Policy

Information Security Policy

Approved by: Chief Information Officer

Approval date: 30 January 2025

Acknowledgement of Country

In the spirit of reconciliation, TAFE NSW acknowledges Aboriginal and Torres Strait Islander peoples as the Traditional Custodians of Country throughout Australia and their connections to land, sea, and community. We pay our respect to Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

Table of contents

Policy

Section 1. Purpose

The TAFE NSW Information Security Policy ensures that TAFE NSW and its supply chain take appropriate measures to maintain confidentiality, protect integrity, and enhance availability of information assets and digital services. It aligns with the NSW Government's Cyber Security Policy and mandatory requirements for managing cyber risks.

Key Points:

Confidentiality, Integrity, and Availability: The policy emphasizes these three pillars of information security.

Supporting Innovation: Effective information security enables TAFE NSW to drive business objectives and maintain stakeholder trust.

Cultural Behaviour: The policy aims to foster a culture where all TAFE NSW community members prioritise information security.

Strategic Goals: Implementation of this policy contributes to achieving TAFE NSW's strategic objectives while managing cyber risk.

The establishment, implementation and enforcement of this policy will help TAFE NSW achieve strategic goals while meeting cyber security risk appetite as articulated by the TAFE Commission Board and by the Executive Leadership Team (ELT)

Section 2. Scope

The Information Security Policy applies to the staff, students, partners within the supply chain and all forms of information assets and digital services. This includes but is not limited to:

- Staff (permanent, temporary, casual and contractors);
- Supply Chain (where they manage or use TAFE NSW's information assets or digital services).
- Students.
- Physical locations, including off-site locations where business activities are conducted.
- Digital technologies, including cloud services, communication services, networks, servers, storage, and all end-user computing devices; and
- Information assets, including but not limited to digital and paper-based assets.

Policy

Section 3. Policy statements

3.1 Principles

3.1.1 The principles of the Information Security Policy require TAFE NSW to maintain:

a. **Confidentiality** – to uphold authorised restrictions on access to and disclosure of information assets including personal or proprietary information.
b. **Integrity** – to protect information assets and digital services against unauthorised alteration or destruction and prevent successful challenges to their authenticity.
c. **Availability** – to provide authorised users with timely and reliable access to information assets and digital services.
d. **Safety** – to provide technological solutions and services in digital ecosystems with the consideration of safety for students and staff.
e. **Compliance** – to comply with applicable legislation, regulations, Cabinet Conventions, policies, and contractual obligations requiring information assets and digital services to be available, safeguarded or lawfully used.

3.2 Goals

3.2.1 The primary goals of the Information Security Policy are to:

a. Cultivate cyber awareness among all employees and stakeholders, empowering them to make informed security decisions and actively contribute to the defence against cyber threats.
b. Implement effective cyber security planning and governance to ensure appropriate oversight and visibility of cyber risk across the environment.
c. Continuously improve our resilience to cyber events, including our ability to rapidly detect, respond to and mitigate cyber incidents.
d. Establish a 'Zero Trust' architecture model and uplift our capability for managing secure and trusted access to our systems, information and learning resources through ways of working changes.
e. Maintain and improve our system security framework, safeguarding our digital assets from current and emerging threats. Continuously monitor the threat landscape, assess vulnerabilities, and implement proactive measures to mitigate risks effectively.
f. Maintain our alignment with Cyber Security NSW and other regulatory obligations for cyber security.

3.3 Objectives

3.3.1 TAFE NSW leadership has endorsed the following Security Objectives which forms the foundation for security investments and sets forth the direction for establishing the ISMS:

a. Fostering a culture of cyber security accountability & awareness.
b. Maturing cyber security governance.

c. Protection of our systems and data from current and emerging threats.
d. Alignment with NSW Government policies, cyber security frameworks, and industry best practices.

3.3.2 TAFE NSW shall monitor the activities undertaken to achieve above objectives through periodic updates to relevant governance forums.

3.4 Information Security Management System (ISMS)

3.4.1 TAFE NSW must implement an ISMS that is based on a comprehensive assessment of risks to information assets and digital services; appropriately address all identified risks in accordance with:

a. TAFE NSW Enterprise Risk Management Policy aligned with ISO 31000:2018.
b. NSW Cyber Security Policy;
c. TAFE NSW Business Resilience Policy;
d. TAFE NSW Data Governance Policy;
e. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
f. Payment Card Industry Data Security Standard (PCI DSS); and
g. Right Fit for Risk Cyber Security Accreditation (RFFR).

3.4.2 This includes controlled implementation of TAFE NSW's externally provided processes, products or services that are relevant to the information security management system.

3.4.3 TAFE NSW shall evaluate the information security performance and the effectiveness of the information security management system at least annually.

