



The  
University  
Of  
Sheffield.

Corporate  
Information  
and Computing  
Services

# Business Continuity Plan

March 2007

## **Purpose and outline of the Plan**

This Plan exists to help the staff of CiCS to respond effectively in any situation where the ability to provide important services to the University is impaired or threatened, or where CiCS facilities or services are involved in any other damage or threat to the University.

The Plan describes a special mode of management for use in abnormal situations.

It clarifies issues of authority, priority, management and communication. It provides resources such as contact and priority lists, procedures etc. The Catalogue of Risks provides a focus for the continuing development of preventative measures.

## **Stages in the operation of the Plan**

- a) Recognition that a serious situation exists and CiCS Management Team informed about the issue.
- b) An Incident Management Team (IMT) is called together. This may be a CiCS response to a local issue or as a subset of a University Incident Management Team.
- c) The IMT begins both to manage the situation, taking action via one or more recovery teams, and communicating and consulting with others as necessary.
- d) If the incident is not short-lived the IMT continues to manage the situation internally and deal with external organisations and people.
- e) The situation no longer requires special management. The IMT is disbanded and its functions are handed smoothly to normal groups.
- f) Events are reviewed to learn how current and emergency procedures can be improved and future incidents prevented.

## **Section A: Continuity Plan**

1. Initiation of the Plan (All CiCS staff should be familiar with this section)
2. The Incident Management Team
3. Closing the Incident
4. Review and Development

## **Section B: Catalogue of Risks**

## **Section C onward: Resources and Appendices**

## **Table of Contents**

### **Section A: Continuity Plan**

1	Initiation of the Plan.....	4
2	Definitions of Incidents.....	5
3	Responding to Incidents.....	6
3.1	Obvious emergencies .....	6
3.2	Less obvious situations .....	6
3.3	When to initiate the plan .....	6
3.4	Standing orders for ‘First Aid’ .....	7
3.5	Actions to avoid .....	7
4	The Incident Management Team .....	8
4.1	IMT activities.....	8
4.1.1	Administrative.....	8
4.1.2	Communications .....	8
4.1.3	Practical action.....	8
4.1.4	External communications.....	9
4.2	Ongoing management of the situation. ....	9
5	Closing the Incident .....	10
6	Review and development of the Plan.....	10
6.1	Incident review.....	10
6.2	Development of the Plan.....	10

### **Section B: Catalogue Of Risks**

1. Catalogue Of Risks

### **Section C: Appendices**

1. Business Impact Assessment And Methodology
2. Business Continuity Test Plan
3. Information Security Policy
4. Security Incident Protocol
5. System Administrators’ Charter Technical Services Call Out List
6. Code Of Practice And Related Information

## **1 Initiation of the Plan**

All CiCS staff should be familiar with this section.

**The Plan is initiated simply by contacting a member of the Management Team and passing on details of the situation.**

**Any member of University staff may make this contact, either direct or via the University Control Room or Security staff.**

**Individuals should take no further action, apart from obvious safety measures, without guidance from the Management Team.**

**The Management Team consists of the Director of CiCS, Deputy Directors and Team Leaders. Contact details, with telephone numbers for use out of hours, are in the Appendix. The Control room can relay a call out of hours.**

### **The University Control Room.**

**Emergencies 4444**

**Other calls (22) 24085**

**This is the first point of contact, day or night, for any University security or emergency matter. Security staff are always present, including a response team.**

**Situations where the Control room should be contacted without hesitation include:**

**Calling emergency services or utility companies - gas, electricity, water etc.**

**Reporting discovery of a break-in**

**Assistance with University locks or alarms**

**Reporting suspicious, dangerous or offensive activity around the University**

**Calling senior staff out of hours – the Control room holds a call-out list.**

## 2 Definitions of Incidents

The University Business Continuity plan defines three levels of incident, the most serious being a Level 3 incident,

### Level 1 incident – Local incident

Defined as a local incident that is not an emergency and does not cause serious physical threat to people or property. Results are likely to be limited disruption to services and would pose no threat to the reputation of the University. These should be catered for under Departmental Contingency Plans and Procedures with assistance, as necessary, from University support services and the Emergency Services.

### Level 2 incident - Minor incident

Defined as incidents that could pose an actual threat to people or property, but not seriously affect the overall functioning of the University. They may have legal ramifications or threaten the reputation of the University, and might include the isolation or evacuation of part of a building or buildings, with the assistance of the Emergency Services and the University's Estates, Safety and Security staff as necessary. Such incidents may be covered by existing emergency procedures.

