Services
Security and Business Continuity
Business Continuity Policy
Ser-Sec-003
07/11/2017

<table>
<thead>
<tr>
<th>Author Name</th>
<th>Alan Cain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author Job Title</td>
<td>Head of Security and Business Continuity</td>
</tr>
<tr>
<td>Version No.</td>
<td>1.1</td>
</tr>
<tr>
<td>EIA Approval Date</td>
<td>28/06/2017</td>
</tr>
<tr>
<td>Committee Recommend for Approval</td>
<td>Business Continuity Steering Group 06/09/2017</td>
</tr>
<tr>
<td>Final Approval</td>
<td>University Executive Group 07/11/2017</td>
</tr>
<tr>
<td>Review Date</td>
<td>07/11/2018</td>
</tr>
<tr>
<td>Draft</td>
<td>No</td>
</tr>
<tr>
<td>Document Sensitivity</td>
<td>PUBLIC</td>
</tr>
</tbody>
</table>
Services: Security and Business Continuity
Business Continuity Policy

Table of Contents

- Glossary / List of Acronyms 3
- Background 5
- Policy statement 6
- Business Continuity Objectives 6
- Business Continuity Management System (BCMS) Objectives 7
- BCMS Requirements 8
- Legal and Regulatory Requirements 9
- Scope 9
- Governance 10
- BC Roles and Responsibilities 10
# Glossary / List of Acronyms

<table>
<thead>
<tr>
<th>Term</th>
<th>Abbreviation</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity</td>
<td>BC</td>
<td>The capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.</td>
<td>ISO 22300</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>BCM</td>
<td>A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>BCM</td>
<td>Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Business Continuity Plan</td>
<td>BCP</td>
<td>Documented procedures that guide organisations to respond, recover, resume and restore to a predefined level of operation following disruption.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Business Impact Analysis</td>
<td>BIA</td>
<td>Process of analysing activities and the effect that a business disruption might have on them.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Term</td>
<td>Abbreviation</td>
<td>Definition</td>
<td>Source</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Crisis</td>
<td>-</td>
<td>A situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organisation and requires urgent action.</td>
<td>ISO 22300:2012</td>
</tr>
<tr>
<td>Incident</td>
<td>-</td>
<td>A situation that might be, or could lead to, a disruption, loss, emergency or crisis.</td>
<td>ISO 22300:2012</td>
</tr>
<tr>
<td>Maximum Acceptable Outage</td>
<td>MAO</td>
<td>The time it would take for adverse impacts, which might arise as a result of not providing a product / service or performing an activity, to become unacceptable. The university requires that business processes should be fully recovered within the MAO.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Recovery Time Objective</td>
<td>RTO</td>
<td>The period of time following an incident within which a product or activity must be resumed or resources must be recovered to a minimal level of operation.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Risk</td>
<td>-</td>
<td>Effect of uncertainty on objectives.</td>
<td>ISO Guide 73</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>-</td>
<td>Overall process of risk identification, risk analysis and risk evaluation.</td>
<td>ISO Guide 73</td>
</tr>
<tr>
<td>Risk Management</td>
<td>RM</td>
<td>Coordinated activities to direct and control the organisation with regard to risk.</td>
<td>ISO Guide 73</td>
</tr>
</tbody>
</table>
1. Background

Manchester Metropolitan University is one of the most extensive higher education centres in Europe with 36,000 students and more than 1,000 undergraduate, postgraduate and professional courses. The University educates and trains large numbers of legal and business professionals, scientists, engineers, teachers, health workers and creative professionals.

The University is in the top three nationally for environmental sustainability, in the top 3% of global universities as ranked by the Times Higher Education and has an 85% research impact rated world-leading and internationally excellent.

The University is arranged into six faculties; Faculty of Business & Law, Faculty of Education, Faculty of Health, Psychology & Social Care, Faculty of Arts & Humanities, Faculty of Science & Engineering and the Cheshire Campus.

The University engages in a number of activities including teaching, research & knowledge exchange, consultancy, training & CPD, halls of residence, sports centres, catering and conferencing.

The University works closely with various internal and external stakeholders including students, staff, government departments, funding councils, research councils, research sponsors, employers and local communities. Each of these stakeholder groups will be included within the BCMS.
2. Policy Statement

Business Continuity Management (BCM) is the holistic management process that identifies potential threats to the University and the impacts to its operations those threats, if realised, might cause. It provides a framework for building organisational resilience, thereby safeguarding the interests of its students, alumni, staff and external stakeholders and protecting its reputation as the leading modern university of the future.

Continuity of business is a key priority for the University. It is the responsibility of anybody working for or on behalf of the University to take all reasonable steps to avoid any incident that may require a business continuity response. In addition individuals must maintain and improve the BCMS in accordance with their role within it. In the event that such an incident does occur, anybody working for or on behalf of the University must take all reasonable steps to minimise any disruption to the University and its stakeholders. The University’s strategy for business continuity management represents the practical implementation of this Policy.

This Policy Statement has been approved by the University Executive Group (UEG). It has been communicated to all staff and will be communicated to other parties as appropriate.

