

**IT Services**

**Disaster Recovery Plan**

Document Control

|  |  |
| --- | --- |
| Responsibility for Policy | Chief Information Officer |
| Frequency of review | Annually |
| Date | Revision/Amendment Details & Reason | Author |
| October 2011 | Initial Document | M Beecroft  |
| April 2012-2022 | Annual Update | M Beecroft |
| December 2024 | Amendments made due to the introduction of Degree Apprenticeships, including formatting and cosmetic changes | John Cross |

## Introduction

The University relies heavily on the IT facilities to provide the required services to students, apprentices, academics and administrative staff. Consequently, IT services are a critical component in the daily operations at the University, requiring a comprehensive IT Disaster Recovery Plan.

Major incidents at the University are managed by a core Incident Management Team comprising: -

* Vice Chancellor
* Head of Governance
* Executive Director of Finance, Services and Resources
* Director of Estates
* Deputy Vice Chancellor and Provost
* Head of Legal Services, Governance and Risk
* Campus Manager

There will be other members of the Team, dependent on the specific incident e.g. Chief Information Officer, Head of IT, Director People Services, Director of Student Life. The support and advice of outside services (e.g. Ambulance, Police, Gas) may also be needed to enable the plan to function properly.

The IT Disaster Recovery Plan presents the actions which will be taken in response to a disaster affecting IT services, with the key aim being to allow basic business functions to resume and continue until such time as all systems can be restored fully.

For financial reasons, the University does not run redundant servers that would minimize potential business disruption in the event of a disaster. Additionally, the university does not utilise a redundant “warm-site” or “hot-site” for quick recovery of the Data Centre.

This plan is reviewed and updated yearly by IT Services and approved by the Pro Vice Chancellor (Research).

A hard copy of this plan is stored as follows:

* IT safe in Social Sciences Building A
* Chief Information Officer Office (HCA)
* Desktop / AVA Team Leader Office (HCA)
* Desktop / AVA Office (Creative Campus)

## Scope

Due to the uncertainty regarding the magnitude of any potential disaster on the campus, the plan will only address the recovery of systems under the direct control of IT Services and that are critical for business continuity. This includes the following major areas:

* Servers
* Data Networks (networks, data storage)
* Logon facilities
* Desktop Equipment (Offices, Classrooms, Labs)
* Administration Services (Student Record Management (SRM), SITS, E-Reporter, CIPHR)
* Finance (Agresso)
* Electronic Mail and Internet Services
* Learning Resources (Network drives, Library facilities, Moodle)
* Miscellaneous Services (Accommodation and Conferencing System, Security Access Control System, E-Profile, Course Design and Approval)

The plan covers all phases of any IT related disaster. These phases include:

* Incident Response
* Assessment and Disaster Declaration
* Incident Planning and Recovery
* Post Incident Review

## Assumptions

This plan is based on the following assumptions:

* Once an incident covered by this plan has been declared a disaster, the appropriate priority will be given to the recovery effort. The resources and support required as outlined in the plan will be made available.
* The safety of students, including Degree Apprentices and staff are the priority and the safeguard of such will supersede concerns specific to hardware, software and other recovery needs.
* Depending on the severity of the disaster, other departments may be required to modify their operations to accommodate any changes in system performance, computer availability and physical location until a full recovery has been completed.
* IT Services will assist other departments to have contingency plans for their operations, which include operating without IT systems for an extended period of time.
* The content of this plan may be modified and substantial deviation may be required in the event of unusual or unforeseen circumstances. These circumstances are to be determined by the Disaster Recovery Team under the guidance and approval of the Chief Information Officer, or Head of IT

## Communication Plan

The communication plan will provide policies and procedures to coordinate communications with staff and students within the university. If communication is required between the University and the media or the public, this will be conducted via the Deputy Vice Chancellor and Provost Office.

The plan will not only address communication issues but also includes procedures for the rapid identification of potentially harmful situations and the methods for responding to these situations quickly and effectively.

**The objectives of the plan will be to: -**

* assure that communications activity is coordinated via the designated individuals
* factually assess the situation and determine whether a communications response is warranted
* implement immediate communications to staff and students, apprentices and employers of Degree Apprenticeships where relevant
* ensure on-going communication of facts about the incident
* minimize rumours
* restore confidence

Once accurate information has been obtained, the Head of IT will recommend whether an immediate response is necessary and, if so, will consult with:

* Chief Information Officer
* Chief Operating Officer
* Head of Legal Services, Governance and Risk

The relevant groups to be notified of an incident will be identified. It will be important to keep administration, faculty staff, students and apprentices informed of appropriate details and actions taken by the University during an incident.  Effective communications will help quell rumours, maintain morale, and ensure continued orderly operations of the university.

