Finance and Information Technology Directorate

Disaster Recovery Policy

Contents

0. Revision History

Version 1.0 October 2002 – October 2003.
Version 2.0 August 2007.
Version 3.0 May 2009.
Version 4.0 January 2012

Next major revision scheduled for January 2014

This policy should be used in conjunction with Business Impact Analysis which is being used to assess the requirements and priorities of business units. Such analysis is used to create Business Continuity Procedures for each application.

Such procedures should document

- Recovery strategy
- Roles and responsibilities
- Key contacts
- Technical configuration of systems

1. Background

IT systems have assumed a crucial importance in the day-to-day work of the University. Many systems are critical to the every-day operation of administrative tasks, research and for learning and teaching. It is important to assess the impact on the University community of any major prolonged loss of service.

The University maintains a Disaster Recovery Policy written to cope with any disaster befalling critical IT systems. The policy is written by the Directorate of Finance & I.T. and is reviewed every two years. Significant service disruption may include network loss; server loss due to fire, theft or accident; building loss; loss of data and software or hardware failure. Consideration is being made of the business critical nature of IT systems, and questions are asked of our customers as to their own planning in the event of any loss of service affecting their normal working.

It should be noted that while this policy covers the entire network infrastructure and telephone systems of the University, there are significant IT systems managed by other departments which are not benefiting from the I.T. Services server room infrastructure. Such systems should be subject to their own disaster recovery and business continuity plans.

2. Risks

A disaster in IT terms would be some event which led to an extended loss of service or loss of critical data. Loss of service might include:

- Internet access to external sites
- Internet access from external sites to Keele web services
- Disruption to network access for whole schools or buildings
- Loss of application service to e.g. Student records, VLE
- Loss of email service
- Loss of directory services

Loss of data might include:

- Business data systems, e.g. student records, VLE
- Web server pages
- Managed staff and student filestore

Significant events would include:

- Building loss or other environmental event (e.g. fire, flood)
- Theft of equipment
- Malicious damage, possibly via electronic attack
- Hardware failure
- Loss of significant data due to error
- Loss of staff

Major Consequences:

- Loss of revenue
- Disruption to academic programs
- Loss of student recruitment
- Delays in payments
- Reputational damage

Major network events would include:

- Loss of external networks (JANET – outside Keele's control)
- Loss of network links between buildings and campuses
- Loss of core networking equipment e.g. switches
- Failure of network control software
- Loss of key staff

3. General Principles of Service Provision

This section describes some of the parameters used in service design to deliver a robust service. Each service is then implemented within a well-understood framework using re-usable components.

- A small number of hardware suppliers (e.g. Cisco, Dell, Sun)
- Recognised software platforms (Microsoft, Redhat Linux, Solaris)
- Redundancy: multiple servers and switches per service
- Redundancy: multiple power supplies, raid storage
- Virtualization of hardware resources; server instance cloning
- Distribution of hardware and services between server rooms
- Re-use of well understood mechanisms for service delivery
- Power: use of multiple power sources, UPS technology
- Hardware and software maintenance contracts
- Backup: all significant data is backed up disk to disk and disk to tape
- Strategic data is archived to tape and stored in secure repositories off-site
- Restores of archived data are tested
- Replacement of hardware is tested where required
- Fault tolerant network connection
- Networks segmented and protected by classes of service
- Firewalls deployed at all significant network nodes and servers
- Anti-virus and anti-phishing software deployed on mail gateways
- At least two staff familiar with the support of each service

4. Server Rooms

There are two major server rooms of similar size, physically well-separated in two buildings. Each of the major server rooms is designed on the same lines with redundant power sources (including backup power generators), significant UPS capacity, full air-conditioning, fire and intruder alarms, and server racks.

A further server room is used at the University Hospital campus for hospital-based services and remote archiving. Any service located there could be hosted on the Keele campus if necessary.

