems and services after a disaster. |
| **Essential Eight** | Eight key cyber security strategies recommended by the ASD to make it much harder for attackers to compromise systems and data. |
| **Full backup** | Testing the full restoration of backups when first implemented and whenever major infrastructure changes occur. |
| **Functional exercise (simulation)** | A simulated exercise where participants carry out their roles during a cyber incident. It tests systems, tools and communication, and helps teams practise detecting and responding to threats. |
| **Industrial automation and control systems (IACS)** | Also called industrial control systems (ICS), these are systems that monitor or control industrial and physical operations. They include systems used in manufacturing and processing plants; building environmental controls; utilities such as electricity, gas, and water; pipelines and petroleum facilities; transportation networks; and other operations that rely on automated, remotely controlled, or monitored assets. |
| **Information and communications technology (ICT)** | Also called information technology (IT), this includes the systems, devices, software and networks that organisations use to store, manage and share information. |

| Item | Definition |
|---|---|
| **Information security** | Protecting information and systems from unauthorised access, use, change or disruption so they stay secure and available. |
| **Information security management system (ISMS)** | A structured set of policies, processes and resources that an organisation uses to protect its information assets. An ISMS provides a systematic way to establish, operate, monitor, review and improve information security so it supports the organisation's business objectives. |
| **Inherent risk** | The level of risk based on the current situation, without considering additional risk treatments. |
| **Internet of Things (IoT)** | A network of connected devices, such as sensors, vehicles and appliances, that collect and share data over the internet. |
| **Macro** | A set of instructions that runs automatically to perform a task. |
| **Multi-factor authentication (MFA)** | A way to verify identity by requiring 2 or more types of evidence, such as something you know, have or are. |
| **Operational technology (OT)** | Hardware and software that monitor or control physical equipment, processes or events. |
| **Partial backup** | Restoring some data, such as selected files or a database, rather than the whole system. |
| **Patching** | Updating software to fix problems, improve performance or address security issues. |
| **Portfolio** | Also called the lead portfolio department or department, this is a group of NSW Government agencies organised under a lead department, as set out in the Government Sector Employment Act 2013, to coordinate related services and policy areas. |
| **Post-quantum cryptography** | Cryptographic algorithms designed to resist attacks from quantum computers which can break widely used schemes. |
| **Privacy officer** | A person responsible for managing privacy matters within an agency, as recommended by the IPC NSW. |
| **Private Automatic Branch Exchange (PABX)** | A private telephone system that an organisation uses to manage internal and external calls. |
| **Privileged user** | A user who has high-level access and can change system settings or bypass security controls, even if their role has only limited privileges. |
| **Public service agency** | A NSW Government agency defined under the Government Sector Employment Act 2013, including a department, a public service executive agency or a separate public service agency. |

| Item | Definition |
|---|---|
| **Remote access** | Accessing a system from outside an organisation's network, usually over the internet. |
| **Residual risk** | The level of risk that remains after controls or treatments are in place. |
| **Risk appetite** | The level and type of risk an organisation is willing to accept. |
| **Risk tolerance** | How much risk an organisation is prepared to accept after it has put controls in place. |
| **Secure-by-design principles** | Designing systems and software to be secure from the start by reducing vulnerabilities and anticipating potential threats. |
| **Security breach** | A cyber incident where someone gains unauthorised access to systems, data or devices by bypassing security. |
| **State-owned corporation** | A commercial business owned by the NSW Government, such as Essential Energy, Forestry Corporation of NSW, Hunter Water, Landcom, Port Authority of NSW, Sydney Water, Transport Asset Manager of NSW – Asset Management Council. |
| **Supply chain** | The people, organisations and activities involved in delivering a product or service. |
| **Systems** | The software, hardware, data and networks an organisation uses, including specialised systems, such as industrial control systems, phone systems, building management systems and internet-connected devices. |
| **Tabletop exercise** | A discussion exercise where participants work through a hypothetical cyber incident and agree on how to respond and recover, using the organisation's plans and processes. |