A designated spokesperson will be identified who will agree the content and timing of any communication issued by the University during an incident. Frequent updates will be provided to staff, students, apprentices and appropriate administrators.

The method of communicating will be determined by the facilities available. Potential methods of communication include:-

* Notices on the University Web Site
* Updates on key applications such as the Student Record Management (SRM), SITS and Moodle
* Telephone updates to key areas such as Student Administration, Faculty Offices, Finance, Library, Student Union, People Services, Telephone Switchboard
* Recorded messages on telephones
* Posters in key areas such as Library, Halls of Residence, Building Reception areas, classrooms
* Personal visits to appropriate areas of the University

Following any incident, appropriate action must take place to ensure that members of the University community, and others as necessary, receive information to bring closure to the incident.  Consideration will also be given to identifying and implementing measures to improve the action plan used during the incident.

## Management Details

**Chief Information Officer**

|  |  |
| --- | --- |
| **Home Phone Number** | 07720072778 |
| **Mobile Phone Number** | 07720072778 |
|  **Work email** |  crossj1@hope.ac.uk |

**Alternative Senior Management**

|  |  |
| --- | --- |
| **Home Phone Number** | 07736106184 |
| **Mobile Phone Number** | 07736106184 |
|  **Work email** |  stonej@hope.ac.uk |

**IT Incident Team:**

|  |
| --- |
| Chief Information Officer |
| IT Technical Architect  |
| Desktop / AVA Team Leader |
| Support Desk Manager |

**Major Incident Management Team:**

|  |
| --- |
| Vice Chancellor |
| Chief Operating Officer (COO) |
| Director of Estates |
| Head of Legal Services, Governance and Risk |
| Deputy Vice Chancellor and Provost |
| Head of Governance  |
| Campus Manager |

## Staff / suppliers / access rights / keyholders

**Network / Server Recovery Team**

The Network / Server Recovery Team support the University central computing environment comprising of:-

* the servers and storage devices housed in FML and the Sheppard-Worlock Library
* network infrastructure including all fibres, cabling, switches, routers and network applications

The primary function of this group is:-

* the restoration of the existing data centres to a condition where individual recovery teams can accomplish their responsibilities with regard to application restoration
* the restoration of LAN and servers to the most recent pre-disaster configuration in cases where data and network loss is significant. In less severe circumstances, the team is responsible for restoring the system to an operational status as necessitated by any network hardware failures or other circumstances that could result in diminished performance.

The team should be mobilized only in the event that a disaster occurs which impacts the ability of the existing central computing facility to support the servers and applications running there.

This recovery effort will normally be accomplished prior to most other recovery efforts on campus as having a central computing facility is a prerequisite for the recovery of most applications and IT services to the campus.

|  |  |
| --- | --- |
| **Name** | \* IT Technical Architect (NS) (Recovery Team Lead) |
|  | \* IT Technical Architect (JS) |
|  | \* Senior Network Engineer |

***\**** *hold access rights for the FML and SWL server rooms.*

**Desktop / AVA Recovery Team**

The Desktop / AVA Recovery Team support the University desktop / laptop / mobile hardware, client applications, classrooms and labs.

The primary function of this group is the restoration of these facilities to a usable condition. During the recovery effort, the team is not responsible for restoration of any data the user may have on their desktop computer.

The team should be mobilized in the event that any component of the network or infrastructure experiences a significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

The leader of the Desktop / AVA Team has the responsibility to keep the Head of IT & Chief Information Officer up to date regarding the nature of the disaster and the steps being taken to address the situation. The co-ordination of this recovery effort will be accomplished with other recovery efforts on campus by the Chief Information Officer.

|  |  |
| --- | --- |
| **Name** | Desktop/AVA Team Leader (Recovery Team Leader AW) |
|  | Desktop AV Officer |
|  | Desktop/AV Officer |
|  | Desktop/AV Officer |
|  | Desktop Support Engineer |

**Application Recovery Team**

The Application Recovery Team is composed of the specialists within IT Services who support the various application systems utilised by the University.

The primary function of this group is the restoration of all critical business applications to the most recent pre-disaster configuration in cases where data loss is significant. In less severe circumstances the team is responsible for restoring the applications to an operational status as necessitated by any hardware failures, network outages or other circumstances that could result in diminished system performance.

