AUSTRALIAN INSTITUTE
OF HIGHER EDUCATION

Critical Incident Management Plan

Policy Category	Administrative
Policy Code	ADM-HE-33
Policy Owner	Chief Executive Officer
Responsible Officer	Chief Executive Officer
Approving authority	Board of Directors
Contact Officer	Registrar
Approval date	1 March 2017
Commencement date	6 March 2017
Review date	3 years
Version	2017.1
Related Documents	

1. Purpose

This document is designed to address various types of possible scenarios following a critical incident within the Australian Institute of Higher Education Pty Ltd ('the Institute'). Preparation for, response to, and recovery from a critical incident affecting the information resources, education facilities, administration, personnel or clients of the Institute requires the cooperative efforts of all managers in partnership with the functional areas supporting the operations of the Institute.

The objectives of this Critical Incident Management Plan ('CIMP') are to make sufficient preparations for responding to a critical incident in order to minimise the effect upon the operations of the Institute.

A CIMP is necessary to consider the legal responsibility of management, the possibility of financial loss and the effect of an interruption to operations due to a critical incident which affects the business, its staff or its clients. Firstly, management has a legal responsibility to protect its corporate resources and information. Secondly, because of the importance of IT resources in the running of the business, the Institute is dependent on its IT infrastructure and stored data as part of its normal business operations. If any facet of the IT resources breaks down, a significant financial loss to the company could develop, or even destroy the business if proper planning has not been carried out. Thirdly, any interruption to the normal operations of the Institute could be damaging to the future relationships with students and other stakeholders (including regulators) and could affect the public image of the Institute. The costs of not taking precautions could be much more damaging and costly than preparing for critical incidents.

This CIMP is not designed to provide an answer to each and every type of critical incident that could happen, but rather is provided to identify the methods on how to handle and recover from a critical incident if one was to occur.

2. Background

Critical incidents are extraordinary events that because of their scope, intensity or duration, and overwhelm the Institute's capacity to cope. Critical incidents may be classified as natural; such as floods, bushfires, earthquakes, and storms; or human-caused, through deliberate attack on the resources, personnel or clients of the Institute.

This CIMP relates to the overall emergency plans of the Institute and aims to minimise the damage incurred during an emergency, by providing guidelines for a rapid and effective response to an emergency situation. The CIMP is designed to complement procedures laid down elsewhere concerning safe work practices for staff, regular maintenance of buildings and facilities and evacuation procedures in case of emergency. Nothing in this plan is to be taken as contrary to guidelines and procedures laid down elsewhere concerning these matters.

3. Examples of Critical Incidents

- The death or critical injury of a staff member, student or visitor on Institute premises (or elsewhere).
- The destruction of whole or part of premises that the Institute occupies (e.g. by fire).
- The threat of damage to premises that the Institute occupies (e.g. a bomb threat).
- Staff and/or students being taken hostage.
- A break-in accompanied by major vandalism.
- Students being killed/injured while engaged in an Institute-sponsored activity.
- A natural or other major critical incident in the community.
- The breakdown of key IT infrastructure, either by mechanical means or human intervention.
- Incidents in which sights, sounds, or smells are distressing.
- Storms/natural disasters.
- Acute illness (physical or mental).
- A student under the age of 18 going missing.
- Physical or sexual assault.
- Any incident that is charged with extreme emotion.

4. Prevention and Preparation

In order to prevent and prepare for a critical incident the following will be implemented:

- All facilities are subject to regular maintenance
- Emergency evacuation notices illustrating the location of assembly in the event of a fire or other similar situation are to be prominently displayed throughout the building (***Appendix B***).
- Emergency exits are clearly marked and kept clear of obstacles at all times.
- Emergency wardens are to be appointed and trained regularly in emergency procedures.
- First aid officers are to be appointed and their first aid certificate is to be kept up to date.
- The availability of appropriate resources and the development of safety measures to be monitored on a regular basis through the WHS contact and relevant managers.
- Regular practice building evacuations are to be carried out.
- Backups of computer records are stored off-site and are retrievable.
- Staff are encouraged to report any possible safety issues to management.
- New staff are made aware of the Critical Incident Policy and Procedure as part of induction processes.
- Lock down procedures including safe and secure lockable rooms or escape paths in event of a terrorist entering building.
- Reporting of suspicious activity and persons, for example, strangers entering AIH building areas.

