

# **Guidance on developing and maintaining Computer Disaster Recovery Plans in Further and Higher Education**

**Produced by Belfast Institute and North West Institute of Further and Higher Education funded by the DEL Strategic Alliance fund.**

**Report Date: April 2002**

## **Introduction**

The provision of Information systems is now an integral part of the learning process and administrative systems in all colleges of Further and Higher Education. It is therefore imperative that all colleges prepare a detailed recovery plan in the event of a disaster resulting in the loss of some or all of the information systems. This plan should be rigorously tested and updated annually, and should have the facility that it can be implemented at anytime either inside or outside normal working hours. The plan is intimately linked with backup procedures, and the secure storage of media.

The process of developing the plan can also be useful in highlighting vulnerability or weaknesses in the physical network, or in procedures. The process can therefore feed back into strategic ICT forward planning.

## **The Disaster Recovery Task Team**

Assembling the right team is **the** key initial step in formulating, implementing, maintaining and reviewing the Computer Systems Disaster Recovery Plan.

As a minimum the team will consist of:

Deputy Director responsible for ICT  
Network manager  
MIS Manager  
Computing Department representative  
Buildings Department representative

The team should be headed by the senior manager responsible for ICT in the organisation. This person will generally be a deputy director, and will certainly be a member of the organisation's senior management team. They bring a broad strategic perspective to the team, and provide a link to the major decision making forums of the organisation.

The network manager has a detailed knowledge of network topology, hardware deployment, security precautions, backup systems and technical specifications.

MIS, Finance and Payroll are among the most mission critical systems for FE and HE colleges. The MIS manager has a detailed knowledge of these systems, their backup, and recovery precautions.

Most colleges have an academic Department of Computing which is separate from the IT support team that manages the network. Generally this department will have access to specialist systems and software and a high degree of expert knowledge of computing systems and networks. Their representative on the task team should have a good technical knowledge, and an overview of all computing systems and software used by the department.

Lastly the team must involve a senior representative from the Buildings or Estates Department. Many potential disasters could involve fire, flood etc, and the first priority in these cases will be to evacuate the building safely. Additionally the disaster will most often be discovered by a member of the Building or care-taking staff, and the plan will have to clearly identify lines of communication so that key personnel can be informed, and the plan activated if appropriate. The Buildings department representative will bring a detailed knowledge of the procedures for raising the alarm, evacuation procedures, contacting emergency services and building and electricity repair services.

### **Contents of the plan.**

When devising a Disaster Recovery plan it is difficult to restrict the scope of the plan, and a Computer Systems disaster could well have other major implications for relocating large parts of the College activities to another site. The plan should be comprehensive, but also as concise as possible, so that information and procedures can be easily referred to. It is therefore important to define the nature of the disaster to which the plan refers. A risk assessment should be carried out by network element, and also by location. To make important information easily accessible this risk assessment, and the detailed disaster recovery plan should be presented in a tabular format, by location and network element.

A suggested list of contents is:

- Definition of a Disaster
- Network Overview
- Risk Assessment & Business Impact Review
- Disaster Recovery Plan
- By Network element
- By site
- Maintenance
- Testing

The appendices should contain:

- List of servers and their locations.
- List of switches and hubs and their location
- Network diagrams
- Procedures for rebuilding the network
- Procedures for dealing with virus attack
- Details of any maintenance or restart agreements with commercial suppliers
- Important telephone contact numbers
- List of approved suppliers

**Definition of a disaster.**

This is important in defining the scope of the plan.

A suggested definition is:

“For the purposes of this plan a Disaster is defined as loss or damage of part or all of the computer network, which would have a high or very high business impact for the Institute”.

## **How the plan is activated**

State who can activate the plan by declaring a disaster .Typically this should be the Assistant Director (ICT), and / or the Network Manager, and / or the MIS manager.

In the event of a disaster a panel convened by the Assistant Director (ICT) should monitor the progress of the plan, convene the disaster recovery team as required, update and advise the Senior Management Team, and take any further necessary action. It is important that arrangements are identified which will allow the plan to be activated outside normal working hours.

