

Business Continuity Plan

Approving body	Governing Board (GB)
Date approved	17 August 2026
Date of effect	Commencement of operation
Next scheduled review	One year from when plan commences
Policy owner	Chief Executive Officer (CEO)
Policy contact	Chief Executive Officer (CEO)
Related Documents	Critical Incident and Emergency Management Policy and Procedure Health and Safety Policy and Procedure Risk Management Framework Risk Management Plan Risk Register Staff Code of Conduct Student Support Framework Course Discontinuation and Teach-Out Policy and Procedure
Related Legislative and Regulatory Instruments	Higher Education Standards Framework (Threshold Standards) 2021 (Cth) (HESF 2021) Tertiary Education Quality and Standards Agency Act 2011 (Cth) (TEQSA Act) Australian Qualifications Framework (AQF) Education Services for Overseas Students Act 2000 (Cth) (ESOS Act) Education Services for Overseas Students Regulations 2019 (Cth) National Code of Practice for Providers of Education and Training to Overseas Students 2018 (Cth)



ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

Business Continuity Plan

Approved by the Governing Board on 17 August 2026



ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

Business Continuity Plan

Executive Summary	4
Principles	4
Approach	4
Plan	5
Prepare	6
Respond	7
Recover	9
Monitoring	9
Improvement	10
Reporting, compliance and review	10
Responsibilities	10
Definitions	12
Schedule 1 – Business impact analysis	13
Schedule 2 – Preparedness schedules	18
Schedule 3 – Response	22
Schedule 4 – Recovery	26
Version history	Error! Bookmark not defined.

Executive Summary

The Business Continuity Plan sets Zenith Innovation Institute's (**Zenith / ZII / the Institute**) approach to business continuity management, to identify, assess, prevent and mitigate possible disruptions to the Institute's operations and to safeguard against disruptions from having adverse effects on students, staff and other Institute stakeholders.

The Business Continuity Plan covers processes and systems focussed on managing risks to business continuity and facilitating a return to normal operations. This Plan is to be read in conjunction with other documents which provide guidance for the management of impact of critical incidents on student wellbeing and safety or emergencies. For more information on policies and processes for student wellbeing and safety, refer to the *Institute's Critical Incident and Emergency Management Policy and Procedure, Health and Safety Policy and Procedure, ICT and Cybersecurity Management Policy and Procedure, Fraud Prevention Policy and Procedure, Financial Management Policy and Procedure, AI Framework, Assessment Guidelines Course Quality Assurance and Student Support Framework*.

In the unlikely event that the Institute is unable to deliver courses as expected, refer to tuition safeguards in the Institute's *Course Discontinuation and Teach Out Policy and Procedure*.

Principles

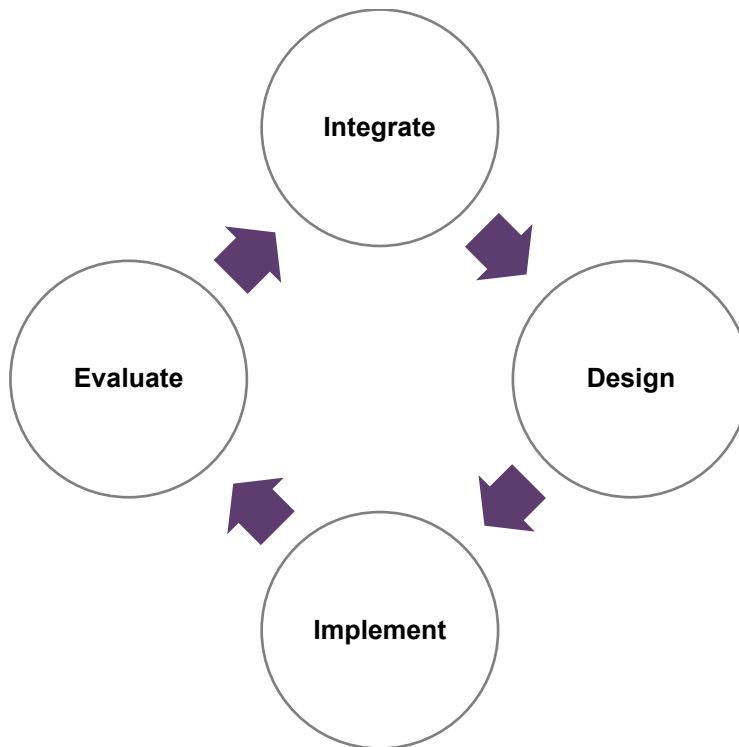
The Institute is committed to managing risks associated with business disruption, system failures, and damage to facilities and equipment. The Institute will implement appropriate processes and systems for:

- as far as possible, preventing the occurrence of disruptive incidents;
- facilitating continued delivery of critical business activities;
- mitigating the impact of disruptive incidents; and
- facilitating return to normal operations.

