POLICY

Title: **Critical Incident and Business Continuity Management**

Policy Owner: **General Counsel and University Secretary, Director Strategic and Governance Services**

Keywords: **Enterprise risk**

Reference: **PL202**

1. INTENT

The purpose of this policy is to establish the principles for the management of all Major or Critical Incidents that have the potential to impact the University, including recovery through business continuity processes.

2. ORGANISATIONAL SCOPE

This policy applies to all members of the University Community and Controlled Entities.

3. DEFINITIONS

Business continuity definitions are consistent with those defined by the International Standard on Business Continuity ISO 22301:2019.

The University Glossary and the following definitions apply to this policy:

Term:	Definition:
Business Continuity	The capability of the University to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.

All printed copies are uncontrolled. For the latest version of this Policy always check the Legislation, Policy and Governance Documents Database

Term:	Definition:
Business Continuity Plan (BCP)	The documented information that guides the University to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.
Business Impact Assessment (BIA)	The process of analysing the impact over time of a disruption on the organisation.
Critical Incident	An event in which University operations have been critically impacted in one or more areas, or poses a significant risk to the continuity of core University-wide operations.
Critical Incident and Business Continuity Management Framework	The Framework comprised of the: a. Critical Incident and Business Continuity Policy; b. Critical Incident and Business Continuity Guidelines; c. Critical Incident Plan; d. Enterprise-Wide Business Continuity Plan; and e. School and Centre Business Continuity Plans And serves the purpose outlined in paragraph 4.1 of this policy.
Critical Incident Management Team (CIMT)	An incident-specific team, formed each time a Critical Incident occurs and remains in place only for the term of the incident.
Major Incident	An event that has had a major impact on the operations of a specific School, Centre, or campus location.
Recovery Director	The individual nominated by the Vice-Chancellor (or delegate) and who is charged with leading the incident management through effective direction and management of the CIMT.
Risk	The effect of uncertainty on objectives, measured in terms of likelihood and consequence. The potential events which may have an impact (positive or negative) on the ability of the University to achieve its strategic, operational, project or activity-based objectives.

4. POLICY CONTENT

General Principles

4.1. The University will maintain a contemporary framework for Critical Incident and Business Continuity management (the Critical Incident and Business Continuity Management

Framework) in accordance with this policy and to ensure that, as far as reasonable and practicable, the University is able to respond to incidents in a way that:

a. minimises and reduces impact on the University's people, the broader community and the environment;

b. mitigates the loss of university assets and operations;

c. protects the University's reputation; and

d. enables a return to business-as-usual as soon as practical.

4.2. The Critical Incident and Business Continuity Management Framework, and other operational documents relevant to the effective management of Critical Incidents and Business Continuity, may be amended, updated and revoked with the approval of the Policy Owner.

Critical Incident Management

4.3. Under the Critical Incident and Business Continuity Management Framework the University will maintain an escalation approach that defines the different categories of incidents, being *Critical Incident*, *Major Incident* and *Significant Incident*, which are defined and further described in the Critical Incident and Business Continuity Management Guidelines (the Guidelines).

4.4. Critical Incidents at the University will be managed by a Recovery Director and a Critical Incident Management Team (CIMT).

4.5. The Vice-Chancellor, or nominated delegate, have authority to deem an incident as being a Critical Incident.

4.6. Once an incident has been deemed to be a Critical Incident, a CIMT must be convened.

4.7. Major Incidents may require Recovery Director and CIMT oversight as determined by the Vice-President Corporate Services or a Deputy Vice-Chancellor, in consultation with Strategic and Governance Services Centre (SGSC).

4.8. All critical incidents, including major incidents where relevant, are required to be the subject of a post-incident review, to be completed in accordance with the Guidelines.

Business Continuity Management

4.9. Business continuity management is guided by an Enterprise-Wide Business Continuity Plan as well as School and Centre Business Continuity Guides.

4.10. The Enterprise-Wide Business Continuity Plan is managed and maintained by SGSC Enterprise Risk. School and Centre Business Continuity Guides are managed and maintained by the respective Schools and Centres and owned by the relevant Executive Dean or Centre Director.

4.11. The Enterprise-Wide Business Continuity Plan applies to all University campuses and is reviewed on an annual basis.

4.12. School and Centre Business Continuity Guides are intended to support the response to Significant Incidents, and are to be:

a. aligned with the University's Enterprise-Wide Business Continuity Plan and Integrated Risk Management Framework;

b. reviewed annually by the School or Centre; and

c. accessible to staff in the School or Centre in the event of an incident.

4.13. In addition to the annual review, testing of the Enterprise-Wide Business Continuity Framework is performed on a biennial basis and also includes testing of the Critical Incident Framework as applicable. The elements of the Enterprise-Wide Business Continuity Plan and/or the School or Centre Business Continuity Guides considered during testing will be determined by the selected scenario.

5. ACCOUNTABILITIES AND RESPONSIBILITIES

The Director Strategic and Governance Services is the Policy Owner and has overall responsibility for the content of this policy and its operation.

The Chief Risk Officer and Manager, Enterprise Risk is responsible for currency of information and provision of advice relating to the operationalisation of this policy.

The Risk and Incident Management Committee (RIMC) provides strategic advice on Critical Incident and Business Continuity matters, including oversight of post-incident reports as per the RIMC Terms of Reference.

The specific roles of critical stakeholders including University Council, the Vice-Chancellor, University Executive and Senior Management are outlined in the Critical Incident and Business Continuity Guidelines.

6. RELATED DOCUMENTS

Policies

Integrated Risk Management Policy

Operational Documents and Resources

Critical Incident and Business Continuity Management Guidelines

Critical Incident Plan

Enterprise-Wide Business Continuity Plan

Integrated Risk Management Guidelines

7. CONTACT INFORMATION

For queries relating to this document please contact:

Policy Owner	General Counsel and University Secretary, Director Strategic and Governance Services
All Enquiries Contact	Chief Risk Officer and Manager, Enterprise Risk
Telephone	(08) 6304 7109
Email address	enterpriserisk@ecu.edu.au

8. APPROVAL HISTORY

Policy approved by	Vice-Chancellor
Date policy first approved	May 2003
Date last modified	15 October 2025
Revision history	February 2007 November 2009 December 2012 December 2015 May 2017 February 2018 (Approved by Policy Owner) February 2020 (Approved by Policy Owner) August 2021: The policy was reviewed in conjunction with PL204 – Business Continuity Management policy. The review removed operational information and ensure the policy was principle-based. Due to the interrelated nature of Critical Incidents and Business Continuity the two policies were combined with PL 204 being rescinded and this policy being renamed to reflect the expanded scope. November 2024 15 October 2025: Update to the branding of the document. Updates to definitions to align with definitions contained in the Critical Incident Management Plan. Updates and additional detail provided within the Business Continuity Management section to ensure policy position aligned with current practice. This included reflecting that the Business Continuity Plan is reviewed on an annual but tested on a biennial basis.
Next revision due:	1 June 2030