# Detailed requirements

| Mandatory requirement | Detailed requirement |
|---|---|
| **1.1 Allocate and perform roles and responsibilities for cyber security.** | 1.1.1 Ensure the agency assigns, maintains and performs the roles and responsibilities set out in the NSW Cyber Security Policy. |
| | 1.1.2 Define and allocate additional roles and responsibilities for cyber security, and review these according to organisational need. |
| **1.2 Have an executive-level governance committee with appropriate authority to make decisions about cyber security, including OT/IoT.** | 1.2.1 Have a governance committee (shared or dedicated) at the executive level that:<br>• has appropriate delegations or seniority to make decisions on cyber security matters<br>• meets at least quarterly<br>• ensures that the agency head, as the ultimate authority for cyber security, is regularly briefed on cyber security risks, related issues and corrective actions. |
| | 1.2.2 Ensure the committee has an agreed terms of reference with accountability for cyber security governance over information security, as well as the cyber security of ICT, OT and IoT systems. |
| | 1.2.3 Ensure the agency head has ultimate accountability for the cyber security of the agency. |
| **1.3 Ensure that the ARC is briefed regularly on cyber security risks, related issues and corrective actions.** | 1.3.1 Ensure cyber security is a standing item on the agenda at the department or agency audit and risk committees, including risks, related issues and corrective actions. |
| **1.4 Develop and maintain a cyber security strategy.** | 1.4.1 Develop and maintain a cyber security strategy that aligns to the organisation's strategic business objectives and captures key threats, risks, vulnerabilities, actions and initiatives to make improvements and address any gaps. |
| | 1.4.2 The agency head endorses the cyber security strategy. |
| **1.5 Develop and maintain formalised plans, policies and processes for cyber security practices.** | 1.5.1 Develop and maintain plans, policies and processes for managing cyber security risks based on organisational context, the agency's cyber security strategy and NSW Cyber Security Policy requirements. |

| Mandatory requirement | Detailed requirement |
|---|---|
| **1.6 Establish and maintain processes for asset inventory management and identify asset dependencies.** | 1.6.1 Establish and maintain inventories for crown jewel assets, enterprise ICT (including cloud), software, OT, IoT and network assets. |
| | 1.6.2 Establish and maintain processes for periodically reconciling accuracy and completeness of asset inventories. |
| | 1.6.3 Establish and maintain processes for managing the lifecycles of assets and software, including risk-managed disposal and replacement of end-of-support assets and software. |
| | 1.6.4 Identify and document external upstream and downstream dependencies of enterprise ICT (including cloud), OT and IoT assets, covering at least crown jewel assets. |
| **1.7 Assess and identify crown jewels and classify systems.** | 1.7.1 Implement a crown jewel identification framework and identify crown jewel assets. |
| | 1.7.2 Classify systems and information for business value, mission criticality and sensitivity (as defined in the NSW Government Information Classification, Labelling and Handling Guidelines). |
| **1.8 Govern the identification, retention and secure disposal of data.** | 1.8.1 Establish and maintain inventories for data assets covering at least 'Official: Sensitive' classification (as defined in the NSW Government Information Classification, Labelling and Handling Guidelines). |
| | 1.8.2 Define data retention requirements (with reference to any legislative and policy requirements that apply) for categories of data, including minimum and maximum retention timeframes; for at least crown jewels, and conduct periodic reconciliation of data assets against data retention requirements. |
| | 1.8.3 Establish and maintain processes for secure disposal of data and associated assets in line with the type of data and its information classification. |
| **1.9 Define risk tolerance and risk appetite and manage cyber security risks.** | 1.9.1 Define risk appetite and risk tolerance for cyber risks and have the secretary or relevant agency head approve the cyber risk appetite. |
| | 1.9.2 Ensure cyber security risks across all areas of the agency, including inherited and shared security risks, are identified, assessed, managed, documented and reported as part of (or in line with) the agency's enterprise risk management framework. |
| | 1.9.3 Ensure the agency head or authorised officer has formally approved applicable residual risks where NSW Cyber Security Policy mandatory requirements are not in place and has done so in line with the agency's risk management acceptance criteria. |
| | 1.9.4 Escalate unmitigated cyber security risks, including inherited and shared security risks, that exceed risk appetite or tolerance to appropriate delegates in line with the agency's risk management framework or acceptance criteria. |