3.5 Information Security Management System Controls

3.5.1 TAFE NSW must establish, implement, maintain and continually improve an information security management system, including the processes needs and their interactions encompassing control measures that address the risks associated with the following:

a. Organisational Controls
b. People Controls
c. Physical Controls and
d. Technological Controls

3.5.2 Implementing cybersecurity concepts –

a. Identify
b. Protect
c. Detect
d. Respond
e. Recover

3.5.3 Across Security domains – Governance and Ecosystem, Protection, Defence and Resilience.

3.6 Security Culture

3.6.1 TAFE NSW promotes a security culture that protects and generates value by:

a. Supporting senior management to demonstrate leadership in information security management as it applies to their areas of responsibility.
b. Directing and supporting staff to contribute to the effectiveness of the information security management system.
c. Ensuring the information security policy supports and aligns to the strategic direction of TAFE NSW.
d. Ensuring the information security management system requirements are embedded into necessary and appropriate TAFE NSW processes.
e. Ensuring the resources necessary and appropriate for the effective execution of the information security management system, are available.
f. Conforming to the requirements of the ISMS and communicating the importance of effective information security management; and
g. Monitoring the outcomes of the information security management system and promoting continual improvement.

Section 4. Responsibilities

Governance	Details
Chief Information Officer (CIO)	The Chief Information Officer is the approver for this Policy
Executive Leadership Team (ELT)	The ELT is responsible for promoting a security culture and be informed of issues likely to impact TAFE NSW business operations and education Services
Chief Information Security Officer (CISO)	- Assisting the CIO in defining security strategies and implementing a cyber-security plan to protect TAFE NSW information assets and digital systems - To advise the management on emerging threats, approve and maintain written directions to support this policy - Implement policies, procedures, practices and tools to ensure compliance with this policy - Lead investigation, response and reporting on cyber security events - Represent TAFE NSW on whole-of-government collaboration, advisory or steering groups established by Cyber Security NSW - Establish training and awareness programs to increase employees' cyber security capability - Implement and maintain an effective cyber security program including via effective collaboration and/or governance forums - Collaborating with privacy, audit, information management and risk officers to protect TAFE NSW information and systems

Policy

Governance	Details
The security team, and owners/managers of projects, risks, business processes, information, solution, and Platforms	The owners and managers (both business and technology) are responsible for applying risk assessment and management processes within the Information Security Management System
Solution architects and platform managers	Solution architects and platform managers are responsible for implementing the appropriate security controls within the Information Security Management System
TAFE NSW Staff	The staff of TAFE NSW are required to: - abide by the acceptable use of information and technology agreement, signed after induction, and refreshed annually. - implement security practices as communicated within the security awareness program, including when sharing information with external parties, including government and non - government organisations. - report suspected security violations or breaches, including suspected weaknesses and vulnerabilities
TAFE NSW Students	Students of TAFE NSW are required to abide by the acceptable use of information and technology policy communicated at enrolment

Policy

Section 5. Governance information

Governance	Details
Legislation, regulations, and standards	This policy is governed by: **5.1 Relevant legislation – NSW** • Crimes Act 1900 • Defamation Act 2005 • Government Information (Public Access) Act 2009 • Government Sector Employment Act 2013 • Health Records and Information Privacy Act 2002 • Privacy and Personal Information Protection Act 1998 • State Records Act 1998 • Workplace Surveillance Act 2005 **5.2 Relevant legislation - Commonwealth** • Australian Copyright Act, 1968 • Telecommunications Act 1997 • Telecommunications (Interception and Access) Act 1979 • Spam Act 2003 • Privacy Act 1988 • Intelligence Services Act 2001 • Australian Security Intelligence Organisation Act 1979 • Commonwealth Cybercrime Act 2001 • National Security Information Act 2004 • The Security of Critical Infrastructure Act 2018 **5.3 NSW Government policies and directives** • Intellectual Property Management Framework for the NSW Public Sector • Internal Audit and Risk Management Policy for the NSW Public Sector • NSW Government Cyber Security Policy • NSW Government Incident Emergency Sub Plan • NSW Government Internet of Things (IoT) Policy • NSW Government: Information Classification, Labelling and Handling Guidelines **5.4 Australia Commonwealth Government policies and directives** • Australia's Cyber Security Strategy, 2023 • Information Security Manual
Related procedures	This policy governs the following procedures: - TAFE NSW Cyber Security Policy Reporting and Attestation Procedure; - TAFE NSW Internal Audit Procedure - TAFE NSW Information Security Management System Control Manual;

Policy

Governance	Details
Related policies	This policy is to be read together with: - TAFE NSW's Acceptable Use of Information & Technology Policy - TAFE NSW's Enterprise Risk Management Policy - TAFE NSW's Cloud Computing and Outsourcing policy - TAFE NSW's Information Management policy - TAFE NSW Enterprise Risk Management Manual; - TAFE NSW ISMS Statement of Applicability; - TAFE NSE Record Management Policy
Accountable Officer	Chief Information Officer
Responsible Officer	Chief Information Security Officer
Content Manager number	TAFE19/9682
Next review date	30/01/2028

Section 6. Document history

No.	Effective	Approved by	Amendment
1	1 January 2018	Chief Information Officer	Initial Draft
2	02 Mar 2020	Chief Information Officer	Updated sections to align the policy with NSW Government Cyber Security Policy Objectives.
3	21 Mar 2022	Chief Information Officer	Alignment with revised Ways of Working Policy Template, Updated References, and alignment with FOCUS approved Security Objectives.
4	20 June 2023	Chief Information Officer	Added "Payment Card Industry Data Security Standard (PCI DSS)" to section 3.4
5	30 January 2025	Chief Information Officer	Updated section 3.2-3.3 to align with TAFE NSW Cyber Security Strategy. Updated section 3.4 to add requirement from RFFR Updated section 3.5 to align with ISO27001:2022 standard.