The team should be mobilized in the event that the applications experience a significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

The IT Applications Development Manager has the responsibility to keep the Head of IT & Chief Information Officer up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of the Application recovery effort will be accomplished with other recovery efforts on campus by the Head of IT, or Chief Information Officer

|  |  |
| --- | --- |
| **Name** | Corporate Applications Developer (Recovery Team Leader KW) |
|  | Corporate Applications Developer (JK) |
|  | Corporate Applications Developer (SITS CM)  |
|  | Corporate Applications Developer (DJ) |

## Supplier Details

The key suppliers who might be involved in the restoration of services following a significant interruption are: -

|  |  |
| --- | --- |
| **Vendor Name** | **Services** |
| ProofID | Identity Management |
|  | IDM Driver |
| Oracle | Oracle Database |
| Unit4 | Finance system |
| Compel | Ciphr system |
|  | Call Logger Maintenance |
| Dell Computer Corporation | Server Hardware Maintenance |
| Aspex | Salto Security System |
| Poscom | Data / Voice Cabler |
| Switchshop | Ruckus Wireless |
|  | Switch / Router hardware |
| GV Multi Media | AVA Hardware  |
| Vodafone | Telephone Calls |
| Tribal | SITS system |
| Terminal Four | Hope Web Site |
| Ex Libris | Library System |

1. **Disaster Preparedness**

A critical requirement for disaster recovery is ensuring that all necessary information is available to ensure that hardware, software, and data can be returned to a state as close to “pre-disaster” as possible. Specifically, this section addresses the backup and storage policies as well as documentation related to hardware configurations, applications, operating systems, support packages, and operating procedures.

**Data Recovery Information:**

Backup/Recovery files are required to return systems to a state where they contain the information and data that was resident on the system shortly prior to the disaster. Details of the backups taken by the University are held in the document Electronic Data Backup Policy and Procedures.

N.B. The University does not backup and restore information/data located on individual desktop hard drives. Only the servers located in the Data Centre are backed up and, therefore, only data resident on these systems will be able to be recovered. In the event that a disaster occurs on the campus which destroys personal computers, the information located on these computers will be extremely difficult or impossible to recover.

IT Services recommends and encourages the use of network drives (on servers) to store all important files. The recovery of data not backed up to a network drive and/or full system backups are not covered under this plan.

**Data Centre and Server Recovery Information:**

In the event of any disaster which disrupts the operations in the Data Centre, re-establishing the Data Centre will be the highest priority and a prerequisite for any IT recovery. As such, IT Services is required to have detailed information and records on the configuration of the Data Centre, network and all servers and ancillary equipment located in the Data Centre. Detailed information is held in the document LHU Current State Model located in the Disaster Recovery folder on the Z drive (ITServices\ITS-TeamLeaders\Disaster Recovery). This document is included in the daily backups of the Z Drive. A paper copy is also held in the safe in the Business School. The Head of IT is responsible for keeping the document up to date.

**Application Recovery Information:**

Information necessary for the recovery and proper configuration of all application software located on the central servers is critical to assure that applications are recovered in the identical configuration as they existed prior to the disaster. Detailed information on critical central applications is held in the document LHU Current State Model located in the Disaster Recovery folder on the Z drive (ITServices \ITS-Team Leaders\Disaster Recovery).

**Desktop Equipment Recovery Information:**

Information necessary for the recovery and proper configuration of all desktop computers and printers supported by IT Services is critical to assure that client systems can be restored to a configuration equivalent to pre-disaster status. Detailed information on client systems (both PC and MAC) is held in the document LHU Current State Model located in the Disaster Recovery folder on the Z drive (ITServices\ITS-TeamLeaders\Disaster Recovery).

1. **Incident Procedures**

**Incident Response**

The need for the Major Incident procedure to be invoked and the membership of the Incident Recovery team will be dependent on the size and type incident. Examples of situations which would normally activate the team include: -

* Severe structural damage to the server rooms where personal safety is in question, and where assessment must be completed to assure the building is acceptable for access.
* Environmentally hazardous situations such as fires, explosions, or possible chemical or biological contaminations where the situation must be contained prior to building occupancy.
* Flooding or other situations which may pose the risk of electrical shock or other life threatening situations.

**IT Incident Team**

The role of the IT Incident Team (under the direction of the IT Incident Director) is to coordinate activities from initial notification to recovery completion. Primary initial activities of the team are:

Upon the occurrence of an incident affecting the IT services, the Chief Operating Officer (COO) and the Head of Legal Services, Governance and Risk will be notified by the Chief Information Officer or nominated deputy, usually the Head of IT. A high level assessment of the size and extent of the incident will be provided. Based on this information, the Chief Information Officer will assume the responsibilities of the IT Incident Director (unless delegated to Head of IT), and will contact the other members of the IT Incident Team. The following basic information will be provided:-

* Brief overview of the incident, buildings affected, etc.
* Where the Incident will be managed from
* Scheduled time to meet at the incident management location for initial briefing
* Any additional information beneficial at this point.

