Transport Information and Cyber Security Policy

CP24008

1. Purpose of the policy

Transport is committed to ensuring resilient cyber security for Transport, safeguarding systems, and information from risks of compromise. This policy prescribes the principles, requirements, and accountabilities that give effect to that commitment for information security as part of Transport's overall security and is to be reviewed annually.

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.

Note: Advice concerning aspects of information security not covered by this policy can be sought from Transport Security (for physical security) and the Transport Information Management team (for information classification, storage, and destruction).

2. Who does it apply to?

This policy applies to permanent, temporary, and casual staff, staff seconded from another organisation, and contingent workers including labour hire, professional services contractors and consultants performing work for any of the following:

Department of Transport	YES
Transport for NSW	YES
NSW Trains	YES
Sydney Trains	YES
Sydney Metro	YES
State Transit Authority	YES
Transport Asset Holding Entity	YES
The Point to Point Transport Commissioner	YES
Transport Asset Manager of NSW	YES

3. Principles and requirements

3.1 Principles

This policy is supported by the following principles:

- Empower everyone with the responsibility for the appropriate protection of information and infrastructure owned by or entrusted to Transport or a third party.

- Actively promote cyber security awareness to ensure all managers, employees, contractors, and suppliers fully understand their responsibility for cyber security in their day-to-day activities.
- Regularly review cyber security threats and risks to the organisation, and the appropriateness of measures to manage them.

3.2 Requirements

To give effect to the principles in this policy, we must:

- Ensure cyber security roles and responsibilities are assigned and appropriately supported with the necessary authority, training, and resources.
- Ensure cyber security practices comply with legislative, regulatory, and contractual obligations, including the Security of Critical Infrastructure Act 2018 (Cth) and the NSW Cyber Security Policy, and are aligned with the AS/NZS ISO 27001 Information Security Management Standard.
- Ensure a systematic and practical approach to safeguard Operational Technology (OT) and Industrial Automation and Control Systems that complies with applicable Asset Management Standards and the ISA/IEC-62443 Series of Standards.
- Ensure payment card-related data security and related practices comply with the PCI-DSS Standard.
- Ensure systems are monitored on an ongoing basis and cyber security incidents are investigated and their reporting meets contractual and regulatory obligations.
- Ensure ongoing assurance and improvement on the effectiveness of cyber security controls, processes, and practices.
- Continuously identify our common risks and strengthen our defences to respond effectively to attacks.
- Create a diverse cyber culture that can adapt to increasing cyber threats, with everyone committed to strengthening our collective defence.

4. Compliance and breach

You are required to comply with this policy and its related procedures and standards. If you do not do so, this may result in disciplinary action up to and including termination of your employment or contract.

5. Accountabilities and responsibilities

Transport for NSW must comply with the responsibilities set out in the NSW Cyber Security Policy for:

- Agency Heads (e.g., Chief Executives), including the Secretary of a department.
- Chief Information Security Officers (CISOs) or Chief Cyber Security Officers (CCSOs), including Portfolio CISOs and CCSOs.
- Chief Information Officer (CIO) or Chief Operating Officer (COO)
- Information Security Manager, Cyber Security Manager or Senior Responsible Officer
- Information Management Officer
- Privacy Officer
- Internal Audit
- Risk
- Agency staff
- Third-party services providers

NOTE: While it is acknowledged that some roles in Transport may be called differently, all responsibilities, as per the NSW Cyber Security Policy, must be allocated and performed regardless of role title

Furthermore, the below roles and responsibilities have been defined for compliance with this policy.

Who	
The Secretary of Transport, and Chief Executives of Transport agencies to which the policy applies.	Ultimately accountable for cyber security within the portfolio and their agencies, ensuring program areas in the agencies align and comply with this policy and related cyber security standards, procedures, and guidelines. Ensuring Transport develops, implements, and maintains an effective cyber security strategy and plan in line with its organisational objectives and compliance obligations. The Secretary is also accountable for assigning an appropriate senior executive band officer in the agency or across the portfolio, that is accountable for cyber security of the portfolio, and with the authority to perform the duties outlined in this policy.

Chief Information Security Officer, Finance, Commercial & Technology	Accountable for cyber security of Transport and its portfolio, ensuring a cyber security strategy and plan is defined and implemented in line with this policy, and that aligns with Transports organisational objectives and compliance obligations. Ensuring support, guidance and controls are in place to help agencies in the portfolio measure and monitor compliance with this policy and any related standards, procedures, and guidelines.
All staff to whom the policy applies	Responsible for complying with the principles and requirements in this policy and any related standards, procedures, and guidelines.

6. Related/supporting material

1. NSW Cyber Security Policy
2. Transport IT Strategy
3. Transport Security Policy
4. PCI DSS Standard
5. Security of Critical Infrastructure Act

7. Document control

7.1 Superseded documents

This Policy replaces the following document:

- CP21004.1 Information Security Policy

7.2 Document history

Date & Policy No	Document owner	Approved by	Amendment notes
27 September 2024 CP24008	Group Chief Information Security Officer	Group Chief Financial Officer	Updates to purpose, requirements and accountabilities.

7.3 Feedback and help

For advice on interpreting or applying this document, please contact **infosec@transport.nsw.gov.au**.