Approach

The Institute adopts a risk-based approach to business continuity management, placing students' interests at the centre of its processes, and embedding business continuity requirements and processes in day-to-day activities. Business continuity management follows an Integrate – Design – Implement – Evaluate model (adopted also as part of the Institute's *Quality Assurance Framework and Risk Management Framework*).

Figure 1 – Risk Management Framework adapted from the International Organisation for Standardisation (ISO), Risk Management – Guidelines (ISO 31000:2018)



The Governing Board (GB) is responsible for ensuring the sound and prudent management of the Institute's affairs, which it has delegated to the Chief Executive Officer (CEO), who is supported by the Executive Management Team. The CEO is responsible for coordinating the Institute's business continuity management activities according to six stages described below.

Figure 2 | Stages of Business Continuity Management



Plan

The CEO will coordinate the planning stage of business continuity management and confirm that planning activities undertaken in consultation with the Institute's operations demonstrate or include:

- understanding of the context of the Institute;
- understanding of the needs and interests of students, regulatory requirements, and stakeholders and community expectations;
- delineation of the scope of business continuity management;
- definition of organisational roles, responsibilities and authority for business continuity management;
- risk assessment;
- identification of critical business activities;
- business impact analysis (refer to Schedule 1 below);

- strategies for the recovery of critical business activities;
- determination of resource requirements; and
- determination of required communication protocols in the event of a disruption.

The Institute's key risk assessments are contained in the Institute's *Risk Management Plan and Risk Register*.

- The CEO will maintain an understanding of current threats to business continuity in the sector and in the context of the Institute's operations. These include but are not limited to:
- IT system failures, cybersecurity threats, malware, ransomware
- Pandemics and
- environmental events.

Prepare

- a) The CEO will confirm that the Institute is adequately prepared to respond and recover from business disruptions, including:
- b) demonstration of commitment from leadership and management with respect to business continuity management;
- c) availability, competence, and adequacy of resources for the delivery of business continuity processes;
- d) awareness of staff, students and other stakeholders of the Institute's business continuity arrangements;
- e) regular exercise and testing of the Plan, including particular response and recovery plans and adequacy of suppliers' own business continuity arrangements.
- f) Plans and schedules for preparedness are provided at Schedule 2 below.
- g) Officers responsible for recovery plans must ensure readiness of plans at all times and promptly report any issue to the CEO.
- h) Testing of the Plan will ascertain that:
 - critical business activities have been identified
 - recovery plans are in place
 - recovery strategies are appropriate
 - documentation for the Plan is current
 - recovery time objectives have been established and
 - testing of the Plan has been completed during the previous two years and that recommendations arising from the post-implementation review have been implemented under the CEO's supervision and are effective.
- i) The CEO is supported in preparedness activities by the Executive Management Team (EMT). Each EMT member is responsible for maintaining the readiness of recovery plans within their area of responsibility and for ensuring that relevant staff within their area are trained and aware of the Institute's business continuity arrangements. EMT members report any issues with plan readiness to the CEO promptly.
- j) The Institute's staff training schedule (Schedule 2) includes all EMT members in crisis management training and business unit recovery plan exercises. Training frequency and outcomes are reviewed annually by the CEO.

Respond

- a) The CEO will coordinate the Institute's response to a disruption, including:
 - assessment of the disruption
 - confirmation and communication of the activation by the CEO of the institutional response to a disruption
 - coordination of the immediate response by the Institute for containing, controlling and minimising impact on critical business activities and other functions and
 - coordination of communication with students, regulators, and other stakeholders.

