



Cybersecurity and Secure Electronic Assessment Policy

Version 1.1 | Date: March 2026 Review Date March 2027

Approved by: RTO Manager and Compliance Consultant

1. Purpose

This policy outlines VASS College's commitment to ensuring the **confidentiality, integrity, and availability** of all electronic assessments, in compliance with the **Standards for RTOs 2025 (SRTOs)** and the **Skills First 2024–25 V3.0 Contract**.

It sets measures to:

- Protect assessment systems and student data from cybersecurity threats.
- Maintain the authenticity and integrity of student work.
- Ensure secure storage, retention, and disposal of assessment data.

(References: SRTOs 2025 Clauses 1.8, 1.9, 3.1, 3.3; Skills First V3.0 Schedule 1 – Clause 4.2, Clause 7.5)

2. Scope

This policy applies to:

- All **staff, contractors, and third-party providers** involved in the creation, delivery, assessment, storage, and management of electronic assessments at VASS College.
 - All **students** undertaking electronic assessments.
-

2A. Definitions

Cyber Incident – An event that jeopardises the confidentiality, integrity, or availability of assessment systems or student data, including unauthorised access, data breach, or ransomware attack. *(Skills First V3.0 – Clause 7.5)*

Electronic Assessment – Any assessment conducted, stored, or transmitted via digital or online systems.

Multi-Factor Authentication (MFA) – A security process requiring two or more verification methods (e.g., password + one-time code).

Assessment Data – All digital records relating to student assessments, including submissions, feedback, results, and related communications.

Third-Party Provider – Any external organisation providing learning, assessment, or data

hosting services on behalf of VASS College.

Plagiarism Detection Tools – Software used to identify unoriginal content in student submissions.

3. Cybersecurity Measures

VASS College will:

- **Use secure platforms:** Only approved Learning Management Systems (LMS) and assessment tools with encryption and MFA. (*SRTOs 1.8, Skills First 4.2*)
 - **Apply access controls:** Role-based permissions to ensure only authorised personnel access sensitive data.
 - **Update and patch systems** regularly.
 - **Encrypt data** in storage and during transmission.
 - **Maintain data backups** with secure off-site storage and documented disaster recovery plans.
 - **Conduct third-party due diligence:** Security checks and agreements for all providers handling assessment data. (*Skills First 4.2, 7.5*)
 - **Report cyber incidents** to Skills Victoria within **72 hours** of detection, and to ASQA if required. (*Skills First 7.5*)
 - **Follow data retention & disposal:** Retain assessment records as per Skills First (minimum 2 years) and securely destroy when no longer required.
-

4. Ensuring Assessment Authenticity

VASS College adopts the following:

- **Identity verification** via MFA-enabled LMS login or secure video verification. (*SRTOs 1.8*)
 - **Plagiarism detection** and AI-writing detection tools.
 - **Randomised question banks** to minimise collusion.
 - **Assessment declarations** signed by students confirming originality.
 - **Proctored or oral verification** for high-risk assessments.
-

5. Staff Responsibilities

- Complete **cybersecurity and assessment integrity training** annually. (*SRTOs 1.9*)
- Report cyber incidents within 2 hours of detection to the RTO Manager. (*Skills First 7.5*)

- Monitor for unauthorised access or breaches.
- Participate in **regular security audits** and system testing.

6. Student Responsibilities

- Use only authorised systems and platforms for assessments.
- Keep login credentials confidential.
- Report suspicious activity immediately.
- Cooperate in verification processes (e.g., interviews, proctoring).

7. Review and Continuous Improvement

- Policy reviewed **annually** or following a cyber incident.
- Updates reflect emerging threats, new technologies, and changes in SRTOs or Skills First requirements.

Appendix – Compliance Mapping Table

Policy Section	SRTOs 2025 Clause(s)	Skills First V3.0 Clause(s)	Compliance Notes
1. Purpose	1.8, 1.9, 3.1, 3.3	Sch 1: 4.2, 7.5	Links policy intent to compliance obligations for secure assessments and data protection.
2. Scope	1.8	4.2	Ensures all parties handling assessments are covered.
2A. Definitions	1.8	7.5	Provides clarity for compliance interpretation.
3. Cybersecurity Measures	1.8, 1.9, 8.1	4.2, 7.5	Includes MFA, encryption, third-party due diligence, and breach reporting.
4. Ensuring Assessment Authenticity	1.8, 1.9	4.2	Covers identity checks, plagiarism detection, and secure assessment design.
5. Staff Responsibilities	1.9	7.5	Aligns with Skills First incident reporting and SRTOs staff competence requirements.



Policy Section	SRTOs 2025 Clause(s)	Skills First V3.0 Clause(s)	Compliance Notes
6. Student Responsibilities	1.8	4.2	Ensures student compliance with integrity and security requirements.
7. Review & Continuous Improvement	1.8, 3.3	4.2, 7.5	Commits to annual review and post-incident updates.

Approved by: Signature: Leila Alloush CEO

Date: 7/03/2026