

STU13 CRITICAL INCIDENT POLICY AND PROCEDURE

Department	Operations
Approval Authority	Board of Directors
Responsible Officer	Chief Executive Officer
Effective Date for use	1 October 2026
Date of next review	September 2029 (3 years from approval date)

1. Purpose

This Policy and Procedure establishes the framework for the effective management of critical incidents that may impact students, staff, visitors, or the operations of the institution. Its purpose is to ensure that TITAN HIGHER EDUCATION (TITAN/THE) responds promptly, compassionately, and in a coordinated manner to any event that poses a threat to life, health, safety, or institutional integrity.

The Policy and Procedure aims to:

- Protect the wellbeing of all members of the TITAN community.
- Minimise disruption to academic and business continuity.
- Ensure compliance with relevant legislation, regulatory standards, and the *Higher Education Standards Framework (HESF) 2021, as amended*.
- Provide clear guidance for reporting, managing, and reviewing critical incidents.
- Promote a culture of preparedness, resilience, and continuous improvement in risk management.

2. Scope

This Policy and Procedure applies to all TITAN HIGHER EDUCATION (TITAN/THE) activities and operations, including academic, administrative, research (where applicable), student support, work-integrated learning, and corporate functions.

It applies to all students, staff, contractors, volunteers, visitors, governing body members, and any other persons participating in or affected by TITAN activities, whether conducted on campus, online, during placements or work-integrated learning, at TITAN-approved off-site locations, or while representing TITAN.

This Policy and Procedure applies to:

- Critical incidents occurring on TITAN premises, during TITAN-approved activities or events, during work-integrated learning, placements, fieldwork, educational excursions, international study activities, or within online and virtual learning environments.
- Situations that may adversely affect the health, safety, wellbeing, security, or welfare of students, staff, contractors, visitors, or other members of the TITAN community.
- Critical incidents involving domestic or international students, including circumstances requiring support and reporting in accordance with the *Education Services for Overseas Students (ESOS) Act 2000 and the National Code of Practice for Providers of Education and Training to Overseas Students 2018*.
- Emergencies and incidents arising from natural disasters, severe weather events, pandemics or public health emergencies, fire, hazardous material incidents, infrastructure failures, utility outages, or other events that may threaten the continuity of TITAN operations.

- Serious behavioural incidents, including violence, threats, harassment, bullying, discrimination, sexual misconduct, criminal activity, or other conduct that presents a significant risk to individuals or the institution.
- Cybersecurity incidents, data breaches, information security events, or technology failures that may compromise the confidentiality, integrity, or availability of TITAN information, systems, or services.
- Events that may disrupt teaching, learning, research, business continuity, institutional operations, damage property or assets, compromise information or systems, or adversely affect TITAN's reputation, compliance obligations, or legal responsibilities.
- The management of all phases of critical incident management, including prevention, preparedness, response, communication, reporting, recovery, post-incident review, and continuous improvement.

This Policy and Procedure should be read in conjunction with other relevant TITAN policies and procedures, including those relating to Work Health and Safety, Student Wellbeing, Risk Management, Business Continuity, Emergency Management, Privacy, Information Security, Student Conduct, Staff Conduct, and Complaints and Appeals.

3. Policy Principles

TITAN HIGHER EDUCATION (TITAN/THE) is committed to ensuring that:

- 3.1 Critical incidents are managed promptly, effectively, and in accordance with legislative and regulatory requirements.
- 3.2 The safety, wellbeing, and support of students, staff, and visitors are prioritised at all times.
- 3.3 Communication during and after a critical incident is clear, timely, and coordinated across relevant stakeholders.
- 3.4 Appropriate documentation, reporting, and follow-up actions are undertaken to ensure accountability and continuous improvement.
- 3.5 Lessons learned from critical incidents inform ongoing risk management, policy development, and staff training.
- 3.6 Confidentiality and sensitivity are maintained in all aspects of incident management.
- 3.7 Staff are trained and equipped to respond appropriately to critical incidents within their scope of responsibility.
- 3.8 Digital security and data integrity are safeguarded through proactive monitoring and response to cyber threats.
- 3.9 Critical incidents may vary in nature and severity. The following table outlines common types of incidents and provides examples to guide identification and response.