Executive Management Team — Response Roles

1. Upon activation of the institutional response, the CEO immediately convenes the Executive Management Team (EMT). The EMT operates as a collegiate decision-making body throughout the response and recovery phases, with each member accountable for their specialist area:
 - (a) Incident Controller (CEO) — overall coordination of the response; authorisation of escalation decisions; communications with the Governing Board, TEQSA, and other regulatory bodies; and declaration of return to normal operations;
 - (b) Operations Officer (Academic Dean) — management of academic continuity, including alternative delivery modes, assessment adjustments, student academic notifications, and coordination with teaching staff;
 - (c) Student Welfare Officer (Student Services Manager, coordinating with the Wellbeing Officer and Student Support Officers) — coordination of student welfare checks, referrals to external support services, communications with at-risk students, and management of student continuation arrangements;
 - (d) IT/LMS Support Officer (designated by CEO) — management of IT system recovery, LMS continuity, building access, data security, and physical resource continuity. This officer leads the operational response for any incident primarily affecting IT systems, the LMS, or physical facilities; and
 - (e) Marketing Manager (acting as Communications lead, designated by CEO) — management of all internal and external communications, including staff and student notifications, website updates, and media enquiries. The CEO retains responsibility for all communications with TEQSA, other regulatory bodies, and the Governing Board, supported by the Quality Assurance Manager in preparing regulatory correspondence.
 - (f) Finance Officer — management of the financial response, including assessment of the Institute's financial position, determination of short- and medium-term cash requirements, liaison with insurers and financial institutions, and management of unexpected expenditure within delegated limits. Expenditure exceeding the CEO's delegated threshold requires Governing Board monitoring; where urgent, the CEO seeks approval from the Governing Board Chair prior to the next scheduled meeting.

Severity Assessment and Resource Prioritisation

2. On receipt of a disruption notification, the CEO and relevant EMT members assess the severity of the disruption before activating a response. The assessment considers the following factors and is documented in the event log:
 - (a) the nature and likely cause of the disruption (e.g. IT failure, facility loss, staff unavailability, regulatory event);
 - (b) which critical business activities are affected, by reference to the prioritisation ratings in Schedule 1 (Critical, High, Medium, Low);

- (c) the estimated duration of disruption compared to the maximum allowable downtime established in the Business Impact Analysis;
 - (d) the number of students and staff directly affected and the nature of that impact; and
 - (e) financial, reputational, and regulatory implications, including whether TEQSA notification is required.
3. Based on this assessment the CEO classifies the disruption and activates a proportionate response:
- (a) Level 1 — Minor disruption: affects Low or Medium priority activities; estimated recovery within maximum allowable downtime; managed within the affected business unit by the relevant EMT member with CEO oversight; no student impact.
 - (b) Level 2 — Significant disruption: affects one or more High priority activities, or a Critical activity within its recovery window; EMT convenes; recovery plans activated; proactive student and stakeholder communications initiated.
 - (c) Level 3 — Major disruption: affects one or more Critical activities beyond the maximum allowable downtime, or threatens the Institute's ability to deliver its courses or meet regulatory obligations; full EMT activation; Governing Board notified; TEQSA notification assessed; student continuation options activated.
4. Resource prioritisation follows the criticality ratings in Schedule 1. In a Level 2 or Level 3 disruption, Critical-rated activities are resourced first, followed by High-rated activities. The CEO, advised by the relevant EMT member, determines specific resource allocation decisions and documents these in the event log.

Student Continuation of Studies

5. Where a disruption affects students' ability to continue their studies at the Institute, the Student Welfare Officer, in consultation with the CEO, takes the following steps:
- (a) within 24 hours of a Level 2 or Level 3 disruption being declared, identify all students whose studies are affected and the nature and likely duration of that impact;
 - (b) assess whether affected students can continue their studies at the Institute through alternative delivery arrangements (refer to Schedule 4 — Recovery Plans);
 - (c) where students cannot continue at the Institute, identify available options for continuing their studies at another registered provider, in consultation with the Tuition Protection Service and in accordance with the Institute's Course Discontinuation and Teach Out Policy and Procedure;
 - (d) communicate individually with each affected student, in plain language, setting out their options, the Institute's obligations to them, and the next steps and timeline;
 - (e) for international students, advise individually of any implications for their student visa arising from the disruption and liaise with PRISMS to update CoE records as required; and
 - (f) maintain a register of all affected students, the options communicated to them, and the outcomes, which is reported to the CEO and Governing Board as part of the post-implementation review.
- b) Institutional response guidelines are provided at Schedule 3.
- c) The CEO is responsible for
- all communications with TEQSA, other regulatory agencies, and the media, supported by the Quality Assurance Manager in preparing regulatory correspondence.
 - ensuring communications with students.

- ensuring, as far as possible, that students have continued access to adequate support services throughout the disruption.
- d) Other communications, e.g. with suppliers, are handled in accordance with functional responsibilities or as indicated in recovery plans.