To prepare for an emergency, the relevant Student Services Managers should maintain a contact list of all relevant community resources including:

- Medical authorities
- Police
- Funeral Directors
- Religious leaders
- Ethnic group leaders
- Consular representatives
- Insurance people
- Interpreters
- Counsellors
- Mobile and fixed phone numbers of landlord and other occupants/tenants in the building

5. The Plan in Action

The emphasis of this CIMP is based on four major steps:

1. Reaction
2. Recovery and Restoration
3. Review and Action
4. Reporting

5.1 Reaction

a) Communication

When a critical incident occurs, it is important that key people are notified. In all emergency situations, the primary objective is the safety of human lives. Salvage and recovery operations will be of secondary importance, and will take place only when the affected area is declared safe.

When a critical incident occurs, notify the Executive Dean (or his/her alternate). The contact details for the personnel occupying these positions and their alternates are detailed in ***Appendix A***.

The Executive Dean (or his/her alternate) will be the Coordinator of the emergency response and will contact relevant emergency services or other personnel as required.

b) Immediate Response to a Critical Incident

1. Notify the responsible persons as outlined above.
2. Immediately after notification of the incident the following questions need to be addressed by the Coordinator:
   - What happened?
   - What makes the event critical?
   - When did the incident occur?
   - Where did it happen?
   - Who was involved?
   - Who needs assistance?
   - What is the most appropriate intervention?
3. If Emergency Support Services such as fire, ambulance or police are required, contact details are listed in ***Appendix A***.
4. In the case that it is decided that evacuation is an appropriate intervention the evacuation plans included at ***Appendix B*** should be utilised.

5.2 Recovery and Restoration

a) The Timeframe for Recovery

i. The first 24 hours:

- Gather accurate facts and information.
- If possible, re-establish a sense of routine within the Institute. Staff members and students will feel safe once the regular patterns of management and organization have been re-established.

ii. **The first 48 – 72 hours:**

- Restore routines while taking into account the needs of staff and students.
- Engage support services to manage the reactions of staff and students.
- Monitor the support services provided.
- Provide additional assistance if required and when necessary.
- Provide a formal staff meeting with professional input (if appropriate).

iii. **The first two weeks after the critical incident:**

- Monitor progress of those hospitalised, injured or off work.
- Stay alert for delayed reactions from staff and students.
- Provide relevant information to those who require it.

b) Key Actions

- Notify all key personnel of the problem and assign them tasks focused toward recovery from the critical incident.
- Notifying students about the problem minimises panic or concern.
- Recall data backups - if backups are stored offsite, these need to be recalled. If using remote backup services, a network connection to the remote backup location (or the Internet) will be required.
- Organise alternate facilities in order to continue operations.
- Prepare the staff - during a critical incident, staff are required to work longer, more stressful hours, and a support system should be in place to alleviate some of the stress. Prepare staff ahead of time to ensure that work runs smoothly.
- Provide counselling opportunities and support; opportunities should be given for staff and students to discuss the incident in a supportive environment. If the incident involves death, staff and students should be apprised of funeral details and given leave to attend Staff members are not expected to be counsellors; therefore the establishment of counselling support appropriate to the particular critical incident is important.

c) IT Infrastructure and Data

i. **Preventions against data loss:**

In relation to IT Infrastructure the following preventions should be implemented:

- Backups are sent off-site at regular intervals;
- Backups include software as well as all data information, to facilitate recovery;
- Utilise surge protectors - to minimise the effect of power surges on delicate electronic equipment;
- Protect servers and essential equipment with an Uninterruptible Power Supply (UPS) and/or backup generator;
- Fire Prevention – instal effective alarm systems and accessible fire extinguishers;
- Employ anti-virus software, firewalls and other security measures.

ii. **Security Safeguards:**

1. **Against in-house intrusions:**
   - All administration and student computer accounts are password protected.
   - Student user accounts have their own restriction through group policy on their own domain. This policy will restrict the students from changing the standard computer configuration and software setting.
   - Administration and student network are physically separated. There is no physical connection (via hub or switch) between these two networks.