Type of Incident	Description	Examples
Medical Emergency	Situations involving serious injury, illness, or death of a student, staff member, or visitor.	Heart attack, severe allergic reaction, student collapse, death on campus.
Mental Health Crisis	Incidents involving acute psychological distress or risk of self-harm.	Suicide attempt, severe anxiety episode, psychotic episode.
Security or Safety Threat	Events that pose a threat to personal safety or campus security.	Assault, armed intruder, bomb threat, vandalism, theft.
Natural Disaster	Environmental events impacting campus operations or safety.	Flood, bushfire, earthquake, severe storm.
Infrastructure Failure	Disruptions to essential services or facilities.	Power outage, gas leak, building collapse, IT system failure.

Type of Incident	Description	Examples
Public Health Incident	Health-related emergencies affecting the wider community.	Infectious disease outbreak, contamination, pandemic response.
Student Welfare Incident	Events affecting student wellbeing or safety outside normal operations.	Missing student, domestic violence disclosure, unsafe accommodation.
Reputational or Media Incident	Situations that may impact TITAN's public image or reputation.	Negative media coverage, social media crisis, breach of confidentiality.
Transport or Off-Campus Incident	Incidents occurring during TITAN-endorsed activities off-site.	Vehicle accident during field trip, injury during internship, overseas student emergency.
Cybersecurity Incident	Events involving unauthorised access, data breaches, or disruption of digital systems.	Cyber attack, ransomware infection, phishing compromise, unauthorised data disclosure.

4. Policy Statements

TITAN HIGHER EDUCATION (TITAN/THE) is committed to providing a safe, secure, and supportive learning and working environment through the effective management of critical incidents. To achieve this, TITAN will:

- Maintain a comprehensive framework for the prevention, preparedness, response to, recovery from, and review of critical incidents affecting students, staff, contractors, visitors, and institutional operations.
- Manage all critical incidents promptly, consistently, and effectively to minimise harm and protect the health, safety, wellbeing, and security of all members of the TITAN community.
- Comply with all applicable legislative, regulatory, contractual, and reporting obligations, including requirements of government authorities, emergency services, regulatory agencies, and partner institutions.
- Ensure clearly defined roles, responsibilities, authorities, and decision-making processes are established to support coordinated and effective critical incident management.
- Provide timely, appropriate, and equitable support to individuals affected by critical incidents, including access to counselling, wellbeing services, academic adjustments, emergency assistance, and referral to external support services where appropriate.
- Protect the privacy, dignity, confidentiality, and cultural needs of individuals involved in critical incidents, while ensuring information is managed and disclosed in accordance with legislative requirements and institutional policies.
- Maintain timely, accurate, and appropriate communication with affected individuals and relevant internal and external stakeholders throughout the management and recovery phases of a critical incident.
- Support the continuity of teaching, learning, research, student services, and other critical business operations through effective business continuity and recovery planning.
- Significant incidents that disrupt teaching, learning, student support services or corporate operations may result in activation of the Business Continuity Framework.
- Integrate critical incident management with TITAN's governance, risk management, work health and safety, emergency management, and business continuity frameworks to strengthen organisational resilience.
- Ensure staff receive appropriate training, guidance, and resources to enable effective preparation for and response to critical incidents.
- Maintain accurate and secure records of critical incidents, actions taken, decisions made, communications, and outcomes to support accountability, compliance, quality assurance, and organisational learning.
- Monitor, review, and evaluate the management of all critical incidents to identify lessons learned,

strengthen institutional capability, reduce future risks, and support continuous improvement.

- Foster a culture of safety, preparedness, resilience, and continuous improvement that promotes the wellbeing of students, staff, and the broader TITAN community.
- Regularly review this Policy and associated procedures to ensure they remain effective, current, and aligned with legislative requirements, regulatory expectations, and sector best practice.