Recover

The CEO will coordinate the Institute's recovery from a disruption, including:

- prioritisation of resources required for critical business activities
 - assessing the Institute's financial situation
 - determining short-term and medium-term cash requirements, noting that unexpected expenditure exceeding \$10,000 requires Governing Board monitoring in accordance with financial delegations
 - as required, temporary deactivation of other resources
 - adjustment of recovery plans to the circumstances
 - liaising with third parties for recovery, such as insurers and financial institutions, with the Finance Officer managing operational financial matters within their delegated authority
 - implementation and closure of plans and
 - communication with students, staff, and other stakeholders on recovery progress.
6. Recovery is coordinated by the CEO with each EMT member managing recovery within their specialist area. The Academic Dean oversees restoration of academic delivery and communicates progress to students. The IT/LMS Support Officer oversees systems, LMS, and facilities recovery and escalates unresolved issues to the CEO. The Student Welfare Officer continues to monitor the welfare of affected students and manages ongoing student continuation arrangements throughout the recovery period.
7. The CEO reviews resource prioritisation at regular intervals during recovery, adjusting the allocation of staff, financial resources, and supplier support to reflect the evolving status of critical business activities. Any significant reallocation of resources is documented in the event log and reported to the Governing Board.
-

The Institute's recovery plans are provided at Schedule 4.

Monitoring

- a) The CEO will coordinate the collection, analysis, and reporting of data on business continuity management, including response and recovery performance, and student experience.

The Institute uses the collected data to monitor trends and emerging issues and will improve its processes for managing business disruptions based on the collected data.

- b) The Institute will benchmark its performance against relevant sector data and will establish targets as appropriate
- c) The Governing Board receives a post-implementation review report for each activation of an institutional response under this Plan and an annual report on the adequacy and effectiveness of its business continuity management processes as part of self-assurance and continuous improvement.

Improvement

The CEO will coordinate the Institute's processes for review and implements relevant improvement measures following a disruption, including:

- recording events throughout response and recovery stages
- conducting a post-implementation review
- analysing data on student and stakeholder experience of the disruption
- benchmarking response and recovery performance against relevant internal and external metrics and
- reporting to relevant governing bodies for review, corrective action, and improvement.

Reporting, compliance and review

The Institute is required to notify the Tertiary Education Quality and Standards Agency (TEQSA) if an event occurs or is likely to occur that will significantly affect the Institute's ability to meet the *Higher Education Standards Framework (Threshold Standards) 2021*. The notification will be given no later than 14 days after the day that the Institute would reasonably be expected to have become aware of the event.

In particular, the Institute will notify TEQSA of changes that may impact on its financial viability, such as events that may have a significant impact on its ability to continue operating, and of changes that may impact on students, such as critical incidents and other material breaches in safety.

This Plan will be reviewed annually by the Audit and Risk Committee and every two years by the GB.

Responsibilities

The GB is responsible for overseeing the implementation of effective business continuity management processes.

The CEO is responsible for:

- implementing the Institute's business continuity management processes in accordance with this Plan
- liaising with the Executive Management Team
- activating the Institutional response to a disruption
- formally closing recovery plans and declaring the Institute's return to normal operations
- reporting to the GB on the implementation of the any recovery plans and
- escalating any material issue or incident to the GB in a timely manner.

In addition, the CEO is responsible for overseeing and ensuring or facilitating:

- communications with students
- as far as possible, maintaining adequate student support services in the event of a disruption to the Institute's operations and access to these services.

8. The Executive Management Team (EMT) is collectively responsible for:

- (a) responding within their specialist area upon activation of the BCP;
- (b) providing specialist expertise to the CEO to inform severity assessment, response decisions, and resource prioritisation — for example, the IT/LMS Support Officer leads the operational response to IT system failures, LMS outages, and cybersecurity incidents;

- (c) maintaining the currency and tested readiness of their area's recovery plans at all times;
 - (d) reporting recovery progress to the CEO at each EMT meeting during the incident; and
 - (e) contributing to the post-implementation review following each BCP activation.
9. The CEO prepares an annual self-assurance report on the adequacy and effectiveness of the Institute's business continuity management, including any activations during the year, response and recovery performance data, identified risks, and improvement actions. This report is presented to the Governing Board and supports the Governing Board's annual review of the Plan.

Definitions

Term	Definition
Business continuity	is the capability of the Institute to continue delivery of services at acceptable levels following disruptive incidents.
Business continuity management	is a management process that identifies potential threats to the Institute and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its stakeholders and its reputation.
Business continuity plan	A set of documented procedures that guide the Institute to respond, recover, resume, and restore to a pre-defined level of operation following disruption, covering resources, services and activities required to ensure the continuity of critical business activities.
Business impact analysis	is the process of analysing activities and the effect that a business disruption might have.
Critical business activities	are those activities essential to deliver outputs and achievement of business objectives.
Recovery Time Objective (RTO)	The period of time following an incident within which services or specific business activities must be resumed and resources recovered.