## **Network Overview**

This should describe the topology of the network, describe how the main sites are linked, and describe the important features on major sites. Identify how many computers are connected to the network, and the locations having the greatest concentration of machines. Identify the network operating system, and the main types of software on the network and desktops. Identify the main server rooms and main switch cabinets. Identify the locations of the MIS, payroll, finance, e-mail, web, and on line learning servers.

References to network diagrams (in the appendix) should be included here.

Give a brief overview of the main disaster risks at these major network locations eg flooding, fire, power loss etc.

Give a brief overview of maintenance agreements, backup arrangements, and any disaster recovery service agreements.

## **Risk Assessment and Business Impact Review.**

Because of the complex nature of modern computing networks in Further and Higher Education, and the major impact that failure would have on all college business processes including learning and teaching, this section of the plan has the potential to become lengthy and complex.

What is needed, however, is a clearly laid out summary of the risks, and business impact, together with a list of precautions in place, and alternative processes, which is easy to interpret in an emergency.

We recommend that both risk and business impact are assessed on a short scale as follows:

Risk rating		Impact rating	
1	Very high probability	1	Very high Impact
2	High probability	2	High impact
3	Low probability	3	Low impact
4	Very low probability.	4	Very low impact

We further recommend that risk assessment and business impact review are presented in a tabular format, which also identifies location and network element. The following extract from an actual plan serves to illustrate:

Location	Network element	Type of loss or damage	Risk	Impact	Business Impact	Precautions in place.
Building 1	MIS Server	Fire,	4	1	Loss of all past and present student records, enrolment information, timetable information, staffing activities, financial information. Annual returns to DEL and other Government bodies cannot be made	Daily exports made. Weekly image produced. Disaster recovery agreement in place with Compaq (Appendix 4). Space restricted at server – no room for cups, chair etc. Security guard in place for building.
		Theft	3	1		
		Water Damage	4	1		
Vandalism	4	1				
Wind	4	1				
Accidental (eg coffee spilled)	4	1				
		Hard disc failure	3	3	As above	RAID array installed plus precautions above.
		Power Failure	3	3	As above	UPS installed

Location	Network element	Type of loss or damage	Risk	Impact	Business Impact	Precautions in place.
Building 1	Payroll server	Fire,	4	1	Payments to Full time auxiliary and ancillary staff and part time staff cannot be made. Returns to external bodies cannot be made resulting in fines.	System set to backup automatically each night. Backup tapes stored off site. 4 hour call out maintenance contract on server
		Theft	3	1		
		Water Damage	4	1		
		Vandalism	4	1		
Wind	4	1				
Accidental (eg coffee spilled)	4	1				
		Hard disc failure	3	3	As above	No RAID installed, revert to backup.
		Power Failure	3	3	As above	UPS installed
Building 2	Email server	Fire,	3	1	Loss of all internal and external electronic communication for the Institute. Loss of important records and information	Backed up daily with ARC serve Backup 6.6 for Netware Back up tapes stored off site. Physically secure and controlled environment. Server off Floor to minimise water damage.
		Theft	4	1		
		Water Damage	3	1		
		Vandalism	4	1		
		Wind	4	1		
		Accidental (eg coffee spilled)	4	1		

Etc.etc.

## Disaster recovery plan

This is the core of the document. Again the priority here is to present information in as concise a format as possible, and in a way that can be easily accessed in the event of a disaster.

Again we recommend a tabular format that summarises types of possible damage, recovery procedures, and the persons responsible. We recommend that this is laid out (a) by network element, and (b) by location. This is necessary because it is possible for important individual network elements to fail (eg MIS server, Payroll server, email server, on line learning server), that would have a significant impact on the business of the college.

Additionally a disaster can “knock out” an important location such as the main server or comms room.