| Mandatory requirement | Detailed requirement |
|---|---|
| **1.10 Identify and manage third-party service provider risks, including shared ICT services with other NSW Government agencies.** | 1.10.1 Create and maintain an inventory of third-party service providers, including ICT service providers. |
| | 1.10.2 Ensure there is a contractually supported process for third-party service providers to notify the agency of suspected or actual security incidents and data breaches. |
| | 1.10.3 Have processes to monitor and assess adherence of third-party service providers to cyber security requirements, including using assurance reports, audits, test results or other evaluations. |
| | 1.10.4 Include clauses in contracts with third-party service providers for cyber security requirements and break clauses associated with failure to meet security requirements. |
| **1.11 Create and maintain vulnerability management processes.** | 1.11.1 Create and maintain a vulnerability management process to identify and triage technical vulnerabilities. |
| | 1.11.2 Assess alerts from Cyber Security NSW and action those that apply to the agency's systems, consistent with the agency's vulnerability management processes. |
| **1.12 Ensure the assessment of cyber security requirements and impacts as part of change management processes.** | 1.12.1 Assess cyber security requirements within IT and enterprise change management processes, including impacts to implement and maintain any required cyber security controls. |
| | 1.12.2 Manage changes to cyber security technical controls through enterprise IT change management processes. |
| | 1.12.3 Test applicable cyber security controls and secure configurations upon finishing a significant change and update relevant documentation. |
| **2.1 Implement event logging and continuous monitoring to detect unusual activity.** | 2.1.1 Implement and maintain processes to log and monitor critical security events by establishing baseline patterns; align to the threats and risks identified for the organisation, including inherited and shared security risks; and act on relevant anomalies or unexpected behaviour. |
| **2.2 Maintain a cyber incident response plan and use exercises and post-incident reviews to continuously improve the plan.** | 2.2.1 Develop and maintain a cyber incident response plan that defines and documents incident roles, responsibilities and authorities (including incident declaration). Test the plan to support a coordinated internal and external response and recovery, including carrying out preapproved actions. |
| | 2.2.2 Test the cyber incident response plan at least yearly. |
| | 2.2.3 Perform post-incident reviews and use results to update processes and templates. |
| | 2.2.4 Develop and maintain a cyber incident register. |

| Mandatory requirement | Detailed requirement |
|---|---|
| **2.3 Report cyber incidents and provide information on threats to Cyber Security NSW.** | 2.3.1 Create and maintain the agency's incident management procedures. Have a defined workflow that indicates when and where to share information and intelligence, including reporting cyber event information to Cyber Security NSW. |
| | 2.3.2 Report all cyber incidents through the Cyber Security NSW Cyber Portal within 24 hours of detection and classification. |
| **2.4 Include cyber security in business continuity and disaster recovery planning.** | 2.4.1 Incorporate cyber incident scenarios into business continuity and disaster recovery plans, including documented resilience requirements for systems (infrastructure, operating systems, applications and data). |
| | 2.4.2 Include continuity of cyber security operations in business continuity and disaster recovery plans. |
| **3.1 Conduct awareness activities, including mandatory awareness training.** | 3.1.1 Define cyber security awareness training requirements for all staff on evolving threats, compliance obligations and secure workplace practices. |
| | 3.1.2 Require that employees and contractors complete cyber security awareness training both when onboarding and annually. |
| | 3.1.3 Conduct continuous user education on evolving threats, compliance obligations and secure workplace practices through awareness activities (outside mandatory training) that align with the defined training plan and cyber risk appetite of the organisation. |
| | 3.1.4 Conduct regular phishing simulations. |
| | 3.1.5 Define cyber security awareness training for high-risk roles, including privileged users, finance and HR teams, and executives. |
| | 3.1.6 Require that employees and contractors in high-risk roles complete cyber security awareness training both when onboarding and annually. |
| **3.2 Implement access controls to ensure only authorised access.** | 3.2.1 Create a process for granting, maintaining and revoking access for agency systems, applications and information to ensure only authorised access. |
| | 3.2.2 Remove access within a defined period of an employee's termination or when the employee no longer needs access to the information or system. |
| | 3.2.3 Conduct routine user access reviews to ensure that organisation is removing access for terminated staff, inactive accounts and privileges no longer required due to a role change. |
| | 3.2.4 Create a continuous improvement process to address access control gaps. |

