Business Continuity

1. Purpose

Business continuity planning (BCP) is a proactive process that ensures the continuation of essential services during and after a disruption. This policy is designed to align with best practices in the Irish higher education sector (and in public service provision more generally), ensuring that critical academic, administrative, and operational functions continue to support students, staff, and the wider community at Mary Immaculate College (MIC).

2. Scope and Objectives

BCP covers the following:

- Academic delivery (teaching, learning, and research);
- Student services and support;
- IT systems and infrastructure;
- Administrative and financial operations;
- Facilities management;
- Communication and stakeholder engagement

Objectives:
1. Minimise disruption to core activities.
2. Ensure safety and well-being of students, staff, and visitors.
3. Protect and secure critical assets and data.
4. Comply with legal, regulatory, and accreditation requirements.
5. Facilitate recovery to normal operations in a structured and efficient manner.

3. Governance and Responsibilities

Business Continuity Committee (BCC[1]):
The BCC, led by the College President (the policy owner), will oversee the implementation and maintenance of the plan, ensuring it is regularly updated and tested. The committee, which shall report to the Executive Team and which shall (normally) meet at least twice per Academic Year will include the following members:

- College President (Chair);
- Vice President Academic Affairs;
- Vice President Administration & Finance;
- Vice President Governance & Strategy;
- Vice Dean, Thurles;
- Assistant Dean of Arts;
- Assistant Dean of Education;
- Director of ICT Services;

[1] The policy drafting team suggest that inclusion of a member of Academic staff should be considered prior to adoption of the policy.

- Director of Finance;
- Director of HR;
- Director of Buildings & Estates;
- Director of Student Life;
- Director of Student Academic Administration;
- Director of Strategic Communications & Marketing;
- Director of Teaching & Learning;
- Director of Information Governance & Compliance Management;
- Graduate School Director;
- Director of Library & Information Services;
- Director of Operations, Faculty of Education;
- Manager of Faculty of Arts Office
- Director of Quality;
- Buildings & Estates Manager;
- Coordinator of Risk Management & Internal Control (BCC Facilitator);
- Health and Safety Officer.

In each case, a cross-trained delegate will be available to stand in where the person normally associated with the roles described is temporarily unavailable.

Key responsibilities:

- Development of - and ongoing amendments to - the MIC Business Continuity Plan;
- Coordination of business continuity risk management in respect of core College functions;
- Develop and maintain continuity strategies;
- Recommend procurement of practical resources required for real-time incident management by staff operating 'on the ground;'
- Ensure that all departments create and maintain departmental-level business continuity plans;
- Oversee creation and promulgation of emergency protocols enabling staff (and security personnel) who may find themselves at points of incident detection to rapidly alert key responders and incident response decision makers;
- Convene [2]in emergency situations and lead the incident response team in the event of a systems-level disruption or a critical incident (e.g. through the MIC Critical Incident Management Plan / CIMP).

[2] The convening of the BCC will provide a single point of leadership and decision-making in the event of all unexpected or emergency situations which reach the threshold for business disruption and also require rapid, coordinated, cross-functional responses. Accordingly, responses in all circumstances will be led by the BCC.

4. Risk Assessment

A thorough risk assessment identifies potential threats that could disrupt operations. Examples include:

- Workplace Incidents: Serious workplace accidents or sudden illnesses, fire, violent assaults or attacks, incidents triggered by mental health factors;
- Brand or Reputational Damage: Serious brand damage or sudden and significant reputational crises;
- Natural Disasters: Flooding, extreme weather conditions;
- Pandemics and Public Health Crises: COVID-19 and similar events;
- Human Factors: Staff shortages due to illness or industrial action;
- Technological Failures: IT system outages, cyber-attacks;
- Utilities and Supply Chain Disruption: Power outages, shortages of critical supplies;
- Estate & Facilities: Major failure of estates or facilities infrastructure with consequences for operations and physical health of students/staff/visitors;
- Data management: major loss or breach of corporate data, regulatory fines, financial losses (and reputational damage arising);
- Safeguarding: major child or adult safeguarding incident;

5. Business Impact Analysis (BIA)

A BIA identifies critical functions and the impact of their disruption. For MIC, key areas include:
Critical Academic Functions:

- Delivery of lectures, seminars, and assessments;
- Access to research facilities and resources.

Administrative and Support Services:

- Student registration and admissions processes;
- Payroll and financial management;

IT Systems:

- Learning management systems (Moodle, etc.);
- Email and communication platforms;
- Data management and backups.

For each area, the BIA will assess:

1. Recovery Time Objective (RTO): The maximum acceptable length of time that a function can be disrupted.
2. Recovery Point Objective (RPO): The maximum amount of data loss that can be tolerated.