Schedule 1 – Business impact analysis

Current as at: 21/03/2024

Responsible Officer (Coordination): CEO

1. Prioritisation of business activities

Function	Responsibility	Process	Priority
Human Resource Management	CEO	Hiring of staff	Medium
		Staff Development	Low
		Training	Low
		Payroll	High
		WHS	Medium
Admissions	Marketing Manager	Issuance of Confirmation of Enrolment	High
		Non-compliance with any legislative requirements or changes in legislative requirements	High
		Student Grievance	Medium
		Enrolment	Critical
		Orientation	High
Academic quality and delivery	Academic Dean	Course Review	Medium
		Non compliance with regulatory or professional standards	High
		Subject Review	Medium
		Moderation	High
		Subject Selection	Critical
		Exam or Assessment Preparation (e.g. breaches)	High
		Timetabling	High
		At-Risk Students	High



Function	Responsibility	Process	Priority
		High levels of or a pattern of academic misconduct e.g. inappropriate use of GenAI	High
		Academic Management System	Critical
		Academic Staff Management	Medium
		Course delivery	Critical
Finance Management	Finance Manager	Budgeting	High
		Payroll	High
		Reporting of financial management	High
		Cost Control	Low
		Accounts Payable	High
		Accounts Receivable	High
		Disbursements	High
		Fees and refunds	Critical
		Unauthorised access to or use of financial information, including cybersecurity breaches	Critical
		Fraud	Critical
Facilities Management & IT	IT Manager	Infrastructure	High
		Premises	Critical
		Fixed Assets	High
		Systems Maintenance	High
		Unauthorised use of information including cybersecurity breaches	Critical
Administration	Registrar	Reception	High
		Filing	Medium



Function	Responsibility	Process	Priority
		Data Entry	Medium
		Unauthorised access to information including cybersecurity breaches	Critical
Student Support Services	Student Services Manager	Counselling and other support services	Critical
		Study Skills	Critical
		Any Critical Incidents under the Critical Incident and Emergency Management Policy and Procedure	Critical
Library	Librarian	Cataloguing	Medium
		Library System (e.g. access, discontinuation of supplier)	Critical
Marketing	Marketing Manager	Education agent management and review	Medium
		Education agent breaches	Critical
		Career expos	Low
		Open Days	Medium
		PRISMS	Critical
Strategic Management & Planning	CEO	Succession Planning	Low
		Training	Low
		Business Plans	High
		Governance	High
		Compliance and self-assurance	High
		Articulations	Medium

2. Impact analysis

Function	Critical Business Activity	Impact	Maximum Allowable Downtime	Required Resources
Student Administration	Admission application processing	Lower student numbers	20 days (non-peak) 10 days (peak)	Website Application portal
Student Administration	Enrolment and fee payment	Decline in student intake Delayed revenue resulting in reduced cash flow	20 days (non-peak) 10 days (peak)	Student Management System
Academic	Delivery of units	Decline in student intake Course discontinuation Cancellation of accreditation/registration/ professional bodies	10 days	Classrooms Lecturers
Academic	Provision of Learning Management System Provision of learning resources	Disruption to current students' ability to access learning materials, submit assessments, and track their academic progress, with consequent risk to course completion and, for international students, visa compliance. Decline in future student intake if disruption is prolonged or publicly known. Risk to assessment integrity and academic record currency.	10 days	Learning Management System Learning resources Learning Support staff
Academic	Conducting assessments and examinations, including marking	Decline in student intake	10 days (non-peak) 5 days (peak)	Assessors Invigilators



ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

		Cancellation of accreditation/registration		Examination hall Examination scripts
Student Services	Recordkeeping of student progression and completion	Decline in student intake Cancellation of accreditation/registration	10 days	Student Management System Staff for data entry
Student Services	Provision of student services, including support services	Decline in student intake Cancellation of accreditation/registration	10 days	Student Services staff Learning support

Schedule 2– Preparedness schedules

1. Business Continuity Distribution List

Current as at: 01/02/2025

List owner: CEO

Institute staff listed below are in possession of a hard copy of the latest version of the Business Continuity Plan.

