POLICY

Information Security Policy

Written Direction No. WDICT18201
Approved by: Chief Information Officer
Approval Date: 18 April 2020
Effective From: 1 June 2020

1. Introduction

TAFE NSW is the NSW Government's public provider of Vocational Education and Training (VET).

The New South Wales Technical and Further Education Commission (trading as TAFE NSW), was established as a statutory agency by the Technical and Further Education Commission Act 1990 (NSW).
Under this legislation, TAFE NSW performs a number of functions, including:

- Providing technical and further education services to meet the skills needs of individuals and the workforce, in ways that recognise the changing nature of workplaces and the need for new skills and retraining
- Consulting with industry and the community to ensure technical and further education services are relevant to industry, business, students and other groups
- Providing educationally or vocationally disadvantaged groups with access to technical and further education and other specialised services
- Providing students with the maximum opportunity to progress to further education and training by linking their studies to further TAFE NSW courses or those of other education and training providers.

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 deliver 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 integrity and improve availability (CIA) 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. Purpose

The purpose of this policy is to ensure that TAFE NSW and it's supply chain implement appropriate measures to maintain confidentiality, protect integrity and improve availability of TAFE NSW's information assets and digital services.

3. 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 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.

4. Policy

The primary objective of the Information Security Policy is to protect:

- **Confidentiality** – to uphold authorised restrictions on access to and disclosure of information assets including personal or proprietary information.
- **Integrity** – to protect information assets and digital services against unauthorised alteration or destruction and prevent successful challenges to their authenticity.
- **Availability** – to provide authorised users with timely and reliable access to information assets and digital services.
- **Safety** – to provision technological solution and services in digital eco systems with the consideration of safety for students and staff.
- **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.

4.1 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:

I. TAFE NSW Risk Management Policy;
II. NSW Government Cyber Security Policy;
III. TAFE NSW Business Resilience Framework;
IV. TAFE NSW ICT Governance Framework; and
V. AS ISO/IEC 27001:2015 Information technology - Security techniques - Information security management systems – Requirements;

4.2 Information Security Management System Controls

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

- Governance;
- Information security systems independent review;
- Information classification, labelling and handling;
- Controlling access to information systems;
- Protect the integrity of information and documents while processing, handling & storing
- Acquisition, development and maintenance of information technology and services;
- Controlling relationships with external parties;
- Business processes and continuity;
- Security incident management;

- Collaboration and information sharing; and
- Training and awareness

4.4 Security Culture

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

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

5. 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)	• 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
Project, risk, business process, information, solution and platform owners and managers	Project, risk, business process, information, solution, platform 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	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 agreement communicated at enrolment

6. Definitions

Term	Meaning
Accredited Third Party	An independent certification body recognised by Standards Australia.
Digital services	A service (i.e. not goods) delivered via the internet, or an electronic network. Supply is essentially automated, or involves only minimal human intervention.
Information asset	An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets may be physical or electronic.
Information classification	The process of assigning an appropriate level of classification to an information asset to ensure it receives an adequate level of protection.

7. Related Documents

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

- 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 Policy'
- NSW Government's 'Classification Labelling and Handling Guidelines'

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

- TAFE NSW RISK APPETITE STATEMENT 2019
- 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 27001:2015x

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

- TAFE NSW Information Security Management System Controls Manual
- TAFE NSW Acceptable Use of Information and Technology Guideline

8. Contacts

Accountable Officer	Chief Information Officer
WD Officer	Chief Information Security Officer

9. Document Information and Review

This policy document will be reviewed at least every three years.

Record No. PROJ18/828

Review Due: 1 JUNE 2023

Approval History

No.	Effective	Approved by	Amendment
1	1 January 2018	Chief Information Officer	NA
2	02 Mar 2020	Chief Information Officer	Updated sections to align the policy with NSW Government Cyber Security Policy Objectives.