

# Information Technology Disaster Recovery and Business Continuity Policy

## 1 *Aims*

- 1.1 The aim of this policy is to establish the responsibilities for ensuring that the University's IT facilities can be recovered in the event of a disaster, and that the business of the University can continue.
- 1.2 This policy relates only to IT, and should be read in conjunction with wider University continuity and recovery plans.

## 2 *Definitions*

- 2.1 Business continuity (BC) details how an organisation or business area keeps its processes going during a disaster or system failure, either by use of alternative computer systems, paper or simply by not doing certain things.
- 2.2 Disaster recovery (DR) is the restoration of systems and infrastructure back to agreed service levels following a disaster. This may be temporary in the first instance, requiring full service restoration later.

## 3 *Disaster Recovery*

- 3.1 The Chair of the Information Systems Committee has overall responsibility for ensuring that there is a DR plan for all University IT facilities.
- 3.2 The development and testing of this plan is delegated jointly to the Head of Computing Services and the Head of Corporate Information Systems. They will form a DR Planning Group which will meet 4 times per year.
- 3.3 This group will publish a DR plan which can be used to manage the recovery of any IT facilities lost, damaged or otherwise rendered unusable due to any incident.
- 3.4 The plan will aim to allow recovery of any service within a period of 7 (seven) days.
- 3.5 The plan will not focus on any specific potential incident, but be general enough to cope with any possible disaster up to an agreed scale.
- 3.6 The Planning Group will test the plan via a managed scenario walkthrough once per year.

## 4 *Business Continuity*

- 4.1 The University will define and publish a corporate Business Continuity plan and procedure. IT Business Continuity plans must fit into this wider framework.

- 4.2 Every Head of Department is responsible for identifying their department's critical business processes which rely on any IT facilities for the delivery of those processes.
- 4.3 Each Head must then put in place a documented BC plan identifying how these processes will be delivered in the event of IT facilities being unavailable.
- 4.4 The Director of Finance will document University-wide processes in the event of the failure of the Finance Management and Payroll system.
- 4.5 The Registrar will document University-wide processes in the event of the failure of the Student Record system.
- 4.6 The Director of Human Resources will document University-wide processes in the event of the failure of the Human Resources system.
- 4.7 All plans should be reviewed annually and tested at least every two years.

<b>Document control/change history</b>				
<b>Version</b>	<b>Author(s)</b>	<b>Date</b>	<b>Circulation</b>	<b>Comments</b>
1	IE	Sept 2008	ISC policy T&F group	Basic first draft
2	IE	Sept 2008	ISC	Revised after comments

<b>Document approval and review</b>	
<b>Approved by:</b>	Information Systems Committee
<b>Date approved:</b>	
<b>Review date:</b>	
<b>Author(s):</b>	Head of Computing Services
<b>Owning Department:</b>	Computing Services