Copy Number	Role	Location
001	CEO	Campus
002	Academic Dean	Campus
003	XX	TBA
004	XX	TBA
005		TBA

2. Staff Training Schedule

Current as at: 01/02/2025

Responsible Officer: CEO

Training	Frequency	Training Date	Staff	Outcome	Comments
Crisis Management and BCP Activation	Annually	TBA	CEO and all EMT members (Academic Dean, Registrar/Student Services Manager, IT/LMS Support Officer, Marketing Manager (Communications lead))	TBA	TBA
Business unit recovery plans	Annually	TBA	All staff required for critical business activities	TBA	TBA

3. IT Exercise and Testing Schedule

Current as at: 01/02/2025

Responsible Officer: Academic Dean

Exercise / Test	Frequency	Date	Outcomes	Actions
Major operational disruption	Every two years	TBA	TBA	TBA
Major operational disruption and penetration exercise (desktop)	Annually	TBA	TBA	TBA
IT systems recovery	Annually	TBA	TBA	TBA

4. IT Systems schedule

4.1 IT systems preparedness

- (a) Assessments of threats and vulnerabilities of the Institute's IT systems are conducted regularly by appropriately qualified personnel, based on a current understanding of known risks to higher education providers in Australia. Controls relating to IT systems are implemented by Institute staff or required from students and third-party suppliers and include:
- (i) awareness and training
 - (ii) identity management and access control
 - (iii) protective technologies
 - (iv) prioritisation of recovery of critical IT systems
 - (v) cloud security requirements
 - (vi) data security measures
 - (vii) back-up strategy and definition of required scope, frequency, methodology, location, and testing of back-ups
 - (viii) IT systems and network change management and
 - (ix) detection of cyber events.

The IT Systems schedule includes:

Current as at: 01/02/2025

Responsible Officer (Coordination): CEO.

IT System	Security	Data back-up	Agreement Expiry Date	Supplier contact	Responsible Officer
Student Management System	TBA	TBA	TBA	MeshEd Yordan Kiranov 0451233543	TBA
Learning Management System	TBA	TBA	TBA	NeXus Business Technology Mike Tse 02 9238 2290	TBA
Website	TBA	TBA	TBA	NeXus Business Technology Mike Tse 02 9238 2290	TBA
Intranet	TBA	TBA	TBA	TBA	TBA
Personal and Shared drives	TBA	TBA	TBA	TBA	TBA
Applications and software	TBA	TBA	TBA	TBA	TBA
Accounting Management System	TBA	TBA	TBA	MYOB 1800 836 226	TBA
Library resources and subscriptions	TBA	TBA	TBA	Softlink +64 9887 3113	TBA
IT equipment	TBA	TBA	TBA	NeXus Business Technology Mike Tse 02 9238 2290	TBA

5. Emergency Evacuation Drill and Preparedness

A member of the Critical Incident Team will be designated Chief Warden and be responsible for developing and maintaining the Critical Incidents and Emergency Policy and Procedure with the CEO. The Chief Warden will work in conjunction with emergency services where applicable.

Building evacuation drills will be conducted annually. Drills will ensure the building is prepared and ready to undergo an evacuation. Additional periodic drills and tests may be required to ensure proper readiness of emergency response mechanisms.

A space will be designated as an assembly space for drills and emergencies. The designated assembly space will be a safe and easily accessible space removed from potential hazards.

Each building will be equipped with evacuation diagrams. Building occupants should familiarise themselves with the contents of these diagrams for buildings they enter and as part of inductions.

Evacuation diagrams will contain information on exit pathways, emergency assembly areas, evacuation procedures, and the location of firefighting and first aid equipment.

Current as at: 01/02/2025

Exercise / Test	Frequency	Date	Outcomes	Actions
Test of the Emergency Evacuation Alarm	Annually	TBA	TBA	TBA
Test of Fire Alarms	Annually	TBA	TBA	TBA
Test of Smoke Alarms	Annually	TBA	TBA	TBA
Emergency evacuation drill	Six-monthly			

Schedule 3 – Response

1. Immediate response

The following steps are provided as a guide only and may need to be adjusted depending on the circumstances.

Phase	Responsibility	Action
Notification	CEO	Notify each EMT member of the disruption and confirm their availability. Notify all staff of the disruption and advise that further information will follow. Confirm event log is being populated by Registrar.
EMT Activation	CEO / EMT	CEO convenes the EMT within 1 hour of notification. Each EMT member confirms readiness and takes ownership of their specialist area: • Academic Dean: academic continuity and student academic communications • Registrar / Student Services Manager: student welfare and continuation • IT/LMS Support Officer: systems and facilities recovery • Marketing Manager (Communications lead): all internal and external communications EMT meets at intervals set by CEO. All decisions recorded in event log.
Recordkeeping	Registrar	■ Populate the event log.
Assessment	CEO / EMT	CEO and relevant EMT member(s) assess the disruption against Schedule 1 criticality ratings. Classify severity level: - Level 1 — Low/Medium activities affected, within downtime tolerance - Level 2 — High activities affected, or Critical within recovery window - Level 3 — Critical activities beyond maximum allowable downtime, or course delivery at risk Document classification and basis in event log. For IT-related incidents, IT/LMS Support Officer leads assessment.