| Mandatory requirement | Detailed requirement |
|---|---|
| **3.3 Patch applications (Essential Eight).** | 3.3.1 Use an automated asset discovery method at least fortnightly to help detect assets for subsequent vulnerability scanning. |
| | 3.3.2 Use a vulnerability scanner with an up-to-date vulnerability database for vulnerability scanning. |
| | 3.3.3 Use a vulnerability scanner at least daily to identify missing patches or updates for vulnerabilities in online services. |
| | 3.3.4 Use a vulnerability scanner at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products. |
| | 3.3.5 Apply patches, updates or other vendor mitigations for vulnerabilities in online services within 48 hours of release when vendors assess vulnerabilities as critical or when working exploits exist. |
| | 3.3.6 Apply patches, updates or other vendor mitigations for vulnerabilities in online services within 2 weeks of release when vendors assess vulnerabilities as non-critical and no working exploits exist. |
| | 3.3.7 Apply patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products within 2 weeks of release. |
| | 3.3.8 Remove online services that vendors no longer support. |
| | 3.3.9 Remove office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player and security products that vendors no longer support. |

| Mandatory requirement | Detailed requirement |
|---|---|
| **3.4 Patch operating systems (Essential Eight).** | 3.4.1 Use an automated method of asset discovery at least fortnightly to help detect assets for subsequent vulnerability scanning. |
| | 3.4.2 Use a vulnerability scanner with an up-to-date vulnerability database for vulnerability scanning. |
| | 3.4.3 Use a vulnerability scanner at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices. |
| | 3.4.4 Use a vulnerability scanner at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices. |
| | 3.4.5 Apply patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices within 48 hours of release when vendors assess vulnerabilities as critical or when working exploits exist. |
| | 3.4.6 Apply patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices within 2 weeks of release when vendors assess vulnerabilities as non-critical and no working exploits exist. |
| | 3.4.7 Apply patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices within one month of release. |
| | 3.4.8 Replace operating systems that vendors no longer support. |
| **3.5 Implement MFA (Essential Eight).** | 3.5.1 Use MFA to verify users to their organisation's online services that process, store or communicate their organisation's sensitive data. |
| | 3.5.2 Use MFA to verify users to third-party online services that process, store or communicate their organisation's sensitive data. |
| | 3.5.3 Where available, use MFA to verify users to third-party online services that process, store or communicate their organisation's non-sensitive data. |
| | 3.5.4 Use MFA to verify users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data. |
| | 3.5.5 Use MFA to verify users to third-party online customer services that process, store or communicate their organisation's sensitive customer data. |
| | 3.5.6 Use MFA to verify customers to online customer services that process, store or communicate sensitive customer data. |
| | 3.5.7 When using MFA, users should use something they have and something they know or something they have that is unlocked by something users know or are. |