The core network systems for the LAN are mirrored in both server rooms, there are separate connections to JANET terminating in each room, and the servers are equally distributed (in both type and function) between them.

The major goal in operating with this level of duplication and capacity is to allow for one location to take over all of the functions of both in the event of the loss of all facilities in one of them.

In the opinion of the University's insurers (May 2009) the provision of two server rooms is sufficient to mitigate the risk of total loss and there should be no need for extra costs relating to engaging an off-site disaster recovery resource.

5. Local Area Network

The local network offers considerable resilience against disaster. The two main site routers are situated in each of the server rooms and the routers have redundant processors and power supplies.

In the event of major loss of network function within one server room, the other server room would still be able to provide the necessary network infrastructure to service I.T. systems.

Each major building is directly connected to both server rooms and wherever possible physically diverse routes have been taken.

The University Hospital campus is served by a dedicated high-speed link from the Keele campus. A lower speed backup link is also maintained in case of service disruption.

Our links to JANET and the Internet are provided through Net North West which is a Metropolitan Area Network based at Manchester University. External links to Net North West come into both server rooms and go to separate locations at Manchester University via diverse routes.

The LAN consists of fibre optic cables in the main trunk and copper cables within buildings. This reduces the risk of service disruption due to lightning strike between buildings.

Standard Cisco hardware is deployed at the network nodes and enough spares are held on site to deal with moderate levels of failure. All configuration files are generated and stored on central servers. Most network kit is readily replaceable in 1-3 working days.

The network equipment is physically protected within the major server rooms and smaller access points around the campus. Access to such rooms is controlled and alarmed at the

major nodes. Maintenance is provided in-house using trained staff and a sufficient stock of spares.

Network security is enhanced by using firewalls protecting the LAN from the Internet, and further access controls based on the type of use of particular subnets.

Anti-virus and anti-SPAM measures are implemented on the mail gateways, and Windows anti-virus is used on all Windows servers and desktop PCs.

6. Common Services

Oracle

Oracle database services run on Dell hardware with attached RAID storage distributed between server rooms. All databases are configured in a similar fashion (depending to a degree on the application being supported). Strategic databases (Finance, SITS Live, VLE) are replicated in real time to standby databases which can be manually instructed to take over at short notice in the event of a significant failure.

Backups

Services are backed up to disk, in all cases on to servers in the opposing server room. In some cases multiple backups are available. The backup system also generates some snapshots to tape, which are stored in a fire-safe. Every week encrypted snapshots from the Keele campus servers are written to servers based at the UHNS.

7. Cloud Services

Keele is subscribed to an increasing number of services in the cloud. Clearly the major local risk of disruption to such services is dependent upon the health of the network. However we have assessed the risk of disruption to those cloud services in the event of a failure at the service provider's end.

Significant cloud services adopted are

- Googleapps and gmail (taught students from September 2011, all others from Summer 2012)
- eProcurement system
- Eduserv Openathens service (local service with remote elements)
- EduRoam service (local and remote elements)

8. Academic Service

IT systems identified as important to the academic staff and student service are

- Outgoing internet access (via JANET)
- Incoming internet access to web servers and email
- Outgoing access to googleapps and gmail
- IT Registration System
- Directory services (LDAP, Active Directory)
- The VLE
- Hallsnet
- Web services
- Local network access to campus services

- Electronic mail systems
- Electronic diary
- Managed filestore
- Library system
- OpenAthens single sign-on, Eduroam service
- eVision

With the exception of the library system which runs on Oracle/Solaris hardware, the majority of the academic service is based on servers using the Intel platform and running Linux. Servers tend to be bought in batches with identical specification and in sufficient quantity to provide for testing and spares. A manufacturer's five year next business day hardware support contract is purchased with each server. From time to time such warranties are extended. The servers use a Redhat based Linux distribution. Security patches are routinely and regularly applied.