Phase	Responsibility	Action
		For academic delivery incidents, Academic Dean leads assessment. For student welfare incidents, Student Welfare Officer leads assessment.
	CEO	Determine appropriate institutional response.
Activation	CEO	Active institutional response and appropriate recovery plans.
Communication	CEO	- Inform staff and students of the activation of the relevant plans and required actions. - Inform stakeholders as required. - Provide communication protocols to staff and students, i.e. who and when to contact Institute staff and when further information will be available.
Operation	CEO	- Confirm availability and adequacy of alternate site, alternate systems, and other contingencies. - Identify staff and resources for continuity of critical business activities at alternate site. - Notify stakeholders (e.g. building management) of relocation of staff and students.
Student Continuation	CEO / Student Welfare Officer	Within 24 hours of Level 2 or 3 declaration: - Student Welfare Officer identifies all students whose studies are affected. - Assess whether alternative delivery at the Institute is viable (see Schedule 4). - Where students cannot continue at the Institute: - Identify placement options at another registered provider via TPS. - Communicate individually with each affected student (options, obligations, timeline). - For international students: advise on visa implications; update PRISMS CoE records. - For domestic students: advise on TPS entitlements and refund options. - Maintain student continuation register; report to CEO and Governing Board.

2. Contact lists

Current as at: 26/06/2026

Responsible: CEO

Institute	Contact details
CEO	Vivian Lobo +61426 274 014
Academic Dean	Prof Harvinder Singh +61451 957 421
Student Services Manager (International and Domestic Student point of contact)	TBA
Third parties	
Insurer	FTA Insurance
IT supplier	NeXus Business Technology
Bank	Commonwealth Bank
Student Management System	Yordan Kiranov 0451233543
LMS	Mike Tse 02 9238 2290
Accounting Software	MYOB 1800 836 226
Library	Softlink +64 9887 3113

3. Event log template

Responsible Officer: CEO

Phase	Date/Time	Action / Decision / Event
Incident	TBA	
	TBA	



ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

Phase	Date/Time	Action / Decision / Event
Return to normal operations		

Schedule 4 – Recovery

1. Recovery plans

Current as at: 01/02/2025

Responsible Officer (Coordination): CEO

Critical Business Activity	RTO	Resources	Actions	Responsibility
Admission application processing	< 5 days	Staff for processing applications Computers / laptops Mobile phones	■ Alternate site or working from home ■ Implement to paper-based system ■ Implement alternative IT system	Student Services Manager or relevant officer
Enrolment and fee payment	< 5 days	Staff for processing enrolments and payments Computers / laptops Mobile phones	■ Alternate site or working from home ■ Implement to paper-based system ■ Implement alternative payment facility	Student Services Manager or relevant officer in consultation with CEO/ Marketing Manager
Delivery of units	5 days	Lecturers / teaching staff Laptops Projectors Learning Management System Videoconference and streaming software/application	■ Alternate teaching site ■ Group classes ■ Reschedule classes ■ Hold live and recorded classes using digital technology and Learning Management System ■ Hire casual teaching staff	Academic Dean supported by Course Coordinator
Provision of Learning Management System	10 days	Librarian / Learning support staff	■ Arrange for alternate subscriptions ■ Enter into agreement for utilisation of	Dean supported by librarian



Critical Business Activity	RTO	Resources	Actions	Responsibility
			alternate adequate library ■ Implement alternate LMS ■ Implement face-to-face, email, or other online platform as temporary learning system ■ Purchase hard copies of required textbooks ■ Hold additional consultation hours	
Conducting assessments and examinations	5 days	Assessors / Markers Scripts Examination hall or suitable venue Videoconference software/application	■ Hire casual assessors, markers or invigilators ■ Rent venue suitable for examination ■ Hold online examinations ■ Arrange for secure handling and printing of examination scripts at external location	Dean supported by Course Coordinator
Recordkeeping of student progression and completion	5 days	Staff for collecting and recording student information	■ Implement manual recordkeeping system ■ Arrange for alternate information systems	Student Services Manager
Provision of student support services	5 days	Staff for referring students to services	■ Arrange alternate support services with external providers	Student Services Manager
Student continuation of studies	Ongoing from activation	Student Welfare Officer Supervisory contact list	Identify affected students and assess ability to continue at Institute.	Student Welfare Officer in consultation with CEO



ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

Critical Business Activity	RTO	Resources	Actions	Responsibility
		TPS contact: administrator@a.tps. gov.au / 1300 980 434 PRISMS access	Activate alternative delivery for students who can continue. For students who cannot continue: • Contact TPS to initiate placement process • Issue individual student communications • Update PRISMS for international students • Process refunds / loan re-credits for domestic students as applicable Maintain continuation register; update Governing Board.	