| Mandatory requirement | Detailed requirement |
|---|---|
| **3.6 Restrict administrative privileges (Essential Eight).** | 3.6.1 Validate requests for privileged access to systems, applications and data repositories when first requested. |
| | 3.6.2 Prevent privileged accounts (except those explicitly authorised to access online services) from accessing the internet, email and web services. |
| | 3.6.3 Assign privileged users a dedicated privileged account for use solely for duties requiring privileged access. |
| | 3.6.4 Strictly limit privileged accounts explicitly authorised to access online services to only what users and services require to perform their duties. |
| | 3.6.5 Privileged users use separate privileged and unprivileged operating environments. |
| | 3.6.6 Unprivileged accounts cannot log in to privileged operating environments. |
| | 3.6.7 Privileged accounts (excluding local administrator accounts) cannot log in to unprivileged operating environments. |
| **3.7 Implement application control (Essential Eight).** | 3.7.1 Application control is put in place on workstations. |
| | 3.7.2 Apply application control to user profiles and temporary folders that operating systems, web browsers and email clients use. |
| | 3.7.3 Application control restricts execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. |
| **3.8 Securely configure Microsoft Office macro settings (Essential Eight).** | 3.8.1 Disable Microsoft Office macros for users that have no demonstrated business requirement. |
| | 3.8.2 Block Microsoft Office macros in files originating from the internet. |
| | 3.8.3 Enable Microsoft Office macro antivirus scanning. |
| | 3.8.4 Users cannot change Microsoft Office macro security settings. |
| **3.9 Implement user application hardening (Essential Eight).** | 3.9.1 Web browsers do not process Java from the internet. |
| | 3.9.2 Web browsers do not process web advertisements from the internet. |
| | 3.9.3 Disable or remove Internet Explorer 11. |
| | 3.9.4 Users cannot change web browser security settings. |

| Mandatory requirement | Detailed requirement |
|---|---|
| **3.10 Maintain backups of important data, software and configuration settings (Essential Eight).** | 3.10.1 Perform and retain backups of data, software and configuration settings with a frequency and retention timeframe in line with business continuity requirements. |
| | 3.10.2 Synchronise backups of data, software and configuration settings to enable restoration to a common point in time. |
| | 3.10.3 Retain backups of data, software and configuration settings in a secure and resilient manner. |
| | 3.10.4 Test restoration of data, applications and settings from backups to a common point in time as part of disaster recovery exercises. |
| | 3.10.5 Unprivileged accounts cannot access backups of other accounts. |
| | 3.10.6 Prevent unprivileged accounts from changing and deleting backups. |
| **3.11 Create and maintain secure configurations.** | 3.11.1 Disable or remove unneeded accounts, components, services and functions of all relevant system categories (for example, operating systems, application systems and database management systems). |
| | 3.11.2 Change default accounts or credentials for operating systems, including preconfigured accounts. |
| | 3.11.3 Only authorised users may have access to change settings for the security functions of operating systems. |
| **3.12 Define and implement data security controls.** | 3.12.1 When manually importing data to systems, scan the data for malicious and active content. |
| | 3.12.2 Encrypt data at rest using an ASD-approved cryptographic algorithm. |
| | 3.12.3 Encrypt all data communicated over network infrastructure. |
| **3.13 Implement email security controls.** | 3.13.1 Use email anti-spoofing measures, including domain-based message authentication, reporting and conformance (DMARC); Sender Policy Framework (SPF); and DomainKeys Identified Mail (DKIM). |
| | 3.13.2 Implement email content filtering to filter potentially harmful content in email bodies and attachments. |
| | 3.13.3 At the email gateway, block emails that come through an external connection where the email source address uses an internal domain or internal subdomain. |

| Mandatory requirement | Detailed requirement |
|---|---|
| **3.14 Implement controls for endpoint protection, including mobile devices.** | 3.14.1 Implement antivirus software on endpoints and servers. |
| | 3.14.2 Implement a software firewall on endpoints and servers to restrict inbound and outbound network connections to an approved set of applications and services. |
| | 3.14.3 Enforce separation of work data from personal data on staff mobile devices. |
| **3.15 Implement network security controls.** | 3.15.1 Separate networks into network zones based on the criticality of servers, services and data. |
| | 3.15.2 Change default accounts or credentials for network devices, including preconfigured accounts. |
| | 3.15.3 Prevent connections to or from known malicious endpoints using a Protective Domain Name System (PDNS) service or other security mechanism. |
| | 3.15.4 Implement network access controls to limit network traffic within and between network segments to only those required for business purposes. |

Cyber Security NSW

2/24 Rawson Place
Haymarket NSW 2000

**E:** info@cyber.nsw.gov.au
**W:** https://www.digital.nsw.gov.au/delivery/cyber-security

NSW GOVERNMENT