5. Procedures

5.1 Reporting and Initial Response

5.1.1 Identification and Notification

- Any staff member or student who becomes aware of a critical incident must immediately notify the Campus Manager or designated Critical Incident Coordinator.
- The Coordinator will assess the nature and severity of the incident and initiate the appropriate response level.

5.1.2 Immediate Actions

- Ensure safety and provide first aid or emergency assistance where required.
- Contact emergency services (police, ambulance, fire) if necessary.
- Secure the affected area to prevent further harm or disruption.
- Record preliminary details of the incident using the **Critical Incident Report Form**.
- Where evacuation is necessary, Emergency Wardens will implement evacuation procedures in accordance with the **Emergency Management Plan**.

5.1.3 Escalation Requirements

- Category 1 – Emergency services immediately.
- Category 2 – Registrar within the 1 hour.
- Category 3 – CEO immediately.
- Category 4 – Registrar and Business Continuity activation if required.
- Category 5 – CEO and Registrar immediately.

5.2 Management and Communication

5.2.1 Activation of the Critical Incident Team (CIT)

- The Coordinator will convene the CIT to manage the response and allocate responsibilities.
- The CIT will coordinate communication with internal and external stakeholders, including students, staff, emergency services, and regulatory bodies.
- The CIT will ensure accurate and timely information is disseminated to prevent misinformation or reputational harm.
- The Business Continuity Plan will activate when:
 - the campus closure exceeds 24 hours;
 - there are major IT outages;
 - there is significant infrastructure damage;
 - teaching is significantly disrupted.

5.2.2 Support and Follow-Up

- Provide counselling and welfare support to affected individuals.
- Arrange academic or operational adjustments as appropriate.
- Family liaison, embassy/consulate liaison for international students.
- Memorial arrangements where appropriate, and ongoing welfare monitoring.
- Conduct a debriefing session with involved parties to review actions taken.
- Document all decisions and communications for compliance and continuous improvement.

5.2.3 Regulatory Reporting

- CEO in consultation with the Quality and Compliance Manager assesses whether the incident constitutes a reportable event.
- TEQSA notification requirements are considered and notified as required.
- Other regulators and agencies are notified where required.

5.2.4 Media and External Communications

- The CEO is the authorised spokesperson.
- Staff must not make unauthorised public statements.
- Communications must be coordinated through the CIT.

5.3 Review and Preventive Measures

- Conduct a post-incident evaluation to identify lessons learned.
- Update policies, procedures, and training materials based on findings.
- Implement preventive strategies to reduce the likelihood of recurrence.
- Report outcomes to senior management and include in annual compliance reviews.
- Annual evacuation drills, desktop simulation exercises, and CIT exercises.
- Review of outcomes and corrective actions.

5.3.1 Record Management

- TITAN will maintain accurate records of critical incidents, investigations, communications, actions taken, outcomes and corrective measures.
- Records will be retained in accordance with legislative requirements and TITAN Records Management requirements.

5.4 Model Alignment Statement

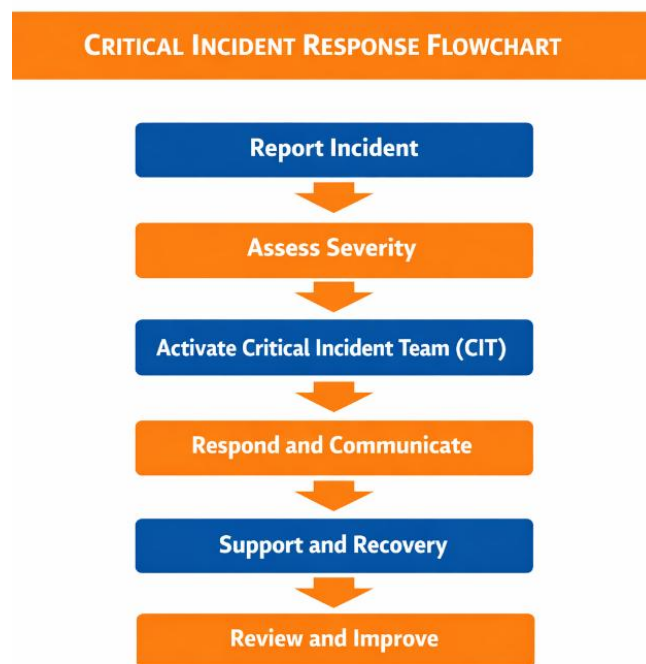
TITAN's Critical Incident Procedures are informed by recognised emergency management and higher education governance frameworks to ensure consistency, compliance, and best practice. Specifically, these procedures align with:

- The **PPRR Model** (Prevention, Preparedness, Response, Recovery):
 - providing a structured approach to incident management and continuous improvement.
- The **Australasian Inter-Service Incident Management System (AIIMS)**:
 - ensuring coordinated command, communication, and control during critical incidents.

- The **ISO 22320:2018 Emergency Management Guidelines**:
 - promoting interoperability, documentation, and systematic evaluation of incident response.
- The **Higher Education Standards Framework (Threshold Standards) 2021 (Australia)**:
 - ensuring student safety, welfare, and continuity of learning are maintained throughout all incident phases.

This alignment supports TITAN’s commitment to effective crisis management, regulatory compliance, and the wellbeing of its community.

5.5 Critical Incident Response Flowchart



This flowchart illustrates the six stages of TITAN’s critical incident management process — Report Incident, Assess Severity, Activate Critical Incident Team (CIT), Respond and Communicate, Support and Recovery, and Review and Improve — using TITAN’s official orange and blue branding for visual consistency and professional presentation.

6. Roles and Responsibilities

6.1 The Board of Directors are responsible for:

- Endorsing this **Critical Incident Policy and Procedure** and ensuring alignment with TITAN’s governance framework.
- Overseeing risk management and compliance reporting related to critical incidents.
- Reviewing post-incident evaluations and approving recommendations for continuous improvement.

6.2 The Chief Executive Officer is responsible for:

- Providing strategic leadership and ensuring adequate resources for incident management.
- Authorising activation of the Critical Incident Team (CIT) for major incidents.
- Liaising with external authorities and regulatory bodies as required.
- Reporting significant incidents to the Board of Directors.

6.3 The Operations Director is responsible for:

- Coordinating operational response activities and resource allocation during critical incidents.
- Ensuring campus facilities and infrastructure are safe and secure.
- Supporting the CEO and CIT Leader in incident management and recovery planning.
- Overseeing documentation and reporting of operational impacts and actions taken.

6.4 The Academic Director is responsible for:

- Ensuring academic continuity and quality assurance during critical incidents.
- Coordinating with the Registrar to implement academic adjustments and student support measures.
- Providing guidance to academic staff on student welfare and assessment flexibility.
- Participating in post incident reviews to identify academic impacts and improvement opportunities.

6.5 The Registrar is responsible for:

- Managing student records and academic continuity during and after critical incidents.
- Coordinating communication with students regarding academic adjustments and support services.
- Ensuring confidentiality and accuracy in student data handling throughout the incident process.
- Liaising with the Academic Dean and Quality and Compliance Manager to ensure regulatory requirements are met.

6.6 The Quality and Compliance Manager is responsible for:

- Ensuring all incident management activities comply with regulatory and legislative requirements.
- Maintaining records of incident reports, investigations, and follow-up actions.
- Coordinating reporting to external agencies and regulators as required under the HESF 2021 and TEQSA standards.
- Supporting continuous improvement through policy review and training recommendations.

6.7 Critical Incident Team (CIT) is responsible for:

- the operational management of critical incidents and acts as the central coordination body during response and recovery.

6.7.1 Composition:

- Chief Executive Officer (or delegate).
- Registrar.
- Academic Dean.
- Quality and Compliance Manager.
- Communications Officer (if appointed).

6.7.2 Responsibilities:

- Assess the severity and scope of the incident, determine appropriate response actions, and direct operational responses.
- Suspend activities, and coordinate communication between internal and external stakeholders, including emergency services.
- Implement the incident response plan and monitor progress through each stage of the flowchart.

