Critical Incident, Emergency Planning and Business Continuity Procedure

Section 1 - Summary

(1) This Procedure states how Victoria University (VU) will manage critical incidents, emergency planning and business continuity.

Section 2 - Scope

(2) All staff.

Section 3 - Policy/Regulation

(3) See Critical Incident, Emergency Planning and Business Continuity Policy.

Section 4 - Procedures

Part A - Summary of Roles and Responsibilities

Roles	Responsibilities
Vice-Chancellor / Senior Vice-President and Chief Operating Officer	Provides strategic direction in consultation with relevant bodies and apprises the University Council. The public spokesperson for the University. Ensure the continuing strategic purpose of the University is met during a disruption and through recovery.
Chief People Officer University Incident Controller (UIC)	Lead and manage the Critical Incident Team (CIT) and program. Provide subject matter expertise for critical incident/business continuity management and response for the University. Declare a critical incident and manage the University's response.
Chief Student Officer (Deputy UIC)	Responsible for student services, support, communications and engagement, including the wellbeing and welfare procedures relating to all students, the Safety and Triage Team and learning and teaching support areas such as Libraries and lab-based Technical Services. Is the Deputy Incident Controller and will assume the role of the University Incident Controller as required.
Interim Deputy Provost (Students & Academic Services)	Responsible for leading the implementation of a variety of initiatives related to technology enhanced learning and teaching, block model initiatives, academic and quality standards, student support services, enhancement and management, and access to higher education.
Deputy Vice-Chancellor Enterprise and Digital	Responsible for Facilities, Information and Technology Services, including University Security and systems to detect, respond and report on incidents impacting VU communities.

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Victoria University's Policy Library for the latest version.

Senior Vice-President and Chief Operating Officer	Responsible for key supporting and enabling services that manage institutional resources, including Finance, Infrastructure and People and Culture. Responsible for managing, reporting and providing financial approval in managing of the critical incident to maintain business needs.
Chief TAFE Officer	Responsible for the delivery of VU's Vocational programs, overseeing the delivery of all VET programs, as well as commercial operations and learning, quality and support functions.
Senior Vice-President and Deputy Vice-Chancellor, Global (Interim)	Responsible for leading strategy and operations on a number of critical internal and external-facing functions in local and global contexts, including marketing and communications, transnational education programs, international student mobility programs, Victoria University Sydney, and new ventures opportunity development.

Section 5 - Procedures

(4) The UIC may delegate some or all management functions of incident control - planning, intelligence/public information, operations, logistics and finance as the incident or critical incidents escalate in size or complexity.

(5) The CIT will:

a. Seek advice from the Office of the General Counsel about any statutory obligations or external reporting obligations arising from a critical incident.
b. Ensure that stakeholders and regulatory bodies, including but not limited to, the Tertiary Education Quality Standards Agency, Work Safe Victoria and the University's insurer are notified in a timely manner and provided with appropriate information.
c. Enlist Subject matter experts within the University to:
    i. assist with the response as required;
    ii. implement any operational guidelines relating to a specific incident type, e.g. international student incidents, off-shore incidents or national/international disasters.

(6) Each nominated key decision-making member of the CIT has delegated powers for operational decisions made within the scope of their specific role. Such decisions must always place primary importance on the impact on the VU community. These decisions must also be consistent with the purpose, values and objectives of the University.

(7) Predefined members of the CIT will be trained for their roles and responsibilities. It is their responsibility to ensure staff within their business units are aware of their responsibilities. The CIT delegates will ensure the continuity of the team in a prolonged incident.

(8) In the event that an emergency or incident results in a critical incident being proclaimed (or not).

a. If onshore, the Chief Warden and Security will manage the matter at a local level and will report to the UIC or designated person for direction.
b. If offshore, the responsible officer will manage the matter at a local level and will escalate the matter to the relevant senior officer and the UIC or designated person for direction.

Activation of Critical Incident Management

(9) The UIC has delegated authority to declare a critical incident and to do all things necessary to manage VU's response and recovery.

(10) The University will respond with appropriate resources arising from a critical incident. The UIC will activate the emergency operations centre as required, convene regular briefings as required for key senior officers and key subject

matter experts. Quick and effective control measures through communication with key stakeholders and the community are required to mitigate against such damage.

(11) The University will maintain a central point from which all critical incidents can be commanded, controlled and coordinated in order to support teams during response and recovery activities. The CIT will identify alternative locations for emergency response operations in the event that the dedicated Emergency Operations Centre is rendered unusable or unsafe.