The following example serves to illustrate:

### (a) By Network element

Location	Network element	Type of loss or damage	Recovery Procedures:	Persons responsible
Building 1	MIS Server	Total loss	Instigate Compaq ‘Restart’ Programme to obtain replacement server. Purchase new server using Special funds (Appendix 6) Re-build server using latest backup tape	MIS Manager MIS Manager MIS Manager
		Hardware failure	Instigate Compaq ‘Restart’ Programme to obtain replacement server.	MIS Manager
		Software failure	Re-build server using latest backup tape	MIS Manager

		Power Failure	Ensure UPS has functioned correctly Contact estate agent for building, and IT and Network Services manager to report problem. Contact NIE quoting customer service number. UPS will hold for a guaranteed 8 hours. Following power restoration MIS manager will check operation of server and where necessary restore system from tape.	MIS Manager MIS Manager Estate Agent MIS Manager
Building 1	Payroll server	Total loss	Purchase new server using Special funds (Appendix 6). Install Windows NT on server Rebuild payroll server using latest backup Configure and Test the server	MIS Manager IT Support / MIS Teams
		Hardware failure	Contact IT Support and Report failure Report Fault to vendor (4 hour response) If vendor cannot repair, treat as a Total Loss	MIS Manager IT Manager IT Manager

Etc etc

(b) By site:

Location	Type of loss or damage (assuming total loss)	Recovery Procedures:	Persons responsible
<p>Building 2 Server Room</p>	<p>Flooding / Fire</p>	<p>(a) Fire – <b>Standard fire evacuation procedures will apply. Contact the fire brigade, and other emergency services as necessary</b></p> <p><b>Only re-enter the building when it is safe to do so. Then proceed as from point (c) below.</b></p> <p>(b) Flood - <b>Raise the alarm and inform the Building Superintendent who will contact the fire brigade, and other building services as necessary. Standard evacuation procedures will apply. Only re-enter the building when it is safe to do so.</b></p> <p><b>Proceed as from point (c) below</b></p> <p>(c) The Building superintendent will:</p> <p style="padding-left: 40px;"><b>inform the Deputy Director ICT, and the IT and Network Services manager.</b></p> <p style="padding-left: 40px;"><b>assess the situation and decide whether to turn off power to the IT room.</b></p> <p><b>IT and Network Services manager will:</b></p>	<p>Buildings Office Buildings staff.</p> <p>Buildings Office Buildings staff.</p> <p>Buildings staff DD ICT</p> <p>IT and Network Services Manager</p>

		<p style="text-align: center;"><b>assess damage to equipment and remove as appropriate.</b></p> <p style="text-align: center;">consult the special equipment inventory (Appendix 1) to order replacement equipment from the supplier schedule (Appendix 6). Funds for the immediate purchase of equipment will be released from upon the agreement of Head of Finance and Head of Support Services</p> <p style="text-align: center;">contact telco to restore/re-route cabling for internet access as necessary.</p> <ul style="list-style-type: none"> <li>• The deputy director ICT will convene a panel consisting of: <ul style="list-style-type: none"> <li style="text-align: center;">Head of Support Services</li> <li style="text-align: center;">IT and Network Services Manager,</li> <li style="text-align: center;">Department of Buildings representative,</li> <li style="text-align: center;">Department of Finance Representative</li> <li style="text-align: center;">Site Managers of Building 2 and Building 3.</li> </ul> </li> </ul> <p>The panel will meet to assess whether the location at the SERVER ROOM can be re-occupied, monitor the progress of disaster recovery, and inform and update college staff.</p> <p>If the Room cannot be re-occupied within 3 days, the IT Support Centre will be re-established in <b>Rooms 4-6 in Building 3</b>. The Site</p>	<p>IT Support Team</p> <p>Head of Finance</p> <p>IT and Network Services manager.</p> <p>DD ICT</p> <p>HoD Support Services</p> <p>IT and Network Services Manager</p> <p>Buildings Representative</p> <p>Finance Representative</p> <p>Site managers BUILDING 2, Building 3.</p>
--	--	---	---



		<p>within 2 weeks.</p> <ul style="list-style-type: none"> <li>Deputy Director ICT will convene the disaster recovery panel as outlined above to discuss and evaluate alternative courses of action, and advise the directorate on courses of action to be followed.</li> </ul>	DD ICT
--	--	--	--------

**Maintenance of the plan.**

It is necessary that this plan is regularly reviewed and updated.

