Business Continuity Policy

1. Purpose

The purpose of the Business Continuity Policy (policy) is to minimise the impact disruptions could have on the Critical Business Functions (CBF) of the Institution. Business continuity management (BCM) is a component of the Institution's Risk Management Framework and contributes to providing assurance to management, Academic Board, the Audit Risk and Compliance Committee and the Board of Directors, that disruptive incidents are identified and managed appropriately.

2. Scope

The policy applies to all staff and to all areas of the Institution's business.

3. Definitions

See Glossary of Terms.

4. Policy Statements

4.1 All organisations, including the Institution, are vulnerable to disruptions, ranging from events that can be anticipated to others that occur without warning. Some disruptions can negatively impact CBF, and the Institution is committed to maintaining an appropriate system of BCM to support the restoration or resumption of these CBF.

4.2 Disruptions fall within the scope of this policy when an incident disrupts the business-as-usual operations of the Institution, and the disruption has breached or threatens to breach the Recovery Time Objective (RTO) of one or more CBF.

4.3 The President and Managing Director (President) is responsible for initiating the BCM response and must advise the Executive Management Group (EMG) immediately of their decision to initiate the BCM response.

5. Policy Principles

General

5.1 The Institution is committed to the efficient and orderly resumption of its CBF in the event of a disruption. The Institution will maintain and implement a BCP which will guide the priorities for the restoration, reinstatement, or resumption of CBF. Disruptions can affect all areas of the Institution's operations including people, facilities and equipment, records, information, and communications technology (ICT), learning and teaching, regulatory compliance and externally provided service or resources.

5.2 In the event of a disruption, the Institution will work to restore, reinstate, or resume operations and functions to an acceptable pre-defined level that is necessary to perform and maintain CBF. The Institution accepts that in doing so, certain non-critical business functions may operate at a reduced level and may take time to resume full capability, capacity, and performance.

5.3 The Institution is committed to developing knowledge and delivering awareness programs as required to ensure staff are familiar with the requirements of good practice BCM.

Relationship and dependencies

5.4 Critical incidents, as defined in the glossary of terms, should be managed in accordance with the Critical Incident Policy and Critical Incident Management Procedures. There may be instances where both the Critical Incident Policy and this policy are relevant to a particular incident and operate concurrently, and other instances where only one policy is relevant.

5.5 If the critical incident leads to disruption to a CBF, the President must initiate the BCM response. The BCM response sets out how to restore/reinstate the affected function or whereas the Critical Incident Policy and procedure are focused on responding to the incident.

5.6 ICT incidents are managed in accordance with the Information Technology Disaster Recovery Plan.

6. Roles and responsibilities

6.1 The Managing Director has responsibility for:

- initiating the BCM response and informing EMG accordingly
- directing the response to disruptions to CBF relating to registration, regulation, and accreditation activities.

6.2 The Chief Operating Officer (COO) is the Responsible Officer of this policy. The COO is responsible for:

- directing the response to disruptions to operations
- leading the annual review of the BCP, within input from EMG
- coordinating reporting to the Audit Risk and Compliance Committee, Academic Board (if applicable) and the Board of Directors on any incidents managed under this Policy
- reporting annually as above on BCM.

6.3 The Chief Information Officer is responsible for directing the response to disruptions to ICT in accordance with the Information Technology Disaster Recovery Plan.

6.4 The EMG has overall responsibility for BCM at the Institution. EMG will provide executive decisions and strategic direction on Institution priorities when responding to disruptions and managing related Business Continuity responses.

6.5 The Vice-President Marketing will determine the appropriate communication strategy for internal and external communications. The Vice-President Marketing and the President are authorised spokespersons for the Institution during a business continuity event.

7. Related documents

Business Continuity Plan

Business Continuity Procedure

Critical Incident Policy

Critical Incident Management Procedures

Information Technology Disaster Recovery Plan

Health and Safety Policy

Incident Reporting Procedures

Infectious Diseases Policy

Infectious Diseases Procedures

Risk Management Framework (Risk Appetite Statement, Risk Management Policy, Risk Register)

Approved by the Board of Directors on 5 December 2023