



TIIS
THE INSTITUTE
OF INTERNATIONAL
STUDIES



IT Resources and Learning Systems Policy

The Institute of International Studies Pty Ltd

Sydney Campus: 13-15 Smail St, Ultimo NSW 2007

Melbourne Campus: Level 1, 112 Newquay Promenade, Docklands, VIC 3008

Tel: (+61 2) 8098 0702 | Email: info@tiis.edu.au

Policy No:

Version No: 1.0

Contents

1. Purpose.....	3
2. Scope.....	3
3. Policy Objectives	3
4. Key Principles	3
4.1 Reliability and Accessibility.....	3
4.2 Security and Data Integrity	3
4.3 Support and Maintenance.....	3
4.4 Innovation and Pedagogical Support	4
4.5 Risk and Continuity Management.....	4
5. Responsibilities	4
6. Compliance with HESF Standards	4
7. IT System Provision and Support.....	4
7.1 Learning Management System (LMS)	4
7.2 Student and Staff Portals	4
7.3 Digital Library Access	5
7.4 Software and Licensing.....	5
8. Cybersecurity.....	5
9. Monitoring and Review.....	5
10. Policy Review	5
11. Related Policies and Procedures.....	5
Version History	6

1. Purpose

The purpose of this policy is to ensure that TIIS provides and maintains secure, reliable, and effective IT resources and learning systems that support high-quality teaching, learning, research, and administration. The policy ensures alignment with the **Higher Education Standards Framework (Threshold Standards) 2021**, particularly:

- **Standard 3.3:** Learning Resources and Educational Support
- **Standard 6.2:** Corporate Monitoring and Accountability
- **Standard 7.3:** Information Management

2. Scope

This policy applies to:

- All **students, academic, and professional staff** at TIIS
- **Onshore, offshore, and third-party** delivery sites
- All institutional IT systems including the **Learning Management System (LMS), student information system, email systems, library platforms, and cybersecurity systems**

3. Policy Objectives

- Ensure **availability, accessibility, and integrity** of digital learning resources and IT infrastructure.
- Promote safe and ethical use of IT and learning systems by staff and students.
- Support **digital literacy**, academic integrity, and pedagogical innovation.
- Protect the confidentiality, integrity, and availability of institutional data.
- Ensure **business continuity** and rapid recovery in case of IT disruptions or cyber incidents.

4. Key Principles

4.1 Reliability and Accessibility

- All students and staff will have **timely and equitable access** to required digital learning systems and resources.
- IT systems must support **online, hybrid, and face-to-face** delivery equally.

4.2 Security and Data Integrity

- All user data and institutional information must be stored, transmitted, and processed in compliance with **Australian privacy legislation, HESF 7.3, and internal policies**.
- Access control, encryption, and role-based permissions must be applied.

4.3 Support and Maintenance

- Regular **system maintenance, updates, and patching** must occur with minimal service disruption.
- A responsive **IT help desk** will be maintained with documented SLAs (service-level agreements).

4.4 Innovation and Pedagogical Support

- TIIS supports the **adoption of educational technologies** that improve teaching quality and student engagement (e.g., AI tools, LMS analytics, digital assessment platforms).

4.5 Risk and Continuity Management

- IT and learning systems must be included in the Business Continuity Plan and Critical Incident Management Plan.
- Backups of all critical systems must be performed regularly and tested periodically.

5. Responsibilities

Role	Responsibilities
Director of IT and Digital Services	Oversee infrastructure, policy enforcement, and system development
Registrar	Manage LMS configuration, access, content availability
Academic Dean	Ensure academic systems align with curriculum and pedagogical needs
Deputy CEO (Compliance and Quality Assurance)	Monitor system performance, security, and compliance
Teaching Staff	Use LMS tools appropriately, upload materials, ensure accessibility
Students	Engage with learning systems, follow usage policies, report issues

6. Compliance with HESF Standards

HESF Clause	Policy Application
3.3.1	Ensures digital learning systems support effective student engagement and access to resources
6.2.1	Enables regular monitoring and reporting on IT system performance and improvements
7.3.1 – 7.3.3	Ensures secure, accurate, and compliant information and records management

7. IT System Provision and Support

7.1 Learning Management System (LMS)

- The LMS must be accessible 24/7 with >98% uptime annually.
- Each unit must be set up in the LMS **2 weeks before trimester start** with:
 - Unit outlines
 - Weekly topics and learning materials
 - Assessment details and rubrics
 - Discussion boards and submission portals

7.2 Student and Staff Portals

- Students and staff must have secure, role-based access to:

- Email systems
- Academic calendars
- Grades and enrolment information
- Assessment results

7.3 Digital Library Access

- Systems must provide access to licensed databases (e.g., ProQuest, EBSCO).
- Integration with the LMS must allow seamless access.

7.4 Software and Licensing

- Licensed software (e.g., MS Office, Turnitin, SPSS) must be available for academic use.
- Licensing must comply with usage terms and be monitored for expiry and renewal.

8. Cybersecurity

- TIIS Data & Cybersecurity Policy governs:
 - User authentication and password policies
 - Firewalls, anti-virus, and intrusion detection systems
 - Data encryption and regular vulnerability assessments

9. Monitoring and Review

Evidence Type	Purpose
System Uptime Reports	Track availability and outages of LMS and IT systems
LMS Analytics	Monitor student usage, engagement, and content access trends
Help Desk Logs	Record number, type, and resolution times of support tickets
Annual IT Audit Reports	Evaluate compliance, security controls, and infrastructure status
Stakeholder Feedback Surveys	Assess satisfaction with IT support and system usability
Digital Literacy Training Logs	Track staff/student participation in tech training and CPD

10. Policy Review

This policy will be reviewed **biennially** by the Executive Management Team in consultation with the Academic Board and IT Governance Subcommittee. Reviews will consider:

- User satisfaction
- System performance metrics
- Technological advancements
- HESF and regulatory changes

11. Related Policies and Procedures

- Learning and Teaching Plan
- Digital Curriculum and Online Learning Policy

- Cybersecurity Integrity Policy
- Student Support and Wellbeing Policy
- Privacy and Data Management Policy
- Business Continuity and Disaster Recovery Plan

Version History

Version:	1.0
Creation Date	01 October 2025
Authored by	CEO
Endorsement Body	Academic Board
Endorsement Date	08 April 2026
Approved By	Board of Directors
Approved Date	
Implementation Date	
Duration	2 Years from Approval Date

Version	Approved by	Approval Date	Details
1.0	Board of Directors	8 April 2026	Minor changes

*****END OF POLICY and PROCEDURE*****