There are a number of significant applications running on the Windows Server platform. Generally these are virtualized on Linux servers using KVM. Such applications are organised so that there is a primary service instance in one server room and a standby backup service of a similar configuration held in the other server room.

In the event of major disruption services should be relatively easy to move, either to commodity Intel hardware or to a virtualized platform. Many could be hosted temporarily on desktop PCs, of which there are a substantial number. However some services would inevitably be slowed down or reduced.

Depending on the time of year some choices may be possible between restoring the staff service or the student service, although much is common to both.

The library's book circulation system can be replaced by a paper-based record on a short-term basis. The catalogue would be unavailable until a full restore took place. At the moment we have spare replacement hardware, and a full restore would be assisted by the maintenance agreement in place with the software suppliers.

Both the I.T. Service account registration system and the library borrower records rely on data extracted from administrative systems using Oracle databases. In the event of service loss affecting those systems, both accounts and borrowers could be managed manually. Such data is used to populate the LDAP directory, which is then used widely amongst disparate systems for purposes such as authentication and access control. The LDAP service being strategically important is mirrored between servers in the two server rooms.

The print service runs on a virtualized Windows server with a standby system in place. The print system is subject to a maintenance contract covering the application.

9. Administrative Service

The administrative service is characterized by an increasingly diverse set of business-critical applications which are subjected to thorough business impact analyses. Most of these business systems are able to function in a reduced state for up to five working days in any emergency. In the case of a single server room loss, this should allow enough time to restore missing services to the other server room. Such services would not cope in the

event of the loss of two server rooms, but the risk of this happening is regarded as minimal.

The majority of these applications require Oracle software and databases, though some use Microsoft SQL Server.

Administrative systems currently identified as important are included in Annex C.

10. Infrastructure Services

An infrastructure service delivers information at a relatively low-level to other I.T. services. Each one is replicated in some way and will typically be run on at least two servers distributed between server rooms and located on different segments of the campus LAN:

- Name service (dns)
- Directory services (LDAP, Active Directory)
- OpenAthens sign-on service
- Radius service (Eduroam)
- Network discovery service (dhcp)
- Time service (ntp)
- Web proxies
- Web accelerators and load balancers
- Mail gateways to the Internet
- Lab PC imaging
- Printing Services
- System logging service
- Googleapps synchronization (accounts and contacts)

11. Telephones

The University telephone system is IP based and is integrated into the network and server infrastructure. Mitel equipment and Dell servers are used to host the services and there is sufficient redundancy in the equipment. System data is integrated into the University LDAP service. There is a maintenance contract associated with the telephone system. The telephone service is resilient in the event of the loss of one of the server rooms.

12. Contingency Plans

12.1. Network

A Networking Strategy document is attached as Annex B. Major factors for contingency planning are

- Widespread use of identical hardware
- Dual interconnect to each major node on the LAN
- At least two routes into each building
- Dual connections to the Internet
- Replicated servers for network support, e.g. firewalls, caches, proxies
- Provision of spare hardware
- Maintenance contract for hardware and software on critical components

12.2. Common and Academic Services

The academic service is built and deployed on the following principles

- Using identical specification hardware for similar tasks
- Splitting individual services across a number of servers
- Using a limited range of operating system configurations
- Storing data on raid arrays
- Maintaining a configuration repository for servers
- Deploying a comprehensive archiving strategy

12.3. Administrative Service

Principles similar to those used for the academic service govern the choice and deployment of server hardware and software for administrative computing systems.

Many of the applications are dependent upon Oracle database software and tools. The underlying Oracle database service is organised as a set of primary and standby database servers using techniques recommended by Oracle. Transaction data is logged in such a way that recovery in the event of a disaster may be made to a point in time close to when such disaster occurs. Web-based services reliant upon such databases can be migrated quickly across to other similar hardware or virtual platforms.

Annex A: Physical Environment

The server rooms are approximately 600 metres apart and are contained within brick built buildings. External security is maintained via alarms and strong security doors. Access is restricted to I.T. staff and approved contractors under supervision.