6. Continuity Strategies and Solutions

A. Academic Delivery

- Remote Learning Solutions: Ensure online platforms (Moodle, Microsoft Teams, media content systems such as Yuja) are robust, scalable, and accessible;
- Develop contingency plans for transitioning to full online teaching if required;
- Alternative Assessment Methods: Have alternative plans for conducting assessments, including online exams and coursework submissions;
- Flexible Academic Calendar: Implement options to extend the semester or adjust timelines for exams, as necessary;
- Support for staff and student: Plan for training in the event that remote learning is necessitated and achieve consistency of design and delivery of content through remote learning.

B. IT and Infrastructure

- Continuity of key academic information systems: SRS remains functional and recoverable, SRS data remains backed-up and online, with key systems for continuity available;
- Backup and Disaster Recovery: Regular backups of all critical systems. Data replication to off-site or cloud storage to ensure rapid recovery.
- Cybersecurity: Regular updates to security protocols, firewalls, and incident response plans to mitigate cyber threats.
- Alternative Communication Channels: In the event of email or phone system outages, use social media, SMS, and messaging apps to communicate with students and staff.

C. Student Services and Support

- Remote Counselling and Support Services: Enable virtual counselling and support for students. Ensure mental health services are accessible remotely;
- Student Welfare Fund: Maintain an emergency fund for students facing financial hardship during disruptions.

D. Administrative and Financial Operations

- Payroll Continuity: Ensure that the payroll system has redundancy built in and can be managed remotely.
- HR Continuity: Ensure that HR CMS platforms have redundancy built in and can be managed remotely.
- Admissions and Registration: Develop online systems that ensure continuity of student admissions and registration during disruptions.

E. Buildings & Estates Management

- Building Access and Safety: Establish protocols for partial or complete closure of campus facilities. Ensure that critical infrastructure (labs, libraries) can operate safely, even at reduced capacity;
- Utilities Backup: Contracts with external service providers for emergency utilities such as power generators and alternative water supply.

7. Communication Plan

Effective communication is key during any disruption. MIC will:

- Action the Crisis Communications SOP – See Appendix x
- Establish a proactive communication strategy and a hierarchy for information sharing with the Strategic Communications and Marketing (Communications) team, leading the communication efforts;
- Use multiple means of communication channels as the situation allows, including but not limited to, emails, MIC website, social media platforms, SMS notifications, MS Teams, webinars, and where appropriate, public media channels;
- Ensure timely updates: clear and consistent updates will be provided at regular intervals, ensuring that all stakeholders are informed of the College's status and recovery efforts.

The audience for communications include:

- Internal: MIC Staff and students, contracted staff working on campus, members of Governing Body and Trustees;
- External: Parents/guardians, local residents, suppliers, clients (including parties booking MIC facilities / rooms etc.), media, regulatory bodies, Garda and emergency services and first responders and other stakeholders as deemed relevant in accordance with the situation.

8. Incident Response Framework

Incident Response Stages:

1. Detection and Assessment: Incident detection triggers an immediate assessment by the BCC to determine the scale and impact.
2. Activation of the Business Continuity Plan: If necessary, the BCP is activated, and roles and responsibilities are delegated.
3. Crisis Management Team: This team, drawn from the BCC, takes control of the response. It establishes command and communication structures.
4. Immediate Response Actions: Evacuation, system shutdowns, and other immediate measures are implemented.
5. Ongoing Management: The crisis management team oversees the implementation of mitigation and continuity measures.

6. Recovery and Restoration: Gradual resumption of normal operations in accordance with the recovery timeline.

9. Training, Testing, and Review

- Training: Regular training sessions for staff and key stakeholders on the business continuity processes and their roles during an incident;
- Testing: Annual simulation exercises will test the robustness of the BCP and identify any weaknesses;
- Review and Updating: The plan will be reviewed annually or after any significant disruption to ensure it remains up to date with current risks, technologies, and sector best practices.

10. Conclusion

Mary Immaculate College's Business Continuity Plan is a comprehensive, proactive approach that ensures the College can maintain essential services in the face of disruptions. Through proper risk management, strategic planning, and regular review, MIC will safeguard the interests of its stakeholders and continue its mission to deliver quality higher education, even in the face of unexpected challenges.

11. Policy Owner

College President (supported by Vice President Administration & Finance and Vice President Governance & Strategy).

12. Supporting Policies, Protocols & SOPs

- Critical Incident Management Plan;
- ICT Security Incident Protocol
- Digital Strategy
- ICT Disaster Recovery Plan
- ICT Backup Policy
- Crisis Communications SOP

13. Change History

Reason for the new change and what sections of the procedure are affected. Previous revision and its document/change control number.

Revision	Document History	Reviewed By ET	Approved By UR
0	Initial Release	ET2024#08	UR2025#01