AUSTRALIAN INSTITUTE
OF HIGHER EDUCATION

Critical Incident Management Plan
Category: Administration (ADM)

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 ("AIH" or "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 AIH.

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. The plan assumes that:

- all facilities are subject to regular maintenance;
- emergency exits are clearly marked and kept clear of obstacles at all times;
- fire prevention measures and protection equipment is in place (e.g. fire wardens appointed, smoke detectors, alarm systems and fire extinguishers are in place and maintained);

- normal safe work practices are followed routinely and staff are familiar with fire drill and emergency evacuation procedures; and
- backups of computer records are stored off-site and are retrievable.

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.

4. The Plan in Action

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

1. Reaction
2. Recovery and Restoration
3. Review & Action

4.1 Reaction

4.1.1 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 Chief Executive Officer (or his/her alternate). The contact details for the personnel occupying these positions and their alternates are detailed in Appendix 1.

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

4.1.2 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.

4.2 Recovery and Restoration

4.2.1 The timeframe for recovery:

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 organisation have been re-established.

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).

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.

4.2.2 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.

4.2.3 IT Infrastructure and data

A. 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.

B: Security safeguards:

1. Against in-house intrusions:
    a. All administration and student computer accounts are password protected.
    b. 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.
    c. Administration and student network are physically separated. There is no physical connection (via hub or switch) between these two networks.
    d. Every workstation has images, just in case of a hardware failure, it can be easily restored.
2. Against external intrusions:
    a. All external access is protected by firewalls against unauthorised external access from outside the network.
    b. All servers are protected by anti-virus software.

C: In the case that equipment is damaged or data is compromised:

1. Internet Connection:

AIH has 2 dedicated internet connections for staff and students with one router and modem each. Internet provider guarantees 99.9% SLA which meets AIH demands.

2. Failure of switch/hub within the network:

Switches are installed in a secure, temperature controlled environment. Spare switch is on stock in case of a switch failure which can be replaced in acceptable time.

3. Server Failure:

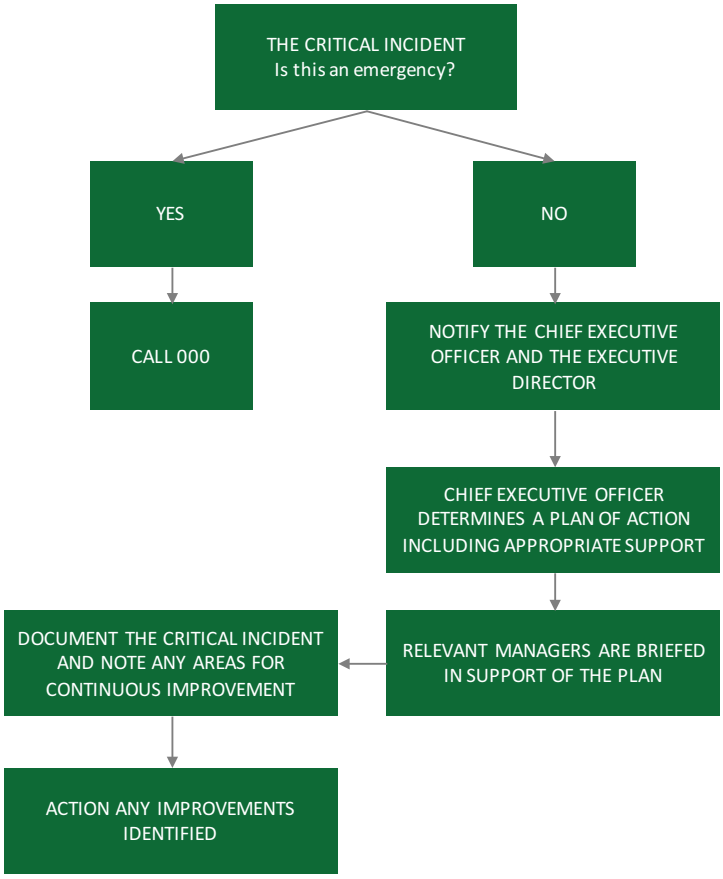
The following equipment is available in the case of server failure:

- 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

4.3 Review & 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.

6. Flowchart



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 AIH to notify DIBP and 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

Policy Code	ADM-HE-01
Version	2015.1
Cumulative Version	Version 8
Policy Owner	CEO
Authorising Body	Board of Directors
Date Approved	13 October 2015
Next Review Date	13 October 2017
Relevant Stakeholders	All staff

APPENDIX A

EMERGENCY CONTACTS

RESPONSIBLE OFFICER	CONTACT DETAILS
In all cases:	
CEO **Dr Joo-Gim Heaney** Dean **Dr Vivienne Saverimuttu**	 Tel: 9020 8050 Tel: 9020 8053
In cases of critical incidents related to IT infrastructure:	
IT officer Vlad Malganov	Tel: 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 2. St Vincent's Hospital Sydney	 95156111 8382 1111	 Missenden Rd Camperdown 390 Victoria St, Darlinghurst Sydney

APPENDIX B

EVACUATION PLANS