Each room is similarly configured with a generator backed power source delivered through uninterruptible power supplies. The environment is controlled with multiple, redundant air-conditioning units. Power to servers is delivered through programmable power distribution switches which may be controlled and monitored over the network.

All servers and network equipment are housed in industry standard racks and are secured in place. Equal numbers of servers are located in each server room, and within classes of server the balance is also maintained.

There is redundancy available at all of the above physical levels.

Annex B: Campus Network

Main Campus Network

The main physical design of the network is a dual star topology with each major building being connected by a direct link to each server room. Each link takes a separate physical path so that a “man with a digger” failure will not affect both connections.

The network design is based on standard Cisco Hardware. The main routers in each server room are Cisco 6500s. These have dual supervisors and dual power supplies. Both systems have a 4 hour response maintenance cover. The system has been designed so that each half of the network can run independently if so required. The main power supply to each machine room is UPS and generator backed.

The distribution layer routers in each building are based on Cisco 3560/3750 range of routing switches. The larger buildings (greater than 200 hosts) have duplicate routing hardware and in the event of a single failure the building network will continue to function.

We hold a set of maintenance spares for this equipment and all the configurations are generated and stored on central servers. A replacement device could be configured and installed in a matter of a few hours. These routers can route to either server room in the event of a failure.

All the edge equipment is based on Cisco 2950 equipment. We also hold spares and configurations for this equipment.

Halls Network

The halls network is designed along similar lines. In each of the Halls there are Cisco 3560/3750 routers with Cisco 2900/2950s at the edge of the network. Each piece of routing equipment is connected to both routers in the main server rooms.

Local spares are held for this equipment and all configurations are stored centrally.

UNHS Network

The on-site network at UHNS is migrating to a service managed by the PFI supplier. Keele maintains some network equipment and servers on their site to manage the connection of the Keele and Hospital networks.

Telephone Network

The telephone service depends upon the main campus network.

Annex C: Business Continuity Requirements

Significant Administrative systems supported by IT Services

- Payroll & Human Resources
- Student Records and Fees (SCIMS, eVision)
- Finance
- eProcurement
- Student Accommodation
- Timetabling
- Purchase Ordering
- Staff Housing Rents, Monthly Debtors and Miscellaneous Invoicing.
- Research Applications (Pfact)
- Research Finance
- Research repository (IntraLibrary)
- Estates Job Costing (Q5)
- Estates Energy Management
- Salary Forecasting (Finance)
- Staff Expense Claims
- Staff Sickness Recording and Processing
- Alumni Database (MAC)
- Teaching and Pool Room Bookings
- Equipment Inventory (Finance)
- Vehicle Registration Number Logging (Planning)
- FEC Diaries
- Web content management system for University web site

Significant services supported by CBE

- CBE Finance and Purchase Ordering
- Keele Card
- Point of Sale Systems
- Conferencing
- Time and Attendance

Effect of Limited Service on systems supported by IT Services

The following systems would be provided and supported in the following order of priority:

- All infrastructure services
- Core networks
- Oracle database servers
- Telephone service
- Clearing if relevant
- Electronic mail
- Filestore
- Main University web site
- Payroll & Personnel
- Student Records and Fees

- Electronic mail
- Filestore
- Finance Package
- Student Accommodation
- Debtor Interfaces
- Staff Housing Rental, Monthly Debtors and Miscellaneous Invoicing
- Research
- Research Databases and Research Publications at critical periods
- Budgeting System
- Timetabling

The remaining systems, described below, would not be supported on the limited service, but would await return of a full service.

- Departmental Financial Systems
- Procurement
- Salary Estimates (Finance)
- Alumni Database (MAC)
- Pool Room Bookings (Planning)
- Equipment Inventory (Finance)
- Vehicle Registration Number Logging (Estates)