### Level 3 incident – Major incident

Defined as incidents causing significant disruption to University operations. It may affect entire buildings, or number of buildings, and affect students and staff, with the potential to escalate and will involve external Emergency Services who would probably take operational control of the incident. Existing emergency procedures will not cover the actions necessary to manage the repercussions of such incidents.

In terms of computer systems the University Business Continuity plan defines the incidents as follows:

	Local Incident	Minor Incident	Major Incident
Computer system failure Greater than 1 day	Affecting < 5% campus	Affecting 10 – 30 % campus but no sensitive department / sites affected	Affecting > 30% campus and sensitive departments / sites / hospitals

In all cases CiCS staff should initiate the CiCS Business Continuity plan. In the case of major emergencies the University Business Continuity plan will be invoked. The decision to notify the University senior management and initiate the University plan will be taken by the Head of Department or her Deputy.

### **3 Responding to Incidents**

#### **Obvious emergencies**

If an environmental emergency is discovered, such as fire, flood, gas leak etc. the first actions must always be:

- Raise the alarm, probably by a break-glass point.
- Begin emergency evacuation of the building.
- Call the University Control Room, 4444. (see box above)

Senior Management should be informed as soon as immediate safety actions have been taken.

#### **Less obvious situations**

Situations which can disrupt or damage IT services provided by CiCS occur under the following major categories:

- Power interruptions
- Air conditioning or other environmental problems
- Fire
- Water
- Weather or other natural event
- Security incidents e.g. hacking, virus attack, unauthorised use of University systems etc.

#### **When to initiate the plan**

Some events will be difficult to detect (e.g. hacking) or progressive (e.g. air conditioning problems) and are likely to be noticed first by operations staff. It will probably not be clear whether critical tasks are affected and it may not be easy to decide whether to contact the Management Team. Other events will be immediately apparent (e.g. power outage or server crash), but a time to fix may initially be difficult to determine. The following should be considered when deciding to call an incident:

- Importance of service affected as defined by the Business Impact Assessment (see appendix 1).
- Number of users affected by the loss of the service.
- Length of time during which the service will be unavailable or impaired.

The Management Team should be called if:

- A mission critical system, as defined by the Business Impact Assessment, is unavailable to more than 5% of the University (either in terms of physical space or number of staff and students effected) for more than an hour.
- A high importance system, as defined by the Business Impact Assessment, is unavailable to more than 5% of the University (either in terms of physical space or number of staff and students effected) for more than 24 hours.
- A medium or low importance system, as defined by the Business Impact Assessment, is unavailable to more than 10% of the University (either in terms of physical space or number of staff and students effected) for more than 24 hours.

Calling a member of the Management Team should not be seen as a major decision. It has none of the drama of a call to the emergency services. It is likely to be a simple

consultation (“I’m worried about this, what do you think?”) and as a small step in the possible escalation of an event. If an out-of-hours call is involved no-one will object. The person(s) called will decide whether the Plan should be invoked. The person initiating the call is not deemed to have made, or expected to make, that decision.

Nothing is lost if those called decide to take no further action, and in any case they need to be kept aware of significant problems and possibly to give advice. It is good to rehearse the first stages of the Plan in this way as it means it will not be forgotten when something more serious occurs.

### **Standing orders for ‘First Aid’**

Some specific situations will have “standing orders” for possible immediate remedial action. These are in the appendices to this document and will be developed continually. These procedures should only be used where the situation is stable and safe and their use cannot cause further complication. Discussion with senior colleagues should take place before they are used.

### **Actions to avoid**

In an emergency:

- Take no action that risks the safety of yourself, other staff, emergency services or the public, or could be regarded as doing so.

- Leave dangerous situations and any kind of risk to the emergency services.

- Do not enter any building or room that has been subject to an evacuation before an all-clear has been given, or premises regarded as unsafe for any reason.

- Do not move or handle anything that may provide evidence of break-in, theft, arson, cause of accident etc. or that insurers may wish to inspect.

- Do nothing in haste or alone; take time to think, consult and plan. Do not pre-empt decisions of the Management Team.

- Do not open any fire safe, following an emergency, until it has been agreed by a member of the Management Team that it may be done safely, cleanly and without risking the integrity of the contents.

- Do not publicise the situation except to system users, as part of a security protocol or as required for public safety. Do not communicate with the media without permission from the Management Team.

*Note that some types of illegal electronic materials must be treated in the same way as physical dangers – i.e. by avoiding contact. Examining or copying them could destroy evidence of a crime or even incriminate you! See the security incident protocol document for further information.*

## **4 The Incident Management Team**

The senior staff available will form a small Incident Management Team. This will normally consist of 3 people, usually the Director or a Deputy and two others. The responsibilities of the IMT are listed in the appendix and its likely activities are described below.