The IT Incident Team will assess the situation, perform a walk-through of affected areas as allowed and make a joint determination as to the extent of the damage and required recovery effort. Based on this assessment, the team will make a determination as to whether the situation can be classified as “routine” and handled via normal processes, or if a formal IT disaster needs to be declared.

* For a routine incident, the areas affected by the incident are identified and the appropriate personnel are contacted to report to work to evaluate and resolve the situation.
* In the case of a disaster, the Head of IT in the first instance, will contact the Chief Information Officer, who will subsequently contact the Executive Director of Finance, Services and Resources and the Head of Legal Services to notify them that an IT Disaster has been declared.
* In the event of a significant disruption to critical activities supporting learning, teaching, research, and infrastructure, employers of Degree Apprenticeships would be informed of the recovery plan and interim arrangements

The IT Incident Team identifies which areas of the IT infrastructure are affected and

contacts the members of the specific Disaster Recovery Teams. Team members will be provided with the following information:

* Brief overview of what occurred
* Location and time for teams to meet
* Additional information as required.

Once an IT disaster has been declared, the ongoing responsibilities of the IT Incident Director include:

* Securing all IT facilities involved in the incident to prevent personnel injury and minimize additional hardware/software damage.
* Supervise, coordinate, communicate, and prioritise all recovery activities with all other internal / external agencies
* Hold regular Disaster Recovery Team meetings/briefings with team leads and designees.
* Appointing and replacing members of the individual recovery teams who are absent, disabled, ill or otherwise unable to participate in the process.
* Provide regular updates to the Chief Operating Officer (COO) and the Head of Governance on the status of the recovery effort.
* Approve and acquire resources identified by individual recovery teams.
* Make final determination and assessment as to recovery status, and determine when IT services can resume at an adequate level.

**Disaster Recovery Teams**

Four disaster recovery teams can be organized to respond to disasters of various type, size, and location. Any or all of these teams may be mobilized depending on the scale of the disaster. It is the responsibility of the IT Incident Director to determine which Disaster Recover Teams to mobilize following the declaration of a disaster.

Each team will utilize their respective procedures, disaster recovery information, technical expertise and recovery tools to successfully return the services to operational status. While recovery by multiple teams may be able to occur in parallel, the Data Centre and Network infrastructure will normally be assigned the highest priority as full operational recovery of most other systems cannot occur until these areas are operational.

The roles and responsibilities of each of the Disaster Recovery Teams are set out in Appendix A below.

**General System/Application Recovery Procedures/Outline**

The following steps are guidelines to be followed for the overall restoration of systems located at the University. While each Recovery Team has specific duties and responsibilities, coordination between the various teams is required to restore operations to the users. While the coordination and extent of personnel involved will depend on the type and severity of the disaster, the following steps may be required:

* Determine extent of damage and make determination as to the following:
	+ Server Room availability
	+ If one of the server rooms is irrecoverable, consolidate activity in the remaining server room.
	+ If neither are available, assess the potential usage of the Creative Campus and other switch rooms in Eden and the old server room in FML.
* Determine extent of applications affected e.g.
	+ Agresso
	+ SITS
	+ Moodle
	+ CIPHR
	+ Web Services
* Determine extent of desktop/client systems affected throughout the campus
* Secure facility as necessary to prevent personal injury and further damage to IT systems
	+ Shutdown any active components.
	+ Physically secure facilities (Data Centre, Communication Rooms, etc.) as necessary to prevent unauthorized access.
* Retrieve most recent back-up. Prepare back-up media for transfer to data centre as determined during the initial assessment.
* Verify operational ability of all equipment on-site in the affected areas (servers, network equipment, ancillary equipment, etc.). Depending on the type and scope of the disaster, the following activities will be conducted to adequately assess the overall damage and impact to the campus, and to assure a comprehensive plan for recovery:
	+ Perform comprehensive cable, fibre, and communications line testing
	+ Assess all communication cabinets and racks/equipment for damage
	+ Test primary copper data feeds for destruction or deterioration
	+ Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that have been exposed to water or other agents.
	+ Assess all equipment with air filtration systems to assure adequate ventilation remains.

If equipment is not operational, initiate actions to repair or replace as needed.

