BUSINESS CONTINUITY MANAGEMENT POLICY

Approving authority	Governing Board
Purpose	This policy sets out how business disruption risks are identified, evaluated and managed.
Responsible Officer	President and CEO
Next scheduled review	September 2026
Document Location	http://www.ozford.edu.au/higher-education/policies-and-procedures/
Associated documents	Critical Incident Policy and Procedure Occupational Health and Safety Policy Risk Management Framework Policy Records Management Policy and Procedure Student Support and Services Policy and Procedure

1. PRINCIPLES

Business Continuity Management (BCM) is critical to responsible management practice and deals with business disruption risks. Business Continuity Management (BCM) is a process for managing operations to ensure that critical functions can, in the event of a material disruption arising from internal or external events, be maintained, or restored in a timely fashion with minimal impact to staff and students.

Some events may exceed the capacity of routine management methods and structure. This policy aims to provide a mechanism for the development of contingent capacity and plans that will enable management to focus on maintaining and resuming critical functions; whilst working in a planned way toward eventual restoration of operations and ensuring unaffected operations are able to continue.

The Ozford Institute of Higher Education (hereafter referred to as the "Institute") Business Continuity Management policy seeks to:

- ensure the continuity of critical business functions;
- allocate BCM roles and responsibilities to staff in the event of a critical incident;
- allocate management responsibility for the implementation, monitoring and review of BCM documentation;
- provide a consistent approach to BCM; and
- integrate BCM within the ***Risk Management Framework Policy*** and ***Critical Incident Policy and Procedure***.

2. SCOPE

This policy applies to all staff of the Institute and the activities they engage in while performing their professional duties.

3. DEFINITIONS

Business Continuity Management (BCM)
A holistic management approach (including policies, standards and procedures) for ensuring critical business functions can be maintained or recovered promptly in the event of a disruption.

Critical Functions
Key business activities and processes that must be restored in the event of a disruption to ensure the ability to protect the Institute's assets, meet business needs, and satisfy regulatory requirements. They include:

- manage student admissions (domestic and international);
- manage student enrolments (domestic and international);
- receive and process student enrolment fees;
- manage and facilitate courses;
- manage and facilitate examinations (paper and electronic);
- pay staff;
- pay creditors; and
- ensure census date arrangements are available (where applicable).

Critical Incident
A critical incident is defined as *'a traumatic event, or the threat of such (within or outside Australia), which causes extreme stress, fear or injury'*. It includes but not limited to incidents that may cause physical or psychological harm. Non-life threatening events can be classed as critical incidents.

Critical incidents are not limited to, but could include:

- Critical illness/serious injuries/medical emergencies involving a student or staff;
- unexpected Student/staff death;
- missing students;
- termination of welfare arrangement where the Institute can no longer take responsibility for the overseas underage student due to student refusing their approved accommodation or leaving their accommodation without notice, even after the Institute has exhausted all possible avenues of assisting the student to maintain appropriate arrangement;
- severe oral, written or psychological aggression;
- Traumatic events/threat/allegation that affect students;
    - Sexual assault
    - Physical and/or sexual abuse
    - Domestic violence
    - A child safe incident
    - Mental Health Crisis
    - Drug/alcohol abuse
    - A child safe incident
- natural disaster
- riot; fire/explosion with injuries or significant damage on campus;
- campus disturbance / riot

Disruption

Disruption-related risks are infrequent, high consequence events that impact people and operations, and are not resolved through routine management. Disruption-related risks include physical and non-physical events such as natural disasters, pandemics, significant loss of utilities, infrastructure, systems, accidents and incidents that threaten the Institute, students and staff.

Emergency

A sudden, unexpected event that endangers or threatens the Institute's community or resources and requires an immediate response from internal or external agencies and emergency services.

ICT Recovery Strategies

A comprehensive ICT strategy with a set of recovery plans to restore technological infrastructure to acceptable levels within a pre-determined period of time following an Incident.

Incident

A range of scenarios including but not limited to: natural disaster (both onshore and overseas); power outage, data corruption, hardware/telecommunications failures, human activity, injury or death; explosives, chemical, biological and nuclear hazards.

4. POLICY

4.1 Business continuity management is an important component of the Institute's Risk Management Framework. Disruption-related risks include:

- critical impact on staff (inability to maintain processes due to insufficient staff numbers);
- denial of access to building(s), floors and precinct (assets inside the building are not lost but cannot be accessed);
- loss of workplace (permanent loss of non-electronic records, research materials, equipment, inability to undertake lectures);
- loss of IT systems (inability to maintain processes or use equipment due to failure of key IT systems); and
- loss of utilities (temporary loss of electricity, gas, water etc.).

