Policy Title: Critical Incident and Business Continuity Management

Policy Owner: **Director Strategic and Governance Services Centre**

Keywords: **critical incident, business continuity, enterprise risk**

Policy Code: **PL202**

---

1. INTENT:

The objective of this policy is to establish the principles for the management of all major or critical incidents that have the potential to impact Edith Cowan University (ECU or the University). The policy outlines the University's approach to managing major or critical incidents, 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 *ISO22301:2019*.

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

Term:	Definition:
Business Continuity	The capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.
Business Continuity Plan (BCP)	The documented information that guides an organisation 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.

Term:	Definition:
Critical Incident	A critical incident is an event that poses a significant risk to the continuity of core University-wide operations.
Critical Incident Management Team (CIMT)	The CIMT is an incident-specific team, formed each time a critical incident occurs and remains in place only for the term of the incident.
Major Incident	A major incident is an event that has significantly impacted the operations of a specific School, Centre, or campus location.
Recovery Director	Individual leading the incident management through effective 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 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. The University will maintain an escalation framework that defines the different categories of incidents, being *Critical, Major and Significant*, which are defined and further described in the Critical Incident and Business Continuity Management 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 and the Senior Deputy Vice-Chancellor 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 Critical Incident Management Team (CIMT) must be convened.

4.7. Major incidents may require Recovery Director and CIMT oversight as determined by a member of the University Executive 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. Each School and Centre will maintain a Business Continuity Plan (BCP), owned by the Executive Dean or Centre Director. The plan will be:

a. aligned with the University's 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.

4.10. Business Continuity Plans are to be tested to ensure effectiveness. Testing will occur:

a. Annually for the Enterprise Wide Business Continuity Plan; and
b. On a rolling 5-year cycle for local business continuity plans, which will be conducted via a desktop review.

5. ACCOUNTABILITIES AND RESPONSIBILITIES:

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

The Chief Risk Officer is responsible for currency of information and provision of advice relating to operationalising 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

Operational documents and resources

Critical Incident and Business Continuity Management Guidelines
Integrated Risk Management Guidelines

7. CONTACT INFORMATION:

For queries relating to this document please contact:

Policy Owner	Director, Strategic and Governance Services Centre
All Enquiries Contact	Chief Risk Officer and Manager, Enterprise Risk
Telephone:	08 6304 5733
Email address:	entepriserisk@ecu.edu.au

8. APPROVAL HISTORY:

Policy approved by:	Vice-Chancellor
Date policy first approved:	May 2003
Date last modified:	March 2021
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.
Next revision due:	August 2024
HPCM file reference:	SUB/8232