**Australian Institute of Technology & Commerce Pty Ltd**
ABN 47 634 668 214 CRICOS Code: 03996D
Head Office: Level 6, 8 Quay Street, Haymarket NSW 2000
Website: www.aitc.nsw.edu.au Email: info@aitc.nsw.edu.au
Phone: 02 9211 4958

AUSTRALIAN INSTITUTE OF TECHNOLOGY AND COMMERCE

# Critical Incident Management Procedure

| | |
|---|---|
| **Purpose** | **This Procedure is to address the risks and consequences to the business activities of Australian Institute of Technology & Commerce (AITC) that may arise from critical incidents and provide effective responses to such incidents and therefore address such risks.** |
| **Location** | **The Procedure is maintained on owncloud** |
| **Responsible executive** | **CEO** |
| **Responsible office** | **CEO's Office** |
| **Contact officer** | **TBA** |
| **Effective date** | **29 June 2020** |
| **Review date** | **TBA** |
| **Modification history** | **Version 1.0** |
| **Related documents** | **AITC Security and Safety Policy**<br>**AITC Business Continuity Management Policy**<br>**AITC Workforce Plan** |
| **Authority** | **Approved by Council** |

## 1. Purpose

The purpose of this Procedure is to address the risk and consequences that may arise from critical incidents and to provide effective responses to critical incidents as well as mitigate future risks produced by similar incidents in the future.

## 2. Scope

As outlined in the Higher Education Standards Framework (2015) AITC needs to demonstrate that it is operating effectively and sustainably monitoring critical incidents and taken actions to address underlying causes (Standard 6), and it also documents and records responses after critical incidents (Standard 7).

This procedure therefore impacts on AITC staff, students and facilities. The TEQSA Threshold Standards, the National Code of Practice and Providers of Education and Training to Overseas Students (National Code 2018) requires AITC to demonstrate its compliance with the National Code 2018 at the point of CRICOS registration and throughout its CRICOS registration period.

## 3. Definitions

A Critical Incident means a situation or traumatic event that causes or presents a significant risk to students and staff of AITC outside a normal range of experiences. Critical incidents encompass situations such as bodily harm, property damage, legal interventions, media activity, pandemics, natural disasters, war or acts of terrorism or other unusual activities that fall outside the scope of activities undertaken by AITC.

## 4. Procedures

### 4.1. Objective

4.1.1. The Registrar is authorised by AITC to manage critical incidents directly involving students and staff at the AITC campus.

4.1.2. The Registrar is the nominated Critical Incident Coordinator (CIC) who manages the Critical Incident Management Team (CIMT).

4.1.3. The Registrar monitors the availability of appropriate resources for managing critical incidents and then develops appropriate safety measures.

4.1.4. Key personnel are trained to understand and manage critical incidents.

### 4.2. Procedure

#### 4.2.1. Phase 1: Prevention

4.2.1.1 The prevention of critical incidents is addressed through risk identification being the major component of the critical incident management protocol. AITC will undertake Critical Incident Risk Assessments and thereby identify the key risks for AITC as well as document and record responses associated critical incidents;

a) record risks, mitigation strategies and resultant risk;
b) advise on individual plans to minimise the risks identified through such measures as education and training, improvements to Work Health and Safety (WH&S), student counselling and discipline, individualised plans for students with challenging behaviour, security measures etc.;
c) undertake an annual audit of the resources for managing key risks and report any shortfall to (the CEO);
d) approve the Risks and Prevention Checklist;
e) ensure all AITC International students complete the Student Contact Information Form and confirm the accuracy of those contact information on a regular basis (usually every 6 months); and;
f) ensure a copy of the Student Contact Information Form is placed on the AITC website.

#### 4.2.2. Phase 2: Response

4.2.2.1 The staff member directly involved with the critical incident is to;

a) ensure the physical safety of students and staff as a matter of urgency (i.e. lockdown or evacuation of premises);
b) call emergency services as appropriate on 000;
c) call the AITC Critical Incident Coordinator (CIC); and;
d) refer directly to the Immediate Response Checklist for response action specific to the incident.

#### 4.2.3. Phase 3: Recovery

4.2.3.1 The CIC at AITC is to;

a) provide all those affected by the incident with access to factual information;
b) contact the AITC CEO;
c) coordinate the de-briefing of those affected within 8 hours of the incident;
d) monitor the need for counselling.
e) initiate and maintain contact with those affected by the incident; and;
f) assess the need for on-going additional support from outside agencies.