The Disaster Recovery Task Team should meet annually to review the plan, to organise and review the outcomes of testing, and modify the plan where appropriate. The Task Team should report to the Deputy Director ICT. Other specialists should be co-opted onto the task team as necessary.

Consideration should be given to where copies of the plan will be stored. As well as the offices of the network manager and the Deputy Director responsible for ICT, copies of the plan should be held in two fireproof safes at two separate locations. This will ensure that in the event of a major disaster at least one copy of the plan will remain intact. Copies of the plan should also be held by all members of the Disaster Recovery Task Team and be circulated to all HoDs.

## **Testing the Plan**

Because of the central role of the network in college communications, and its complexity, it would be generally ill advised to disable the network to simulate a disaster.

However the plan should be tested as fully as possible, by assuming the loss of key servers such as the email, elearning, proxy, and web server. Suppliers should be contacted to check that they can supply appropriate replacement equipment. Finance should be contacted to check that funds can be allocated. Simulate the disaster by rebuilding the email, elearning, proxy, and web server from backup, establishing them at an alternative site and temporarily placing them on the network. This can also be a training opportunity to ensure several staff have the necessary skills to rebuild systems from backup tape. College staff and students should be informed about any temporary impact on the operation of the network.

A report on the test should be presented to the Disaster recovery task team and to the Directorate Member responsible for Information and Communication Technology.

Where there is a restart agreement for the MIS server there should be an annual test of data transfer onto the Disaster Recovery Service loan server. This will provide a certificate of confirmation, which is available for audit purposes. A report on the test should be provided to the Disaster Recovery Task Team and the Assistant Director for Information and Communication Technology. Where this facility is not available sample restores from backup tape should be made.

### **Appendices to the plan.**

As already indicated the appendices should contain:

- List of servers and their locations.
- List of switches and hubs and their location
- Network diagrams
- Procedures for rebuilding the network - should contain complete instructions for rebuilding servers from backup tapes, and indicate in what order the servers should be brought back up.
- Procedures for dealing with virus attack
- Details of any maintenance or restart agreements with commercial suppliers

- Important telephone contact numbers – should contain home and work telephone numbers for Director responsible for ICT, the Disaster recovery task team, the IT Support team, key Buildings staff, and all keyholders.
- List of approved suppliers – for IT equipment

The plan should recognise that a disaster could easily occur outside college opening hours, and arrangements should be made for contacting key staff, out of hours, gaining access to college buildings, and implementing the plan.

### **Signing up to the plan. Staff Development.**

It is important that all persons named in the plan, and all Heads of Department, sign a declaration that they understand their responsibilities under the plan, and that they agree to carry them out. This should also be used as an opportunity for these staff to indicate any staff development requirements they may have, as a result of the role they are expected to play in the event of a disaster.

A particularly important group that need to sign up in this way is the keyholders. This group needs staff development on the disaster recovery plan, which is specially tailored to meet their needs, and emphasises clearly the role they will have to play as keyholders. Delivering this staff development can readily be combined with their signing up to the plan. If possible this staff development should be delivered to the keyholders by the building department representative on the Disaster Recovery Task team.

Suppliers, government agencies and other bodies named in the plan should be contacted and their role outlined. They should be asked to confirm if they will support the college in their role as described in the plan.

### **Storage of backup media.**

Access to up-to-date backup tapes is essential for the restoration of the network. Daily, weekly, monthly, and yearly backups should be made according to a pre-determined schedule, and recorded in a logbook. The tapes (except for daily backup) should be stored off site, in a fireproof safe, to ensure they are readily available.