GMBS

GLOBAL MANAGEMENT
BUSINESS SCHOOL

Malta
Further & Higher
Education Authority

Business Continuity Plan (BCP)

1. Introduction
This document is the Business Continuity Plan (BCP) for GMBS, developed on the basis of the available risk analysis. The objective is to ensure that GMBS can continue its training, administrative and support activities in the event of outages, crises and other operational disruptions.

2. Objectives of the BCP
• Ensure the continuity of teaching and academic activities.
• Minimize the impact of interruptions on students, staff, and partners.
• Ensure the rapid recovery of affected services.
• Define responsibilities and communication lines during crises.

3. Key Risk Areas and Mitigation Measures

3.1 Teaching and Student Services
Risks: LMS/VLE outage, absence of lecturers, loss of student data.
Mitigation:
• Daily LMS data backup to off-site/cloud storage.
• Substitute lecturers prepared to cover absences.
• Maintaining communication with students via email and alternative channels (MS Teams).

3.2 Technical and Digital Infrastructure
Risks: Server failure, internet outage, cyberattacks.
Mitigation:
• Redundant internet connection.
• Cloud hosting of critical systems (VLE, email).
• Use of firewalls, antivirus systems, and regular updates.
• Use of services such as Turnitin/Scribbr to ensure academic integrity.
• Automated backup of all critical data to both on-site and off-site storage in real time.
• Weekly full backups and daily incremental backups.

3.3 Human Resources and Personnel Outages
Risks: Sick leave, quarantine, departure of key staff.
Mitigation:
• A list of backup personnel for each key position.
• Process manuals stored in the cloud.
• System access not dependent on a single person.

3.4 Administrative and Academic Services
Risks: Email outage, failure of the student information system, interruption of student support services.
Mitigation:
• Electronic documentation accessible via cloud storage.
• Contingency communication plan via phone lines and MS Teams.
• Database duplication to backup servers.

4. Crisis Communication
• **Responsible person**: Rector/Vice-Rector for Quality.
• **Channels**: LMS announcements, email, GMBS website, SMS (in case of internet failure).
• **Timeframe**: A statement and recovery plan must be published within 2 hours of the incident.

5. Recovery Timeline

- Critical systems (LMS, email): max. 6 hours.
- Student administration: 24 hours.
- Personnel services: 48 hours.
- Teaching: alternative assignments within 12 hours.

6. Responsibilities

- **Rector**: Activates the BCP and coordinates the team.
- **IT Department**: Restores systems and ensures technical support.
- **Student Services Office**: Communicates with students and teachers.
- **Lecturers**: Provide replacement teaching materials.

7. Conclusion

This BCP proposal represents a framework that must be formally adopted, regularly tested (at least once a year), and updated in line with changes in GMBS infrastructure and the external environment