The IMT has full authority to manage all aspects of the situation for which CiCS is responsible, taking advice and direction as appropriate from senior University management, emergency services and other experts. The IMT will delegate most practical actions to any recovery teams that may have been called together. No other person may take action, or hold significant communication with major players (insurers, media...) without the knowledge of the IMT.

If appropriate, the IMT will have a role in a wider, and more authoritative, University team. Either team may initiate the other during a University-scale contingency.

### **IMT activities**

The actions of the IMT, particularly in the early phase of an incident, fall into four areas as follows:

#### **Administrative**

- Select a suitable location and set up a base
- Ensure that the task is approached in a calm and thoughtful manner
- Ensure that the membership of the IMT is appropriate and add any necessary person(s).
- Use the procedures and resources in the appendices to the Plan as necessary.
- Set up any communications the IMT may need, such as telephone, mobile phone, radio, computer.
- Begin a log of actions, with times etc. and ensure that it is continued.
- Obtain any other practical resources the IMT will need

#### **Communications**

- Contact those directly involved in the incident to inform them that the Plan has been initiated and the IMT is in place and give contact details.
- Pass contact details to all who will need to communicate with the IMT.
- Consult Safety Services if appropriate and if they are not already involved.
- Contact other managers and key people in the University to inform them of the situation and contact details for the IMT.
- Decide whether to invoke the University Contingency Plan, or to consult on the possibility of doing so.

#### **Practical action**

- Ensure that no inappropriate or unsafe actions are currently being taken.
- Contact staff to form any necessary teams as listed in the appendix.
- Instruct teams to log their own activities
- Communicate with all involved to ascertain the extent and seriousness of the incident.
- Assess the state of security of information and systems.
- Instruct teams to take steps to contain damage and make systems stable and safe. This may include closing down computers, powering down equipment, disconnecting from the MAN etc.

Consider remedial action, once the situation is stable and careful thought is possible.

Ensure that staff are used appropriately, e.g. to manage and communicate or to work on the technical issues, not normally both.

### **External communications**

Contact insurers, advisors, engineers, suppliers etc. as necessary.

Contact the media, or set up channels for doing so, normally via the University PR officer.

Inform other universities, funding bodies and major partners.

Contact computer users to inform of failed services.

### **Ongoing management of the situation.**

If the incident is not quickly resolved the IMT will continue to meet as often as required. This may be daily or more often at first, becoming less frequent until the Team is disbanded.

If it is necessary for the IMT to remain in effect for some days or weeks, it is likely to be involved in much more than local planning and management within CiCS. Various activities involving other managers and specialists from within and outside the University may be involved, such as:

- Investigation of the causes of an incident.

- Maintaining and/or restoring security for information and systems.

- Initiating any legal action or claim.

- Personnel issues relating to the event itself, or its effect on normal work.

- Dealing with insurers and loss adjusters

- Liaison with emergency services to produce reports or handle enquiries.

- Gathering evidence for prosecution or insurance claim.

- Dealing with the media, both to give accurate information and correct mistakes.

- Assigning temporary functions to spaces, including IT Centres, student computer workrooms etc.

- Rewiring power, network, telephones.

- Refurbishment of damaged spaces or buildings.

- Clearing debris and salvage operations.

- Obtaining replacement equipment.

- Dealing with engineers and suppliers.

All activity should continue to be logged. More substantial reports may also be required. The location and contact details for the IMT may change during its existence if this is lengthy.

## **5 Closing the Incident**

The duration of the incident – i.e. the period for which the IMT is needed, may be anything from a few hours to a few months. As previously stated, the activities of the IMT may be quite different if it is in existence for a longer term. In this case the IMT should periodically question the need for its existence, and resist the tendency to become a permanent ‘committee’. The point when the IMT is no longer essential and any remaining issues can be managed by normal methods must be recognised.

The IMT will then be disbanded and the incident formally closed. Matters that were being managed by the IMT will be handed to other individuals and groups. All parties involved will be clearly informed of handover of responsibilities, and given contact details for any further communication.

## **6 Review and development of the Plan**

### **Incident review**

As soon as possible after the incident is closed, the whole event will be reviewed. This may involve a single meeting of the IMT and other CiCS staff, or a series of meetings for all involved, depending on the nature of the event. The purpose is:

To evaluate the operation of the Plan with a view to improving it

To find ways to reduce the probability of similar events, minimise their effects or ease recovery.

A formal report will be produced and made available internally, to the HE community or beyond as appropriate.

### **Development of the Plan**

The Plan will be reviewed and tested regularly to maintain its relevance for the current situation. This applies in particular to the resources sections, where details may change rapidly.