Version History

Version	Changes	Approval Body	Approval Date
1.0	New Policy	Governing Board (GB)	21 Mar 24
1.1	In Executive Summary added “<i>ICT and Cybersecurity Management Policy and Procedure, Fraud Prevention Policy and Procedure, Financial Management Policy and Procedure, AI Framework, Assessment Guidelines Course Quality Assurance</i>” Added additional standards Standard 1.1; Standard 1.2; Standard 2.2; Standard 2.3; Standard 2.4; Standard 5.3.7; Standard 7.1; Standard 7.2; Standard 7.3 Schedule 1 updated Table to have Responsibility Column Under Finance Management added “Unauthorised access to or use of financial information, including cybersecurity breaches; Fraud Under Facilities Management and IT added “Unauthorised use of information including cybersecurity breaches” Under Administration added “Unauthorised access to information including cybersecurity breaches” Under Student Services added “Any Critical Incidents under the Critical Incident and Emergency Management Policy and Procedure” Contact Lists updated	Governing Board (GB)	
1.3	Updated contact list for IT supplier and LMS contact Updated contact for IT, LMS and Website in point 4.1	Governing Board (GB)	27 Feb 2025
V1.4	Added EMT roles and responsibilities (HESF s.6.2.1(i)), student continuation and TPS obligations, and BIA separation provisions. Updated from V1.3. Added EMT roles and responsibilities (HESF s.6.2.1(i)), student continuation and TPS obligations, and BIA separation provisions. Updated from V1.3.	Governing Board	
1.5	TEQSA finding a(i)/(ii) — EMT role not described beyond notification; responsibility concentrated in CEO. Integrated EMT roles into Prepare, Respond, Recover, and Responsibilities sections. Each EMT member now has defined responsibilities throughout the BCP lifecycle, not merely at notification. Severity assessment and resource prioritisation framework added to Respond section (Level 1/2/3 classification	Governing Board	17 August 2026



Version	Changes	Approval Body	Approval Date
	with specialist EMT leads by incident type). Schedule 3 response table restructured: Notification row updated; EMT Activation row added with specific accountabilities per role; Assessment row updated to show specialist-led triage by incident type. Schedule 2 staff training updated to include all EMT members in annual crisis management training. TEQSA finding a(iii) — LMS impact limited to ‘decline in student intake’. Schedule 1 Impact Analysis updated: LMS/learning resources impact now describes disruption to current students’ ability to access materials, submit assessments, and track academic progress; risk to course completion and international student visa compliance; and risk to assessment integrity. These impacts correctly reflect that inaccessibility harms enrolled students, not only future intake. In addition the maximum allowable time has changed from 20 days to 10 days. TEQSA finding b) — no options for students to continue at another provider. Respond section now includes a dedicated ‘Student Continuation of Studies’ subsection with a step-by-step procedure: identifying affected students within 24 hours; assessing alternative delivery at the Institute; where students cannot continue, initiating TPS placement; individual student communications covering options and obligations; PRISMS updates for international students; and maintaining a continuation register for Governing Board reporting. Schedule 3 Student Continuation row added with domestic and international pathways distinguished. Schedule 4 student continuation recovery row added. Delegations alignment — cross-checked all BCP roles and responsibilities against the Delegations Policy and Schedule V1.6. Six misalignments corrected: (1) ‘IT and Facilities Officer’ renamed to ‘IT/LMS Support Officer’ throughout to match the established position title in the Delegations Schedule; (2) ‘Communications Officer’ (an invented role with no delegation basis) replaced with ‘Marketing Manager (acting as Communications lead)’ consistent with the Marketing Manager’s established communications authority in the Delegations Schedule; (3) CEO regulatory communications updated to reference Quality Assurance Manager support role per Operational Delegations; (4) Finance Officer added as a named EMT member for financial recovery, consistent with the EMT Operational Delegations row in the Delegations Schedule; (5) Registrar / Student Welfare Officer role clarified to reflect that Student Services Manager coordinates Wellbeing Officer and Student Support Officers in a BCP event, consistent with their respective delegated		



ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

Version	Changes	Approval Body	Approval Date
	positions; (6) Recover section updated to reference the \$10,000 unexpected expenditure threshold requiring Governing Board monitoring, consistent with Financial Delegations.		