(12) Any critical incident should be reported and managed through standard procedures via People and Culture for staff matters and safety and triage team for critical incidents relating to students in consultation with University Security.

a. Support services available include but not limited to informing supervisors or academics, student counselling, safer community, welfare, employee assistance program and Police.

(13) All critical incidents that immediately threaten people, assets or University operations must be reported to the University's Security Services who will notify the University Incident, Controller or nominee.

a. Reporting of critical incidents via Quick Safe aims to achieve timely risk assessment and intervention in the line of supervision extending from students or staff to academics or supervisor through to Senior Executive Group.

(14) The UIC has full discretion over the assigned level of response activated.

a. Minor incident, with or without any disruption to critical business service/process: this will be managed and dealt with at the local level. For example (but not limited to):
    i. Minor injury during a lecture or staff meeting
b. Moderate disruption to critical business service/process: the CIT is notified and a response as required. For example (but not limited to):
    i. Equipment malfunction
    ii. Email being compromised
    iii. Mental health concerns
c. Major disruption to critical business service/process: CIT involvement is mandatory. For example (but not limited to):
    i. Loss of a University building
    ii. Loss of University staff due to pandemic (see Pandemic Influenza Preparedness Framework)
    iii. Major Cyber Attack or indiscriminate acts of Violence

(15) The UIC or nominee will coordinate a post-incident operational debrief (within 10 University business days of the incident) to review actions and to ensure lessons learnt are adopted to ensure continuous improvement.

Statements to the media or public

(16) As soon as possible the UIC will liaise with the Communications Team, prepare a critical incident communication plan.

(17) The critical incident communication plan may include but not limited to:

a. Media update
b. Communications to staff and students
c. Liaison with the emergency service media personnel or other regulatory bodies

d. Maintaining documentation for University’s records.

(18) The Vice-Chancellor or delegate may speak for the University in commenting on matters associated with a critical incident. The Vice-Chancellor may authorise members of the CIT or other officers to issue statements to the media.

Business Continuity

(19) Implementation of an appropriate business continuity response is the responsibility of the relevant delegated officer/s and the relevant most senior officer for that area will liaise with the UIC as required.

(20) Relevant senior officers will be responsible for improving the resilience of their respective areas. This includes ensuring that business as usual operations are fit for purpose and able to cope with a range of disruptions. Contingent to after-hours or before-hours contact arrangements provides additional capability and guidance on approved and adaptive courses of action to be initiated during a disruptive incident (Resilience in Crisis).

Emergency Control Organisation Structure

(21) The University's Emergency Control Organisation has been established in accordance with Australian Standard AS 3745 'Planning for Emergencies in Facilities' and provides members with guidance to the planning for, and management of emergency and critical incident situations across all University Premises.

(22) If an emergency is declared, the campus-based emergency structure will implement an appropriate response to emergency situations in accordance with the Site Emergency Response Plan. In the event that the campus emergency generates into a critical incident, the Emergency Control Organisation hierarchy will come into effect and the CIT will manage the critical incident at the local level, liaising with the Emergency Control Organisation.

(23) During an Emergency or emergency exercise, pending the arrival of the Emergency Services, Emergency Control Organisation personnel shall have absolute authority to issue instructions to evacuate all persons from buildings and/or other areas of the University's Premises.

Records

(24) The UIC or delegated person will ensure records are maintained detailing communications, decisions and actions of the CIT for documentation of the University’s response. Each member of the CIT is responsible for ensuring that similar documentation is developed and maintained for their respective portfolios.

(25) VU will take reasonable steps to ensure that the information it handles is protected from misuse, loss, unauthorised access, modification and disclosure. VU's requirements in relation to information technology security are set out in the Information Security Policy, the Records Management Policy and relevant associated procedures.

Section 6 - HESF/ASQA/ESOS Alignment

(26) HESF: Standard 2.3 Wellbeing and Safety; 6.2.1 Corporate Monitoring and Accountability; 7.3.3 Information Management.

(27) Outcome Standards for NVR Registered Training Organisations Instrument 2025: Standard 2.6 Wellbeing. Compliance Standards for NVR Registered Training Organisations and FPP Requirements 2025: Standard 20 Compliance with Laws.

(28) ESOS National Code of Practice 2018: Standard 5 Younger overseas students, 6 Overseas student support services.

Section 7 - Definitions

(29) Business Continuity

(30) Chief Warden

(31) Crisis

(32) Critical Incident

(33) Critical Incident Team

(34) Emergency Operations Centre

(35) Emergency

(36) Emergency Control Organisation

(37) Emergency Planning Committee

(38) Incident

(39) Incident Classification

(40) University Incident Controller

(41) Site Emergency Management Plan

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Victoria University's Policy Library for the latest version.

