Crisis Management Policy and Procedure

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: BOD-16 Version No: 1.0

ABN: 37 605 540 547 | CRICOS Provider Code: 03705J | Provider No: PRV14085

Contents

Purpose

This Crisis Management Plan (CMP) outlines the structured, institution-wide approach for preparing for, responding to, and recovering from crises that could affect the health, safety, reputation, or continuity of operations at TIIS. It supports legal, academic, and operational compliance with TEQSA, the ESOS Act 2000, and the Higher Education Standards Framework (Threshold Standards) 2021.

Objectives

- Ensure the safety and wellbeing of students, staff, and stakeholders
- Minimise disruption to academic and business operations
- Provide coordinated and transparent communication to all stakeholders
- Ensure institutional compliance with legal and regulatory requirements
- Facilitate timely recovery and continuous improvement

Scope

This policy applies to:

- All TIIS operations and locations (onshore and offshore, including online delivery)
- All staff, students (domestic and international), contractors, and visitors
- All crisis events including, but not limited to:
    - Natural disasters
    - Public health emergencies (e.g., pandemics)
    - Cybersecurity incidents
    - Reputational crises
    - Violent acts or threats
    - Institutional registration suspension or closure

Definitions

- **Crisis:** An unplanned event that causes, or has the potential to cause, serious harm to people, disrupts academic or business operations, or damages the reputation and legal standing of the institution.
- **Critical Incident:** A traumatic or sudden event (e.g. student death, violence, major accident) requiring immediate and coordinated institutional response.
- **Crisis Management Team (CMT):** A group of key TIIS personnel assigned responsibility for managing and coordinating the response to a crisis.
- **Business Continuity:** A plan to ensure essential services can continue or resume quickly following a disruption.
- **Stakeholders:** Students, staff, regulators, partners, families, agents, and community members impacted by the incident.

Policy Statement

TIIS recognises the importance of a proactive and coordinated response to any situation that may threaten its ability to operate, meet its academic obligations, or safeguard its stakeholders. This Crisis Management Policy establishes clear protocols to:

- Protect student and staff wellbeing

- Ensure continuity of academic delivery
- Maintain compliance with HESF and ESOS obligations
- Preserve institutional reputation and operations
- Communicate clearly and consistently with stakeholders

Responsibilities

Role	Responsibilities
Board of Directors	Governance oversight; ensures executive crisis plans exist and are periodically reviewed
CEO (Crisis Controller)	Leads the crisis response; activates Crisis Management Team (CMT); liaises with regulators
Crisis Management Team (CMT)	Executes the crisis response plan; manages communications, student support, operations, and recovery
Academic Dean	Ensures academic continuity, including course delivery, assessment, and student communication
Registrar	Coordinates international student records and compliance reporting (PRISMS, ESOS obligations)
Student Support Manager	Provides wellbeing services and liaison for affected students
Marketing Manager	Manages internal and external messaging to students, staff, media, stakeholders and partners
IT Manager	Responds to cyber-related incidents and ensures digital continuity
All Staff	Follow instructions, report incidents promptly, and support recovery activities as directed

Crisis Management Procedure

Stage 1: Preparation

- Maintain an up-to-date **TIIS Crisis Management Plan** and **Emergency Contacts Register**
- Conduct **annual risk assessments** to determine readiness for high-risk scenarios (pandemic, system failure, etc.)
- Run **simulated crisis drills** every 12 months
- Provide **staff training** in emergency procedures, student support, and communication protocols
- Ensure **course delivery contingencies** (e.g. online learning backup) are in place

Stage 2: Identification and Notification

- Any staff or student who witnesses or becomes aware of a critical incident must report it to the CEO or designated Officer-in-Charge
- The CEO will assess severity and determine if **CMT activation** is required
- If applicable, the Registrar will notify relevant external agencies (e.g. TEQSA, Department of Home Affairs, Police)

Stage 3: Crisis Response (within 24–72 hours)

- CEO activates **Crisis Management Team (CMT)**
- Secure the site and confirm the safety of all individuals

- Provide immediate care and wellbeing support for students and staff (e.g. medical, counselling)
- Communicate:
    - Initial internal notification to staff and students
    - External regulatory bodies as required (e.g. PRISMS provider default within 24 hrs)
    - Agents, parents, and media (if applicable)
- Assess **academic and operational disruption** and implement business continuity actions

Stage 4: Recovery and Continuity

- Resume normal academic operations as soon as practical (including online or hybrid delivery)
- Provide flexible academic arrangements to students (e.g. extensions, deferrals, online access)
- Initiate insurance and financial recovery claims
- Document all decisions and actions taken during the crisis

Stage 5: Post-Crisis Review and Reporting

- Conduct a full review within 30 days of crisis resolution
- Prepare a **Crisis Debrief Report** (including outcomes, response gaps, and improvements)
- Revise the Crisis Management Plan if required
- Submit compliance report to the Board and Audit & Risk Committee
- Communicate improvements and outcomes to staff and students where appropriate

Business Continuity and Teach-Out Assurance

If the crisis results in the **suspension or loss of registration**, TIIS will:

- Notify TEQSA and activate its **Teach-Out and Provider Default Plan**
- Ensure **students are offered completion pathways**, either through:
    - Teach-out at TIIS (if feasible)
    - Articulation to a partner provider (with equivalent AQF recognition)
    - Tuition Protection Service (TPS) arrangements for international students
- Ensure ongoing access to academic records and transcripts

Related Legislation and Standards:

- **Higher Education Standards Framework (Threshold Standards) 2021:**
    - Standard 6.1 (Corporate Governance)
    - Standard 7.3 (Information Management and Recordkeeping)
    - Standard 2.1 (Facilities and Infrastructure)
    - Standard 2.3 (Wellbeing and Safety)
- **ESOS Act 2000**, including:
    - National Code 2018: Standard 6 (Student Support), Standard 8 (Monitoring Course Progress), Standard 11 (Provider Default)

Review and Continuous Improvement

This policy will be:

- Reviewed **annually** by the Audit & Risk Committee
- Updated following **post-crisis reviews** or changes to relevant legislation
- Benchmarked against sector best practices in crisis and continuity management

Related Policies and Documents

- Risk Management Policy
- Teach-Out Agreements
- Student Support Policy
- Privacy and Data Protection Policy
- Academic Quality Assurance Framework
- Course Termination Policy

Version History

Plan title	**TIIS Crisis Management Policy & Procedure**
Version:	1.0
Plan Category	Strategic Plan & Associated Plans
Approved by:	Board of Directors
Authored by	CEO
Endorsement Body	EMT/AB/ARC
Creation Date	03 August 2025
Approval Date:	N/A
Next Review	August 2026 (or earlier if triggered by an incident or regulatory update)

Version	Approved by	Approval Date	Details
1.0	Board of Directors	13 August 2025	
1.1	EMT	29 May 2026	

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