



PP45 – IT Systems and Security Policy

Section: VET Workforce and Governance

Standard: Outcome Standard 4.3

1. Purpose

This policy outlines the measures taken by Austra College to manage and safeguard its information technology (IT) systems and data. It ensures that digital infrastructure supports the secure delivery of training and assessment, protects sensitive information, and complies with the regulatory obligations under Outcome Standard 4.3.

2. Scope

Applies to all Austra College staff, students, third parties, and contractors who access or manage Austra College's IT systems, including Student Management Systems (SMS), Learning Management Systems (LMS), SharePoint, email services, and assessment storage platforms.

3. Definitions

Term	Definition
IT Systems	Infrastructure used to store and process data (e.g., SMS, LMS, email, cloud platforms).
Cybersecurity	Measures taken to protect IT systems from unauthorised access or attacks.
LMS	Learning Management System used for delivering and tracking training activities.
SMS	Student Management System used for storing student enrolment, assessment, and certification records.

4. Legislative and Regulatory Reference

- ✚ Standards for RTOs 2025 – Outcome Standard 4.3
- ✚ Privacy Act 1988 (Cth)
- ✚ Australian Cyber Security Centre (ACSC) Guidelines
- ✚ National VET Data Policy
- ✚ Notifiable Data Breaches Scheme

5. Policy Statement

Austra College is committed to:

- ✚ Ensuring the availability, integrity, and confidentiality of its IT systems and student data.

Version	V2.1	Document Name	Policy and Procedure
CRICOS Code.	03187D	RTO Name	Austra College
RTO Code.	40336	Page number	239



- ✚ Implementing preventative measures to protect data from unauthorised access, breaches, and loss.
- ✚ Providing staff with training and guidelines on secure IT use.
- ✚ Ensuring secure backup and retention of electronic records.

6. Responsibilities

Role	Responsibility
RTO Manager	Oversees IT system policies and audits.
IT Support / Contractor	Implements technical security controls and performs regular maintenance.
Admin and Trainers	Ensure secure handling of student data within SMS and LMS.
All Staff	Adhere to security protocols and report breaches.

7. IT Security Practices

- ✚ All systems require secure logins with role-based access control.
- ✚ Passwords must be changed every 90 days and stored securely.
- ✚ Staff must not share login credentials.
- ✚ Two-factor authentication is enabled for systems holding sensitive data.
- ✚ Antivirus and firewall protections are installed and regularly updated.

8. Backup and Recovery

- ✚ Weekly data backups of SMS, LMS, and SharePoint.
- ✚ Backup copies stored in encrypted cloud storage and secure local drives.
- ✚ Monthly backup integrity tests.
- ✚ Disaster Recovery Plan tested annually.

9. Incident Response

If a breach or cyber incident occurs:

1. Incident must be reported to the RTO Manager within 24 hours.
2. Investigation conducted with IT personnel.
3. Report logged in the IT Incident Register.
4. Notify affected stakeholders where required under the Notifiable Data Breaches Scheme.
5. Preventative measures documented in the Continuous Improvement Register.

Version	V2.1	Document Name	Policy and Procedure
CRICOS Code.	03187D	RTO Name	Austra College
RTO Code.	40336	Page number	240



10. Acceptable Use Guidelines

- ✚ Staff and students must only use Austra College IT systems for authorised educational and administrative purposes.
- ✚ Prohibited uses include unauthorised software installation, data tampering, and use of systems for personal business or inappropriate content.
- ✚ Breaches of acceptable use may result in disciplinary action.

11. Procedure – Step-by-Step

Step	Action	Responsible Person
1	Provide system access based on user role and function.	RTO Manager/Admin Officer
2	Train staff on IT use, data security, and privacy.	RTO Manager
3	Perform weekly data backups and secure storage.	Admin Officer
4	Conduct quarterly audits of SMS, LMS, and file access.	RTO Manager
5	Respond to data breaches using incident protocol.	RTO Manager/ Admin Officer
6	Log all IT incidents and improvements in registers.	RTO Manager
7	Review IT systems annually for risks and improvement.	CEO/ RTO Manager

12. Related Documents

- ✚ PP34 - Data Privacy and Record Keeping Policy
- ✚ PP44 - Workplace Health and Safety Policy (includes workstation safety)
- ✚ PP43 - Critical Incident Management Policy
- ✚ IT Incident Register
- ✚ Staff Induction Manual
- ✚ Acceptable Use Agreement

Version	V2.1	Document Name	Policy and Procedure
CRICOS Code.	03187D	RTO Name	Austra College
RTO Code.	40336	Page number	241



13. Flow chart

IT Systems and Security Process



Version	V2.1	Document Name	Policy and Procedure
CRICOS Code.	03187D	RTO Name	Austra College
RTO Code.	40336	Page number	242