POLICY

Information Security Policy

Approved by: Chief Information Officer
Content Manager Number: Chief Information Security Officer
Approval Date: 21 March 2022
Review Date: 1 June 2023

1. Purpose

The purpose of this policy is to ensure that The New South Wales Technical and Further Education Commission (trading as TAFE NSW) and its supply chain collectively referred to as TAFE NSW here onwards implement appropriate measures to maintain confidentiality, protect the integrity and improve the availability of TAFE NSW's information assets and digital services.

This policy aligns with the NSW Government's Cyber Security Policy and helps meet mandatory requirements to which all NSW Government Agencies must adhere, to ensure cyber security risks to their information and systems are managed.

TAFE NSW recognises that effective information security will help and support TAFE NSW in delivering the innovation required to drive business objectives and maintain the trust of key stakeholders while complying with applicable regulatory and legal requirements.

The Information Security Policy help develop a culture that will drive behaviours of all members of the TAFE NSW community to maintain confidentiality, protect the integrity and improve the availability of our information assets and digital services.

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).

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:

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

Disclaimer: Printed copies of this document are regarded as uncontrolled. Please check http://staff.tafensw.edu.au to ensure this is the latest version.

3. Policy

3.1 Principles

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

The primary goals of the Information Security Policy are to:

a. **Maintain Trust** – Customer at the heart of everything, Maintain Trust of our students, staff, and stakeholders.

b. **Manage Cyber Threats** – Identify assets of value and assess cyber security threats, Manage cyber security posture through prioritised mitigation delivery.

c. **Secure by Design** – Develop, manage, and maintain applications by identifying and building security controls throughout the lifecycle.

d. **Seamless Security** – Focus on usability to simplify and embed security controls to ensure controls are seamless, easy to use and understand.

e. **Monitor, Detect, Respond** – Reduce impactful cyber security events by practising and improving monitoring, response and recovery process.

3.3 Objectives

TAFE NSW leadership has endorsed the following Security Objectives which forms the foundation for security investments and sets forth the direction for establishing the Information Security Management System (ISMS):

a. Ensure that TAFE NSW's ICT systems and information held in our systems are protected against threats

b. Develop policy and provide training and awareness to mitigate and minimise system and application vulnerabilities

c. Provide assurance that sensitive information is protected and stored appropriately and protected from threats

d. Monitor, respond and investigate security threats to minimise impact to confidentiality, integrity, and availability

3.4 Information Security Management System (ISMS)

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 Risk Management Policy;
b. NSW Government Cyber Security Policy;
c. TAFE NSW Business Resilience Framework;
d. TAFE NSW ICT Governance Framework; and
e. AS ISO/IEC 27001:2015 Information technology - Security techniques - Information security management systems – Requirements

3.5 Information Security Management System Controls

TAFE NSW must implement control measures that address the risks associated with the following:

a. Governance;
b. Information security systems independent review;
c. Information classification, labelling and handling;
d. Controlling access to information systems;
e. Protect the integrity of information and documents while processing, handling & storing
f. Acquisition, development and maintenance of information technology and services;
g. Controlling relationships with external parties;
h. Business processes and continuity;
i. Security incident management;
j. Collaboration and information sharing; and
k. Training and awareness

3.6 Security Culture

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.

4. Responsibilities

Position	Responsibility
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)	a) Assisting the CIO in defining security strategies and implementing a cyber-security plan to protect TAFE NSW information assets and digital systems b) To advise the management on emerging threats, approve and maintain written directions to support this policy c) Implement policies, procedures, practices and tools to ensure compliance with this policy d) Lead investigation, response and reporting on cyber security events e) Represent TAFE NSW on whole-of-government collaboration, advisory or steering groups established by Cyber Security NSW f) Establish training and awareness programs to increase employees' cyber security capability g) Implement and maintain an effective cyber security program including via effective collaboration and/or governance forums h) Collaborating with privacy, audit, information management and risk officers to protect TAFE NSW information and systems
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: a) abide by the acceptable use of information and technology agreement, signed after induction, and refreshed annually. b) implement security practices as communicated within the security awareness program, including when sharing information with external parties, including government and non - government organisations. c) 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 agreement communicated at enrolment

5. Related documents

This policy should be read in conjunction with the following related documents:

- 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
- NSW Government's NSW Cyber Security Policy
- NSW Government's Cloud Strategy and Policy
- NSW Government's Information Classification Labelling and Handling Guidelines

This policy is guided and supported by the following related documents:

- TAFE NSW Code of Conduct and Ethical Practices
- Privacy and Personal Information Protection Act 1998 (NSW)
- Standards for Registered Training Organisations (RTOs) 2015 (ASQA)
- Australian Qualifications Framework (ASQA)
- Children and Young Persons (Care and Protection) Act 1998 (NSW)
- AS ISO/IEC 27001:2015

The implementation details of this policy can be found in the following documents:

- TAFE NSW Information Security Management System Controls Manual

6. Contacts

Accountable Officer	Chief Information Officer
Responsible Officer	Chief Information Security Officer

7. Document History

No	Effective	Approved by	Amendment
1	1 January 2018	Chief Information Officer	NA
2	02 Mar 2020		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.

Disclaimer: Printed copies of this document are regarded as uncontrolled. Please check http://staff.tafensw.edu.au to ensure this is the latest version.