4.2 The EMT is responsible for ensuring that a business continuity management program is established and providing leadership on the implementation and maintenance of the Business Continuity Management Framework in line with the Institute's risk appetite.

4.3 The Institute is committed to the efficient and orderly resumption of its critical functions in the event of a major disruption. There are various 'threats' (natural or man-made), which could cause full or partial disruption to the operations of or access to the campus.

4.4 The Institute has appropriate Business Continuity planning in place to ensure that these disruption events can be managed quickly.

4.5 Where an incident is a critical incident involving a student, the Institute's ***Critical Incident Policy and Procedure*** will be followed.

4.6 The first priority in a disruptive incident is the immediate and ongoing safety of students, staff, contractors and visitors. The safety of life and property is the Institute's highest priority. Following this is availability of critical people, systems and processes to revert to normal business or implement a new mode of operation as soon as appropriate.

4.7 The Business Continuity plan following a disruption identifies priorities for the restoration and reinstatement of critical and non-critical operations / functions.

4.8 Staff responsible for critical functions are required to plan, specifically for:

- protection, stabilisation and continuation;
- resumption and recovery;
- dependencies and supporting resources; and
- mitigation, response to, and management of a disruptive incident.

4.9 In the event of a disruption and/or disaster, the Institute will work to reinstate operations at a capacity or level that is sufficient to perform and maintain critical functions.

4.10 The EMT will act as the Critical Incident Team (CIT) responsible for the coordination and management of any disruptive event that has a significant impact on health and safety or other operations. The CIT has delegated authority to make decisions, direct staff and students, communicate with key stakeholders including the media and authorise expenditure. Where incidents occur at the Institute and are ultimately controlled through State or Federal agencies, the CIT coordinate the Institute response to those agencies.

4.11 In restoring critical functions following a major disruption, the Institute recognises and accepts that non-critical business operations will operate at a reduced level and require time to resume full capability, capacity and performance.

4.12 Subsequent to notification of a critical incident, the Critical Incident Team will assess information, potential impact and determine whether normal business operations can resume. In the event normal operations cannot resume, it is the role of the Critical Incident Team to declare a critical incident and initiate partial or full activation of the appropriate plans.

4.13 The Institute maintains records of incidents in the Institute's BCP register.

4.14 The Institute commits to testing, maintaining and updating the procedures and processes documented in this policy and specialist recovery plans on a regular basis.

4.15 In the event a Business Continuity Plan is activated, a post incident review will be held to consolidate lessons learned and develop, address and rectify opportunities for improvement including to this policy.

4.16 The Institute provides a report annually to the Audit and Risk Committee including a review of this policy and the BCP incident register.

General Emergency Situations

Responsible Officer: President and CEO; EMT

4.17 The Institute campus is the hub of learning and teaching delivery and the day-to-day operations of the organisation. It is recognised that loss of access to or operation of could constitute full closure of onsite delivery. If this occurs, the Institute may deliver offsite or online. For example, in 2020 - 2021, the Institute delivered online to students.

4.18 The building management has responsibility for fire protection systems including the building fire sprinkler system which is regularly serviced. The building management has an emergency management system testing schedule including fire alarm and a quarterly fire evacuation drills.

No Access to Building or Infrastructure

Responsible Officer: President and CEO; EMT

4.19 The Institute has identified Institutions who would be willing to lease access to a suitable teaching facility to the Institute. The Institute has inspected their facilities and satisfied standard requirements are met.

No Access to ICT

Responsible Officer: President and CEO; Information Technology Manager

4.20 The Institute's Core Information Technology (ICT) systems have been designed to support the Institute's operations.

4.21 The Institute has appropriate measures in place to quickly rectify any disruption to ICT services. Disaster Recovery Planning is embedded in ICT operations as a key requirement of the Department. Continuous effort is made to improve and test processes to ensure when required, ICT systems can be re-established quickly to reduce the impact of any disruption.

4.22 The following security controls have been put in place and are regularly tested to verify the security of the Institute's ICT

Physical Access

- Managed by building system, floor access is only available from 8am till 5pm.
- The facility's rooms are locked when not in use.

Computer Access

- Staff and contractor network services:
  - Staff receive access to basic drive and folders.
  - Any additional folder access will require approval from Head of Department, the Academic Dean or the President and CEO by special request.
  - All computer systems require username and passwords to gain access.
  - For external access, two factor identification is in place and access is for a limited time.
- Student network services
  - Students have limited access and storage

Computer System security

- All computer systems are locked down and installation of software(s) requires administrator approval.
- All computer systems are equipped with MS security, antivirus and malware software.
- All logins onto computer systems are logged and monitored by the ICT Manager.
- Internet access are routed through WatchGuard firewall solutions, which
    - filters some traffic (blocks unauthorised traffic); and
    - monitors and logs all internet traffic.
- Remote access to computer and network system is by request only
    - completed via VDI (virtual computer) solution;
    - user accesses via remote desktop protocol/software; and
    - access to the desktop to be requested directly to IT department, is enabled and disabled for period required.