- Every workstation has images, just in case of a hardware failure, it can be easily restored.

2. **Against external intrusions:**
   - All external access is protected by firewalls against unauthorised external access from outside the network.
   - All servers are protected by anti-virus software.

iii. **In the event that equipment is damaged or data is compromised:**

1. **Internet Connection:**
   The Institute has 2 dedicated internet connections for staff and students with one router and modem each. Internet provider guarantees 99.9% SLA which meets the Institute's demands.

2. **Failure of switch/hub within the network:**
   Switches are installed in a secure, temperature controlled environment. Spare switch is in stock in case of a switch failure, which can be replaced in acceptable time.

3. **Server Failure:**
   The following equipment is available in the case of server failure:
   - 2 student servers (1 primary / 1 cloud)
   - 2 admin servers (1 primary / 1 cloud)
   - In case of primary server failure the backup server will automatically take over
   - Server activity log is recorded on each server
   - Fileserver data is replicated at 3am daily to the cloud

5.3 Review and Action

After the critical incident has been dealt with it is essential that the Institute undertakes an evaluation to determine if there are any improvements that can be made to better handle critical incidents in the future. Evaluation of the CIMP and the roles and functions of the Coordinators and relevant support staff are an essential part of the process. Executive Management should conduct a formal evaluation of the process involved in the management of the critical incident after debriefing has occurred. Formal evaluation provides opportunities for feedback on the strengths and weaknesses of the CIMP and provides an opportunity for continuous improvement, including changes that may be required to policies and procedures. Feedback should be sought from those who have been involved in various aspects of the operation of the CIMP as part of the evaluation.