Status and Details

Status	Current
Effective Date	5th September 2019
Review Date	5th September 2022
Approval Authority	Vice-President, Planning and Registrar
Approval Date	4th September 2019
Expiry Date	Not Applicable
Accountable Officer	Anne Siegers Chief Risk Officer anne.siegers@vu.edu.au
Responsible Officer	Penny Daly Senior Manager Business Resilience & Critical Incidents penny.daly@vu.edu.au
Enquiries Contact	Penny Daly Senior Manager Business Resilience & Critical Incidents penny.daly@vu.edu.au

Glossary Terms and Definitions

"Crisis" - Any emergency or critical incident that is beyond the capacity or the delegated authority of the campus emergency response or business continuity response, to successfully manage, or a series of events that have the potential to seriously damage the University's operations or reputation.

"Critical Incident" - A Critical Incident is a traumatic or tragic event or situation, or the threat of such (within or outside Australia) affecting a student or staff member within the University community, which is of a sufficient size, type or complexity (or has the potential) to require or warrant a coordinated whole of University response. Critical incidents are not limited to but could include: death (including the death of a dependant residing in Australia for an international student) serious injury preventing or severely affecting a student's ability to continue with a course severe verbal or psychological aggression natural disaster domestic violence, sexual assault, drug or alcohol abuse. *Note: a critical incident may involve an emergency or a non-emergency situation such as a business continuity interruption, or a transition between these two situations.

"Emergency Operations Centre" - Is a defined facility which provides members of the Critical Incident Team and essential services staff with the physical and technological resources to effectively fulfil their role to manage an effective response to an emergency or critical incident.

"Emergency" - An emergency is a sudden, unexpected event that requires an immediate response from internal and external emergency services, that threatens the: Health, safety or wellbeing of people. Integrity or loss of infrastructure or other property including the reputation of the University. Environment.

"Emergency Planning Committee" - Committee of persons responsible for the documentation and maintenance of the emergency plan including the establishment and maintenance of the University's Emergency Control Organisation and Critical Incident Response Groups which report to the Critical Incident Team.

"Emergency Control Organisation" - Person or persons appointed by the Emergency Planning Committee to direct and control the implementation of the facilities emergency response procedures.

"Incident" - An incident is any event, occurrence, or circumstances that may give rise to such an event, and that causes or has the potential to cause any of the following: Disruption of the delivery of core University services relating

to research, teaching or learning. Disruption of the delivery of support services provided to the University community. Threaten the reputation of the University, or by implication threatens a loss of brand value. Loss of confidence of partners and other key relationships. Threaten the integrity, availability, or security of data, information and intellectual property. Damage to, or loss of property owned by, or in the control of the University. Loss, accidental or deliberate, of University funds. Adverse financial impacts on third parties arising from the activities of the University. Compliance breach involving legislation, regulation, codes of practice, or University policy.

"Incident Classification" - The University will use a risk based critical incident classification and escalation process in alignment with the University's risk assessment matrix. Critical incidents are classified into three levels of escalation: 1. Minor event - a minor incident or minor injury, with a localised impact on staff, students or visitors and may entail minor property damage. The incident is contained and is unlikely to escalate in severity. It is usually handled by the emergency response team using normal operating procedures. 2. Moderate event - an incident or event, which has a localised impact on University operations and may threaten life or property, or could potentially escalate to a major incident. A moderate event might include death or serious injury. A moderate event may involve the activation of an emergency response and or the Crisis Incident Team (CIT). 3. Major event - an incident or event that has a high impact or imminent severe adverse effect on University operations stemming from an emergency or business continuity failure. This necessitates the activation of the CIT.

"University Incident Controller" - A senior officer appointed by the Vice-Chancellor to lead the Critical Incident Team, and to take overall direction and control of a critical incident.

"Site Emergency Management Plan" - The written documentation of the emergency arrangement for a facility generally made during the planning process. It consists of the preparedness, prevention and response activities and includes the agreed emergency roles, responsibilities, strategies, systems and arrangements.

"Business Continuity " - Capability of the University to continue to the delivery of services at predefined acceptable levels following a disruptive incident to minimise any reputational risk to the University.

"Chief Warden " - A person appointed at each building or campus with the formal authority to control and direct the University's local responses to an Emergency. The Chief Warden is supported by wardens.

"Critical Incident Team" - Responsible for providing executive decisions on University priorities when responding to, recovering and learning from critical incidents.

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Victoria University's Policy Library for the latest version.