* Test systems and communication equipment as required to validate physical operation and performance
	+ Server testing
	+ Network testing
	+ Desktop/Client testing
* Upon restoration of the Data Centres and servers to operational state:-
	+ Load Operating System and test/validate
	+ Load Application Software and test/validate
	+ Load Data and verify integrity
* Verify overall performance of specific system(s) and report readiness to IT Incident Director and user community.

## Disaster Recovery Plan Testing

The two major criteria are the ability to recover the business process within their Recovery Time Objectives with data at the defined Recovery Time Objective (these are detailed in the Business Impact Analysis document).

The ability to recover business critical applications is tested as set out in the Electronic Data Backup Policy and Procedures.

## Maintaining the Disaster Recovery Plan

Maintenance of the Disaster Recovery Plan is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans and be up to date.

The Disaster Recovery Plan and its associated documents will be reviewed on an annual basis to ensure their currency.

## Awareness, Education and Training

It is essential that all personnel who could potentially be involved in a disaster recovery are aware of the Plan and be knowledgeable of its contents and their own related duties and responsibilities.

All IT staff will be briefed on the Disaster Recovery Plan and their roles and responsibilities within it on an annual basis.

University governance committees will also be made aware of the content and location of the plans. In particular, they will be informed of who to contact if they believe that an incident has occurred.

Copies of all relevant documents will be made available on the Shared Network drives accessible by the staff and a paper copy will be kept in the safe in the Business School.

The on-going training processes within IT Services will also ensure that multiple staff have the skills and knowledge to perform recovery tasks in the event of an incident.

## Appendix A: Responsibilities of Disaster Recovery Teams

**Network / Server Recovery Team**

* Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
* Assess damage and make recommendations for recovery of Data Facility.
* Identify other individuals required to assist in recovery of data centre
* Develop an overall recovery plan and schedule, focusing on highest priority servers for specific facilities / applications first.
* Coordinate hardware and software replacements with vendors
* Recall backup/recovery tapes from storage, as required to return damaged systems to full performance.
* Oversee recovery of data centre based on established priorities.
* Coordinate data centre recovery with other recovery efforts on campus.
* Provide scheduled recovery status updates to the IT Incident Director to ensure full understanding of the situation and the recovery effort.
* Verify and certify restoration of the data centre to pre-disaster functionality.

**Desktop / AVA Recovery Team**

* Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
* Assess damage at all areas affected, and make recommendations for recovery.
* Identify other individuals required to assist in recovery of desktop services, and report this information to the IT Incident Director for action.
* Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure/desktop services first
* Coordinate hardware and software replacement with vendors
* Oversee recovery of desktop computing services (desktops, printers, etc.) based on established priorities.
* Coordinate recovery with other recovery efforts on campus.
* Provide scheduled recovery status updates to the IT Incident Director to ensure full understanding of the situation and the recovery effort.
* Verify and certify restoration of the desktops to pre-disaster functionality.

**Application Recovery Team**

* Assess damage and make recommendations for recovery of applications
* Identify other individuals required to assist in recovery of these applications, and report this information to the Head of IT for action.
* If appropriate, restore limited system function and inform user community of the restrictions on usage and/or availability.
* Coordinate software replacement with vendor as required
* Coordinate application services recovery with other recovery efforts.
* Execute plan to restore application services to full function.
* Provide scheduled recovery status updates to the IT Incident Director to ensure full understanding of the situation and the recovery effort.
* Verify and certify restoration of the application services to pre-disaster functionality.

**APPENDIX B: Asset Management Information**

Detailed information of IT Assets is documented in the LHU Current State Model located in the Disaster Recovery folder on the Z drive (ITServices\ITS-TeamLeaders\Disaster Recovery). This includes information relating to:-

* Servers
* Switches
* Routers
* Application Software Configuration Information
* Desktop Equipment

**APPENDIX C: System Backup/Copy Retention Periods**

All business critical applications servers are backed up. Details of these backups are contained in the document Electronic Data Backup Policy and Procedures located in the Disaster Recovery folder on the Z drive (ITServices\ITS-TeamLeaders\Disaster Recovery).

**APPENDIX D: IT Recovery Priority List**

The priorities for the recovery of IT Services to the university are set out in the document Business Impact Analysis located in the Disaster Recovery folder on the Z drive (ITServices\ITS-TeamLeaders\Disaster Recovery).

These priorities are based on the relationship between systems, and the pre-requisite nature of many of the items in order to be able to return full services to the campus.

* Data Centre
* Network Services
* Application Services
* Desktop Services