Business Continuity Procedures

1. Governing policy

The Business Continuity Procedures (procedures) are pursuant to the Business Continuity Policy. They explain how a disruption to the Critical Business Functions (CBF) of the Institution will be managed.

2. Scope

These procedures apply to all staff and to all areas of the Institution’s business.

3. Procedures

Business Continuity response

3.1 The President and Managing Director (President) is responsible for initiating the Business Continuity Management (BCM) response in accordance with the Business Continuity Policy. The President must advise the Executive Management Group immediately of their decision to initiate the BCM response.

3.2 The President has responsibility to direct the response to disruptions to CBF relating to registration, regulation, and accreditation activities.

3.3 The Chief Operating Officer (COO) has responsibility to direct the response to disruptions to CBF relating to operations. The COO may require other areas who are undertaking non-time critical activities to support CBF, for example, by providing office space or equipment.

3.4 The Chief Information Officer has responsibility to direct the response to disruptions to information and communications technology (ICT) in accordance with the Information Technology Disaster Recovery Plan (see 3.5 & 3.6 below).

ICT disaster recovery

3.5 ICT disaster recovery is a critical component of the Institution’s business continuity capability and ICT recovery is managed in accordance with the Information Technology Disaster Recovery Plan.

3.6 The Disaster Recovery Plan describes the manner in which the Institution will respond to critical incidents that impact the delivery of information systems and services. It details how the Institution will rapidly and efficiently recover critical IT Technology following a disaster event.

Development and design of the Business Continuity Plan

3.7 The Business Continuity Plan (BCP) is informed by a Business Impact Analysis (BIA). The BIA identities the CBF of the Institution and measures the impact of a disruption by assessing the impact over time, the service level timing (if applicable) and the maximum tolerable period of disruption.

3.8 A Recovery Time Objective for each CBF of the Institution is identified and strategies to respond in the event of a disruption are developed for inclusion in the BCP. Disruptions to non CBF are not included in the BCP and should be managed in line with relevant department processes.

3.9 Note, for ICT this information is contained with the IT Disaster Recovery Plan.

Implementation

3.10 The strategies developed at the design stage are documented within the BCP, providing a pre-defined and approved course of action to be initiated in response to an operational disruption.

4. Roles and responsibilities

4.1 The roles and responsibilities for BCM are set out in the Business Continuity Policy.

5. Records management

5.1 The COO will ensure accurate records are maintained and recorded appropriately and be retained for at least two years after an incident managed under the Business Continuity Policy has occurred or if the incident involves a student, for at least two years after the student ceases to be an accepted student. The COO maintains a Business Continuity Incident Register.

6. Related documents

Business Continuity Plan

Business Continuity Policy

Critical Incident Policy

Critical Incident Management Procedures

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