A written record of the critical incident will be maintained by AITC and the remedial action that have been taken by AITC will also be advised to students and staff.

#### 4.2.4. **Phase 4: Review**

4.2.4.1 The Recovery and Response action to assist students affected by a critical incident will be reviewed annually by the CEO or in the event of a critical incident, (i) one-week post incident, (ii) 2 months post-incident and (iii) 6 months post-incident.

**(i) The CIC and the CEO will meet within one week of incident.**

Purpose:

- De-brief the team and update on outcomes.
- The CIC will complete a Critical Incident Report to build on cumulative experience of handling crises so that AITC can improve its crisis response and it will be completed prior to the meeting.
- This report will be discussed, and appropriate actions taken.
- Assess the need for legal advice.
- Prepare a report for the Risk Committee.

**(ii) The CIC and CEO will meet two months post-incident.**

Purpose:

- Review of recovery phase. i.e. assess need for ongoing counselling; for example, provision of memorials, resource management, involvement with coronial inquests etc.
- Re-assess the AITC legal position.
- Prepare a report for the Risk Committee.

**(iii) The CIC and CEO to meet six months post-incident.**

Purpose:

- Review AITC's critical incident policy and procedures.
- Prepare a report for the Risk Committee.

### 4.3. **Risks and Prevention Checklist**

#### 4.3.1. **Fire**

4.3.1.1. Risk

a) Origin could be internal or external.
b) Internal hazards - electrical equipment and connections, chemicals and from other offices in the building.
c) Student computer rooms pose the highest risk factor due to quantity of electrical devices and connections.

4.3.1.2. Preventive Measures

a) The building normally provides fire protection measures including fire alarms, smoke detectors, sprinkler system, fire extinguishers, building construction and floor plans to assist with evacuation.
b) All staff and students participate in the fire drills and practice evacuation procedures.
c) Regular inspection of fire extinguishers and smoke detectors.
d) Emergency electrician contact details are available from the Administration and Marketing Manager.

4.3.2.**Water**

4.3.2.1. Risk

a) Origin could be internal such as leaking or damaged plumbing.
b) Origin could be external such as leaks due to storm damage or flooding.

4.3.2.2. Preventive Measure

a) Regular inspection of the premises - the computer room.
b) Any water leakage must be reported to the building manager.

4.3.3.**Criminal Behaviour**

4.3.3.1. Risk

a) Destructive or threatening behaviour by an individual or group such as: physical attack, bomb threat, theft, vandalism, or firearm incident, etc.

4.3.3.2. Preventive Measure

a) The buildings are alarmed outside operating hours.
b) Offices and facilities are kept locked outside operating hours.
c) All confidential information is physically or electronically secure.
d) Staff training.
e) Emergency contact detail for security staff and emergency services are posted by all staff phones and in student areas.

4.3.4.**Data / Information Security**

4.3.4.1. Risk

a) System failure.

b) Physical destruction of computer server and information storage areas.
c) Corruption or theft of data.
d) Electrical overload.

4.3.4.2. Preventive Measures

a) System back up
b) Scanning of vital hardcopy documents
c) Offsite document storage.
d) System security including firewalls, password protection
e) Lockable storage areas and filing cabinets.
f) Use of quality databases.

4.3.5 **Pandemics**

4.3.5.1 Risks

a) Infection of students and staff
b) Closure of facilities

4.3.5.2 Preventive Measures

a) More on-line delivery
b) Social isolation
c) Lock down
d) Work from home

4.4. **Communication**

Effective communication throughout the organisation is critical during a critical incident. The CIC is responsible for liaison and communication with all relevant persons and organisations.

Students and Staff will be advised on how to seek assistance for and report an incident.

4.5. **Training**

All staff will receive a copy of the Critical Incident Procedure and WH&S training as part of their orientation. All staff and students will participate in regular emergency evacuation training.

4.6. **Equipment and materials**

All emergency equipment will regularly, checked, serviced and replaced when necessary. Enough equipment and material for effectively responding to recovering from emergencies will be available, including First Aid.

4.7. **Useful Documentation**

- The Organisational Chart with staff names and positions
- The Critical Incident Register
- Up to date staff contact details and the nominated critical incident coordinator
- Up to date student lists
- Emergency Services and Security contact details

- Supplier contact details
- Evacuation procedures
- Floor plans showing emergency exits
- Details of staff with First Aid training
- Insurance information
- IT system specification
- Copies of maintenance agreements