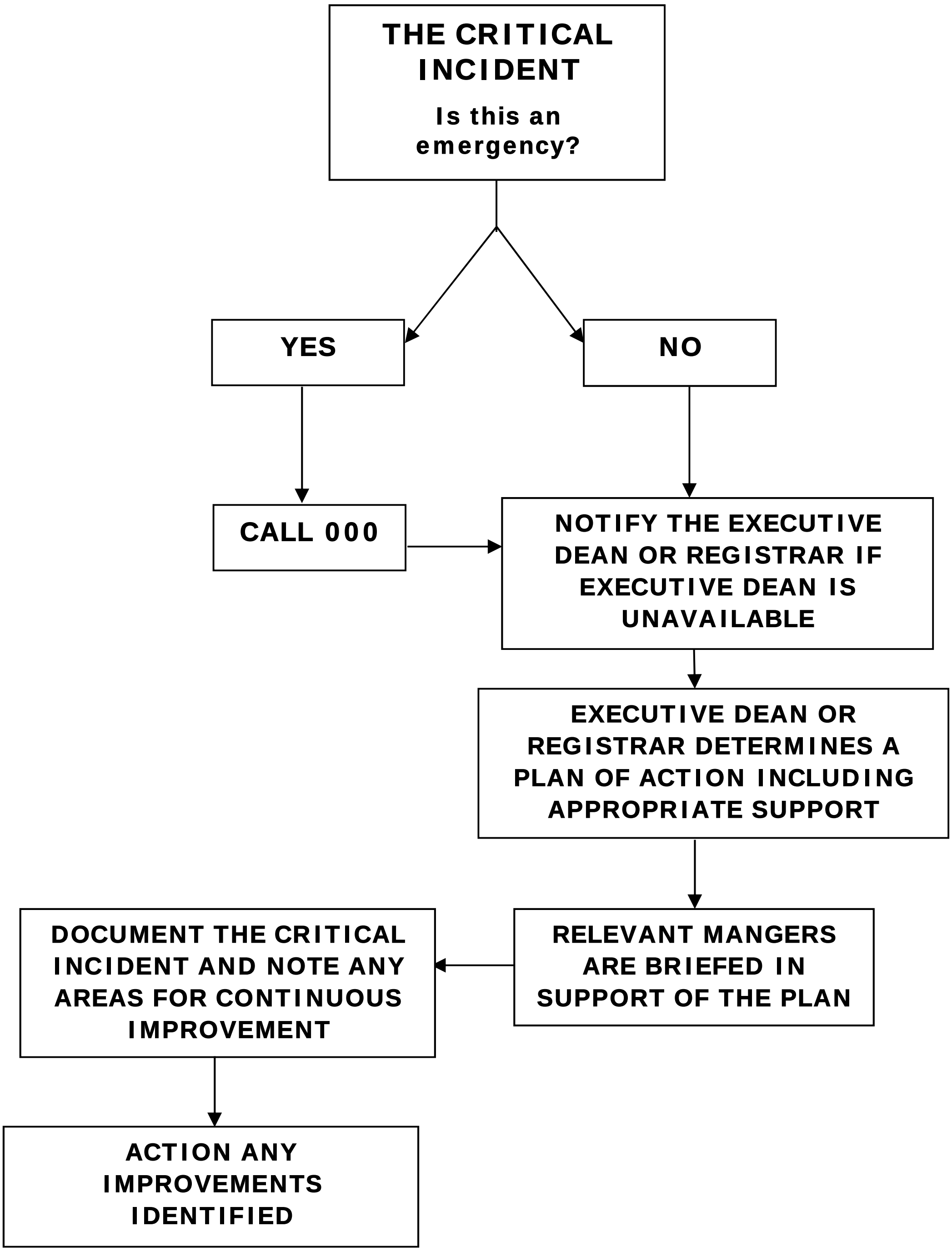
5.4 Reporting

Written and or verbal reports are provided to the appropriate manager including any recommendation on ways to prevent similar occurrences.

Written reports, approved by the student, are to be placed on the student's file and kept in the Institutes Critical Incident file. The reports are to be sent to the parents of the student (if appropriate) and other relevant authorities with permission.

Media enquiries should be referred to the Executive Dean and the Chief Operation Officer.

6. Flowchart


THE CRITICAL INCIDENT
Is this an emergency?
YES
NO
CALL 000
NOTIFY THE EXECUTIVE DEAN OR REGISTRAR IF EXECUTIVE DEAN IS UNAVAILABLE
EXECUTIVE DEAN OR REGISTRAR DETERMINES A PLAN OF ACTION INCLUDING APPROPRIATE SUPPORT
RELEVANT MANGERS ARE BRIEFED IN SUPPORT OF THE PLAN
DOCUMENT THE CRITICAL INCIDENT AND NOTE ANY AREAS FOR CONTINUOUS IMPROVEMENT
ACTION ANY IMPROVEMENTS IDENTIFIED

7. Relationship to the National Code

The *National Code of Practice for Registration Authorities and Providers of Education and Training to Overseas Students* Standard 6.4 requires that providers registered to deliver courses to international students "must have a documented critical incident policy together with procedures that covers the action to be taken in the event of a critical incident, required follow-up to the incident, and records of the incident and action taken".

This CIMP is designed, among other things, to meet the requirements of this Standard.

The Educational Services for Overseas Students Act 2000 (ESOS Act) requires the Institute to notify the Department of Immigration and Border Protection ('DIBP') and the Department of Education and Training ('DET') as soon as practical after a critical incident involving an international student. In the case of a student's death or other absence affecting the student's course progression, this will need to be reported via the Provider Registration and International Student Management System (PRISMS).

8. Version Control

This Policy has been endorsed by the Australia Institute of Higher Education Board of Directors as at March 2017 and is reviewed every 3 years. The Policy is published and available on the Australian Institute of Higher Education website http://www.aih.nsw.edu.au/ under 'Policies and Procedures'.

Change and Version Control				
Version	**Authored by**	**Brief Description of the changes**	**Date Approved:**	**Effective Date:**
2016-2	Registrar	Updated template.	6 July 2016	6 August 2016
2017-1	Ms. McCoy	Revised rules.	1 March 2017	6 March 2017

APPENDIX A

EMERGENCY CONTACTS

RESPONSIBLE OFFICER	CONTACT DETAILS

In all cases:

Executive Dean **Mr Gerald Ng**	Tel: (02) 9020 8053

In case the Executive Dean cannot be reached:

Registrar **Ms Danielle Baird**	Tel: (02) 9020 8059

In cases of critical incidents related to IT infrastructure:

IT Officer **Mr Bruce Cheng**	Tel: (02) 9020 8050

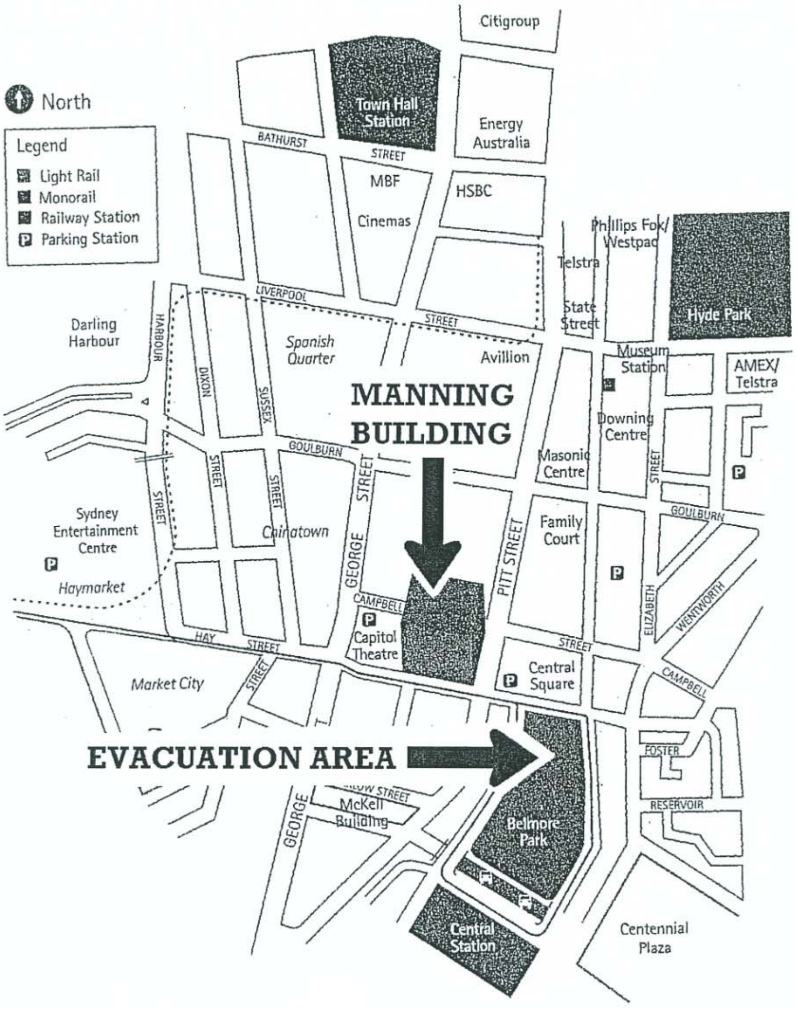
EMERGENCY AND SUPPORT SERVICES

Service	Phone Number	Address
Police	000	
Fire Brigade	000	
Ambulance Service	000	
Local hospitals:		
1. Royal Prince Alfred Hospital	95156111	Missenden Rd Camperdown Sydney
2. St Vincent's Hospital Sydney	8382 1111	390 Victoria St, Darlinghurst Sydney

APPENDIX B

EVACUATION PLANS

MANNING BUILDING EVACUATION MEETING POINT


North
Legend
Light Rail
Monorail
Railway Station
Parking Station
Citigroup
Town Hall Station
Energy Australia
BATHURST STREET
MBF
Cinemas
HSBC
Phillips Fox/ Westpac
Telstra
Hyde Park
State Street
LIVERPOOL STREET
Darling Harbour
HARBOUR
DIXON
SUSSEX
Spanish Quarter
Avillion
Museum Station
AMEX/ Telstra
MANNING BUILDING
Downing Centre
GOULBURN
STREET
STREET
Masonic Centre
STREET
Sydney Entertainment Centre
STREET
Chinatown
GEORGE STREET
PITT STREET
Family Court
GOULBURN
Haymarket
CAMPBELL
ELIZABETH
WENTWORTH
HAY STREET
Capitol Theatre
STREET
Central Square
CAMPBELL
Market City
STREET
FOSTER
EVACUATION AREA
RESERVOIR
McKell Building
GEORGE
Belmore Park
Central Station
Centennial Plaza