OXFORD BROOKES UNIVERSITY

## Business Continuity Policy Statement

### Policy

1 The University's policy is to maintain the continuity of its activities, systems, facilities and processes and where these are disrupted by any event to **enable it** to return to 'normal' operations as soon as possible, taking fully into account the impact of any delay on the University's quality of service, reputation and finances.

2 This policy is intended to ensure:

- The concept of Business Continuity and our policy and approach is understood by all stakeholders.
- Internal and external dependencies on customers, suppliers, partners and resources implications are identified.
- Faculty and Directorate plans are developed to ensure recovery continuity is assured to an acceptable level in the event of an interruption to services.
- Plans are systematically maintained and tested.
- A programme of training and communication is put in place.

### Objectives

3 The objectives of business continuity planning 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 contingency planning response.
- Increases resilience by protecting critical assets and data (electronic and otherwise) through a co-ordinated approach to management and recovery.
- Minimises impacts using a focused, well-managed response activity.

### Scope

4 All University activities wherever conducted, must comply with the requirements of this Policy.

### Requirements

5 The University requires

I A standing Major Incident Team is formed based on a Gold-Silver-Bronze roles. MIT responsibility is to recover University generic facilities, corporately managed systems and central data security and;

II The maintenance of a Major Incident Plan to guide the team on the recovery from major incidents. This to include call out arrangements and MIT operational requirements and the plan must be subject to testing at least bi-annually;

III Each faculty and directorate is responsible for maintaining a register of all local specialist, facilities equipment and data, carrying out a business impact analysis (BIA) and setting parameters on acceptable recovery times for each. Faculty and directorate management teams are responsible for completing a Business Continuity Plan (BCP) in response to their BIA. Registers, BCP's and BIA's must be reviewed annually or following invocation of a plan so as to implement any lessons learnt. Directorate's responsible for the delivery of corporate and University generic facilities should undertake a BIA and BCP for all facilities provided through them.

6. In compiling plans due consideration must be given to:
   - Taking all reasonable measures to prevent and avoid any disruption to normal operations.
   - Considering continuity planning and resilience implications in all process, project, change and system developments.
   - Making advance arrangements for the recovery of infrastructure components (e.g. accommodation, transport, telecommunications, equipment and supplies).
   - Making advance arrangements to re-locate or re-organise operations to allow critical processes to continue.
   - Providing resilience for information systems and data, or alternative ways of working in the event of their failure. All new systems and processes to be in line with the University's Information Security Policy (http://obis.brookes.ac.uk/InfoCompliance/InformationSecurityPolicyv1.0.pdf).
   - Protecting staff, student, visitor and third party welfare during and following an incident.
   - Ensuring the effectiveness of plans and recovery arrangements through robust and regular testing and training.
   - Updating plans following significant changes to contingency planning requirements. Such changes may occur as part of organisational change planning and management.

## Approval and review

7. Original Business Continuity policy approved by the Executive Board in June 2010.

   - The Major Incident Working Group reviews and approves updates to policy.