3. Business Continuity Objectives

The objectives of business continuity are to ensure that the University:

- Understands its critical activities and maintains the capability to resume operations within agreed timeframes, following the deployment of a business continuity response.
- Increases resilience by protecting critical assets and data (electronic and otherwise) through a co-ordinated approach to risk and business management and recovery.
- Minimises impacts using a focused, well-managed response activity.
4. **Business Continuity Management System (BCMS) Objectives**

The objectives of the BCMS are to ensure that, in the context of business continuity, the University:

- Maintains the safety and security of its staff, students and visitors.
- Safeguards the interests of students, alumni, staff and external stakeholders by ensuring that urgent or priority activities continue in the event of a disruptive incident.
- Maintains the reputational integrity of Manchester Metropolitan University.
- Complies with legal and regulatory requirements.
- Deploys adequate resources to maintain the BCMS.
- Can deploy the required resources to implement the Business Continuity Plan in the event that an incident occurs.
- Responds to issues and risks arising that affect the BCMS or ongoing operations in a timely and appropriate manner.
- Ensures that all employees receive appropriate awareness training in business continuity matters, ensuring that they are aware of their responsibilities and able to make informed decisions relating to business continuity issues.
- Via a management review process, identifies weaknesses in the BCMS and implements improvements wherever possible.
- Ensures that relevant interested parties are aware of the BCMS and any requirements / obligations arising from it.
5. **BCMS Requirements**

In order to implement the Policy, persons working for or on behalf of the University are required to assist as appropriate in:

- Taking all reasonable measures to prevent and avoid any disruption to normal operations.
- The preparation and maintenance of the Business Continuity Plans, to promote an effective and timely response to incidents caused by vulnerabilities to people, processes or the operating infrastructure.
- Considering business continuity and resilience implications in all processes, projects and IT developments.
- Where necessary, making arrangements for the recovery of infrastructure components (e.g. accommodation, IT, communications, equipment and supplies).
- Making arrangements to re-locate or re-organise operations to allow critical processes to continue within their defined recovery time.
- Protecting the welfare of people during and following an incident.
- Ensuring the effectiveness of the Business Continuity Plans and recovery arrangements through robust and regular testing, awareness and training.
- Updating the Business Continuity Plans on an annual basis, or following significant changes to requirements.
- Ensuring that information security controls and procedures are not materially diminished in the event of an emergency or business continuity response.
- Ensuring that management and staff comply with the requirements of this policy and any other supporting policies.
- Training all employees in the business continuity issues that are relevant to their role.
- Define a systematic approach to risk management and deploy a method suitable to the BCMS and business requirements.
- Determine criteria for accepting risks and set policies and objectives to reduce business continuity risks to an acceptable level.
- Review the risk assessment and adequacy of implemented controls at least annually, to ensure that they remain effective.
- Implement and maintain a system to detect and respond to potential weaknesses in the BCMS.
- Conduct regular reviews of the BCMS and implement improvements wherever possible.

The Business Continuity Manager has direct responsibility for maintaining this Policy and providing advice and guidance on its implementation.
6. Legal and Regulatory Requirements

Manchester Metropolitan University has a duty of care to its students and staff, as well as those visiting the University.

Some specific duties are set out in statute, examples being:

- Corporate Manslaughter and Corporate Homicide Act 2007.

Additionally, the University could be subject to action through the civil courts were it found to have been negligent in its emergency planning arrangements or duty of care. Failure to put in place and implement appropriate risk management and business continuity management may also compromise the University’s insurance cover.

Associated university policies include the Risk Management Policy, Health and Safety Policy and Environmental Policy.

7. Scope

The BCMS will include the activities of teaching, research & knowledge exchange, consultancy, training & CPD, halls of residence, sports centres, catering and conferencing conducted in both the Manchester and Cheshire campuses. In addition, the University’s supporting services that enable the delivery of core services will be within the scope of the BCMS.

Excluded from scope are exhibitions, events and performances, whether permanent or temporary, conducted within or on behalf of the University, failure of which would not be expected to materially affect the reputation of the University.

The University also works with a number of partner institutions to deliver its activities and a risk-based approach will be adopted in terms of the expectations of these organisations having their own Business Continuity Plans in place.
8. Governance

The Business Continuity Steering Group is responsible for Committee level approval of the Business Continuity Policy. The University Executive Group (UEG) is responsible for final approval and sign off.

An annual review of the BCMS will be carried out by the Business Continuity Lead (Chief Operating Officer); the BCMS will also be reviewed following any Business Impact Analysis (BIA) or Risk Assessment revision which identifies substantive changes in either process or priorities or when significant changes occur within the University.

A validation exercise will be carried out every 18 months by the Head of Security and Business Continuity and be designed so as to confirm that the BCM programme meets the objectives set in the BC policy and that the University’s Incident Response & Crisis Management and Business Continuity Plans are fit for purpose.

Additional governance shall be provided in the form of a three yearly full audit planned and implemented by UNIAC, the shared internal audit and assurance service for Universities. The overall objective of both the UNIAC audit shall be to determine that the BCMS meets the key objectives as outlined in the Policy Objectives (above).

9. BC Roles and Responsibilities

Successful BCM is dependent upon the early identification of clearly defined roles and the associated responsibilities, behaviours and authorities to manage the BCMS throughout the University. The following principal roles have been specified.

Business Continuity Lead

The Chief Operating Officer is the senior executive lead for BCM across the University.
Business Continuity Steering Group
The Business Continuity Steering Group is the senior decision making group for BCM across the University.

Head of Security and Business Continuity
The Head of Security and Business Continuity is the Business Continuity Manager responsible for the operation and maintenance of the BCMS.

Business Continuity Co-Ordinator
The Business Continuity Co-Ordinator assists the Business Continuity Manager and has day-to-day responsibility for operation of the BCMS.

Staff
All staff doing work under the University’s control shall be aware of this policy, their role within the Business Continuity Plans and their own role during disruptive incidents.