User Accounts

- User accounts are created and deactivated upon request from various departments, additionally;
- Students
    - Listing of all student accounts is compiled and sent to the Academic Dean for review every 3-6 months.
    - All deactivated students are deleted from system once every ~12 months.
    - Every 3-6 months' students that have not logged on for more than 180 days are disabled.
- Staff
    - Staff accounts are deactivated upon exit protocol or notification from individual supervisors.
    - Every 12 months, staff files and emails are archived, off the network servers.
- Accounts in other services
    - Papercut - accounts are purged when user limits are reached ~12-24 months (as the system may have paid credits, some student return and move from school to school);
    - Library system - users/patron from the system will be removed from system after 3 years of inactivity; and
    - Moodle
- Accounts are deactivated upon request from EMT members or other key staff.

Email systems

- All emails are filtered using WatchGuard firewall email subscription based filtration and quarantine service
- Suspicious emails require manual intervention to be released

Other services

- Web servers are hosted independently on external services and not linked to internal systems.
- The Institute student administration system (Paradigm EMS) hosted service is managed by Head of Marketing & Student Experience

Back up

- A full testing of backup is conducted quarterly.
- The servers are backed up on daily basis and stored on a backup disk.
- The backup disks are kept by the President and CEO on a secure location off campus.

- In the event of IT failures, the backup disk will be used to restore the systems in the following order:
  - The network drive which contains working documents for all departments
  - The student management system
  - The finance accounting process system
  - The library database system

Significant Staff Unavailability
Responsible Officer: President and CEO; EMT

4.23 The Institute's employees are the key to delivering Institute's services.

4.24 The EMT manage the risk of inability to maintain processes due to insufficient staff numbers by ensuring that:

- Each role within OIHE has a defined list of tasks with the key roles and responsibilities documented. The role is part of a team which enables back filing of any absence.
- The tasks are reviewed on annual basis at the annual performance review.
- Staff ensure that all records are maintained on the Institute's system and are accessible by the team that the staff member belongs to.

5. QUALITY ASSURANCE

To ensure that this policy is fit for purpose and meet the requirements of the HES Threshold Standards the policy will be;

5.1 internally endorsed by the Executive Management Team on development or review, prior to approval by Governing Board, or the Academic Board or other delegated authority;

5.2 externally reviewed as part of any independent review of the HES Threshold Standards approved by the Governing Board;

5.3 internally reviewed by the Responsible Officer every three years from the date of approval (if not earlier).

5.4 referenced to the applicable HES threshold Standard and/or other legislation/regulation.

6. FEEDBACK

Feedback or comments on this policy is welcomed by the listed Responsible officers of the Institute.

7. ACKNOWLEDGEMENT

This policy was developed with reference to the following:

- Melbourne University, Risk Management Policy, 2022 (Risk Management Policy (unimelb.edu.au))

- The University of Adelaide, Business Continuity Policy 2019 (Microsoft Word - D2019 85887 Business Continuity Policy - approved by Chief Operating Officer - 17 April 2019 - refer d2019 85 (adelaide.edu.au))
- The University of Newcastle, Business Continuity Management policy 2019 (Business Continuity Management Policy / Document / UON Policy Library / The University of Newcastle, Australia)

8. VERSION CONTROL

Version	**Date approved**	**Description**	**Approved by**
1.0	April 2014	Initial issue	ARC/GB
2.0	February 2015	Internal review	ARC/GB
3.0	February 2016	Internal review	ARC/GB
4.0	September 2018	Internal Review	ARC/GB
4.1	November 2021	Internal Review, minor editorial amendments	ARC/GB
4.2	July 2023	Internal Review	ARC/GB
4.3	September 2023	Internal review – minor formatting changes and add external referencing	EMT
Related legislation/ regulation/standard	Tertiary Education Quality and Standards Act 2011 Higher Education Standards Framework (Threshold Standards) 2021 Education Services for Overseas Students Act (ESOS) 2000 Education Services for Overseas Students Regulations 2019 The National Code of Practice for Providers of Education and Training to Overseas Students 2018 Standards 6 and 11		

Notes:

ARC = Audit and Risk Committee

GB = Governing Board

EMT = Executive Management Team