- Ensure documentation of all actions, decisions, and communications for audit and review purposes.
- Conduct a post incident debrief and submit recommendations for policy and procedure improvements.

6.8 Responsibility Matrix

Incident Stage	Board of Directors	CEO	Operations Director	Registrar	Academic Dean	Quality and Compliance Manager	CIT
Report Incident	Receive notification of major incidents	Authorise initial response	Secure campus operations	Record student details	Advise on academic impact	Log incident for compliance	Coordinate reporting and assessment
Assess Severity	Review strategic implications	Evaluate scope and risk	Assess operational impact	Confirm student status	Identify academic continuity needs	Verify regulatory requirements	Lead assessment and classification
Activate CIT	Approve activation for major incidents	Authorise CIT mobilisation	Deploy resources	Support data management	Advise on academic adjustments	Ensure compliance alignment	Mobilise team and assign roles
Respond and Communicate	Monitor strategic response	Oversee communication and decision making	Manage campus logistics	Communicate with students	Support academic staff	Report to regulators	Execute response plan and updates
Support and Recovery	Review progress and resource needs	Lead recovery strategy	Restore operations	Update student records	Resume academic activities	Audit incident records	Coordinate support and follow-up
Review and Improve	Approve recommendations and policy updates	Present final report to Board	Evaluate operational performance	Archive student data	Review academic outcomes	Submit compliance report	Conduct debrief and recommend improvements

7. Definitions

Definitions for key terms are presented in the Glossary of Terms which may be accessed on the TITAN website.

8. Relevant Legislation, Guides, and/or Websites

8.1 Legislation:

- [Education Services for Overseas Students Act 2000](#) (accessed July 2026)
- [Higher Education Standards Framework \(Threshold Standards\) 2021](#), as amended – 2.3, 6.2.1 (e, j), 7.2.3 (c), (accessed July 2026).
- [Higher Education Standards Framework Amendment \(Threshold Standards\) Instrument 2026](#) – 6.2.1 (j, k), (accessed July 2026).
- [National Code of Practice for Providers of Education and Training to Overseas Students 2018](#) (accessed July 2026).
- [Tertiary Education and Quality Standards Agency Act 2011](#) (accessed July 2026).
- Work Health and Safety legislation and regulations applicable to TITAN operations
- [Privacy Act 1988 \(Cth\)](#) (accessed July 2026), and applicable privacy principles
- Applicable anti-discrimination, harassment, bullying, and student safety legislation
- Applicable public health emergency and emergency management legislation

8.2 Guides:

- TEQSA Guidance Note: [Wellbeing and Safety](#) (accessed July 2026).

9. Related TITAN Documents

- Business Continuity Policy and Procedure
- Campus and Facilities Management Policy and Procedure
- Human Resources Framework
- Learning and Teaching Plan Records and Data Management Policy and Procedure
- Risk Management Policy and Procedure
- Sexual Harassment and Gender-Based Violence Prevention and Response Policy and Procedure
- Strategic Asset Management Plan
- Strategic Plan
- Grievances Policy and Procedure
- Work-Integrated Learning Policy and Procedure

10. Version Control

Combined Policy and Procedure Version Control		
Version #	Date of Change	Change Summary
2026.1	July 2026 Approved BoD 23.09.2026	Policy and Procedure Documents were combined into one complete document. Layout of the document updated, more information added into each section. Added links to relevant legislation and websites. Document has been recoded and irrelevant information removed.

Original Policy Version Control		
Version #	Date of Change	Change Summary
1.0	12-Aug-20	Draft approved by the Board of Directors (BoD 1-May-20) with minor amendments
1.1	9-Dec-21	Revised for HESF 2021 and administrative updates
1.2	8-Jul-23	Update following TEQSA registration
Original Procedure Version Control		
Version #	Date of Change	Change Summary
1.0	12-Aug-20	Draft approved by the Board of Directors (BoD) 1-May-20 with minor amendments
1.1	8-Jul-23	Update following TEQSA registration

Warning –

- Document uncontrolled when printed! The current version of this document is maintained on the TITAN website.