JTI Information System and Cyber Security Policy

A. Purpose

This policy sets out Job Training Institute’s (JTI) commitment to safeguarding all information systems, student/staff data, and digital services against unauthorized access, misuse, disclosure, modification, or loss.

It ensures compliance with ASQA standards, ESOS/CRICOS obligations, the National Code 2018, and relevant privacy and security legislation.

B. Scope

This policy applies to:

- All JTI staff, contractors, volunteers, and agents.

- All students (domestic and CRICOS/overseas).

- All IT systems, devices, applications, learning platforms (Moodle, Vettrak, PRISMS access), email, cloud services, and data repositories.

C. Key Principles

JTI will:

1. Protect confidentiality, integrity, and availability of all digital and paper-based records.

2. Apply role-based access controls and least-privilege principles.

3. Ensure data is collected, used, stored, and disclosed in line with the Privacy Act 1988, APPs, and ESOS requirements.

4. Maintain business continuity and disaster recovery capability.

5. Train staff and students in responsible use of IT systems, including cyber awareness.

6. Report and remediate data breaches in compliance with the Notifiable Data Breach Scheme.

D. Responsibilities

- CEO & General Manager: Ensure resources and compliance with standards.

- Compliance Manager: Monitor legislative/ASQA/ESOS alignment, report breaches.

- IT Manager/System Administrators: Secure systems, patching, backups, monitoring.

- Trainers/Assessors/Staff: Follow ICT use guidelines, report incidents immediately.

- Students: Use systems responsibly, protect login credentials, report suspicious activity.

E. Procedures

1. System Access & Authentication

- Unique user IDs and strong passwords for all systems.

- Multi-Factor Authentication (MFA) for sensitive systems (e.g., PRISMS, Vettrak).

- Access revoked within 24 hrs of staff/student exit.

2. Data Security

- Encryption of sensitive data in transit (TLS/SSL) and at rest where applicable.

- Regular secure backups stored offsite/cloud.

- Clean desk and secure storage practices for paper files.

3. Cybersecurity Controls

- Anti-virus/endpoint protection on all devices.

- Firewalls and network segmentation for campus systems.

- Patch management within 30 days of vendor release.

- Annual penetration testing and vulnerability assessments.

4. Incident Response & Breach Notification

- Immediate containment of breach (disable access, isolate systems).

- Assessment within 30 days of the incident.

- Notification to OAIC, ASQA, DOE/DHA (if CRICOS-related), and affected parties where required.

- Root-cause analysis and corrective action logged in the Continuous Improvement Register.

5. Training & Awareness

- Cybersecurity induction for all staff and students.

- Annual refresher on phishing, password safety, privacy obligations.

- Targeted training for PRISMS users and data handlers.

6. Third-Party & Cloud Services

- Contracts include data protection and compliance clauses.

- Providers must meet Australian privacy law and cybersecurity requirements.

- Regular review of security certifications.

F. Recordkeeping & Retention

- ICT logs, access records, breach reports → retained for 7 years.

- Student/HR digital records → retained in line with Schedule 5 of Standards for RTOs (30 years for certification) and ESOS/CRICOS obligations.

G. Continuous Improvement

- Policy reviewed annually or after major incident.

- Outcomes of reviews fed into Management Review Meetings.

- Improvements tracked in Continuous Improvement Register.

H. Related Documents

- Privacy, Confidentiality & Recordkeeping Policy

- Critical Incident Policy

- Complaints & Appeals Policy

- WHS Policy

- Student Code of Conduct

- Staff IT Acceptable Use Procedure