1.0 Purpose

This document describes the situations that may arise, and the likely resolution, in the event that a disaster occurs to [company name] computer systems, or critical applications contained thereon.

2.0 Scope of Application

This SOP applies to computer systems at [company name] UK.

3.0 Definitions

- **LAN:** Local Area Network. In this document, "UK LAN" and similar terms refer to the company's internal computer network at the UK site premises.
- **RAID:** Redundant Array of Independent Drives. A fault-tolerant data storage system. (See section 5.2.)
- **DNS:** Domain Name System. The system responsible for resolving names such as "www.google.co.uk" into raw numeric network addresses.
- **DHCP:** Dynamic Host Configuration Protocol. An automated system for configuring the network settings of client machines.

4.0 Responsibilities

Management is responsible for ensuring that a Disaster Recovery Plan is in place and that contingencies are allowed for.

The System Administrator is responsible for implementing the Disaster Recovery Plan.

5.0 System Overview

5.1 Equipment and Organisation

a) [company name] UK is located in a single building on a business park: [address]

b) Currently there are 2 servers, all of which reside in the server room in [location]. They are:

I. [server name] (Windows 2003 Server). This server provides DNS and DHCP network services, and is responsible for user authentication.

II. [server name] (Windows 2003 Server). This is the main file server and also provides print services.

c) All servers are connected by a *local area network* (LAN). This is a TCP/IP Ethernet network operating at up to 1,000 megabits/second. Most PCs are also connected to this network. (A few are stand-alone PCs for instrument control.) There is a network switch unit in the server room. This connects the PCs to each other and to the servers.

d) The LAN is connected to the Internet through equipment residing in the server room. The signal then passes through some ISP-provided hardware and into an underground fiber optic link to the ISP's premises.

e) The company also operates a *virtual private network* (VPN), which allows secure connection between the different company sites world-wide. It also allows secure remote access for company employees.

5.2 Disaster Precautions

a) An integral part of the Disaster Plan is the backup tapes for each server. The ability to recover from certain disasters depends on the available backups. The tape backup procedure is more fully described in the applicable backup SOPs. Briefly, a tape backup happens every weekday, using a father/son rotation. The tapes are then stored in a fireproof safe at an off-site location.

b) All servers use some form of hardware RAID system to help prevent data loss. Under this system, the server distributes data over multiple hard drives and can continue to operate (at slightly reduced efficiency) after the failure of 1 hard drive. (The simultaneous failure of 2 or more hard drives will render the server inoperable).

c) All servers feature redundant power supplies. That is, the unit that interfaces the server to the mains voltage input is replaceable. Each server has two such units, which can be replaced while the server is still operational. Only one functioning power supply unit is required to keep the server operational.

d) The servers and network switches are supported by an *uninterruptable power supply* (UPS). In the event of a mains power failure, the UPS will automatically supply power from a temporary backup battery. The exact running duration varies depending on load.

e) The servers are covered by a support contract with Dell UK providing next business day engineer call-out and parts replacement. The network equipment is covered by a support contract with Cisco Systems, providing 4 hour part replacement. There is an emergency power generator callout contract.

f) There is a 24/7 IT emergency contact number for [company HQ] in [USA]. During normal office hours ([USA] time), contact the main switchboard at [number] and ask to speak to the help desk. Outside office hours, call [number]. (This number is for genuine IT emergencies only. It is *not* for routine technical support.)

6.0 Procedure

The number of problems that can occur with a network, associated hardware and layered products is very high, and within each problem there can be different levels. The degree of “disaster” varies from insignificant (one network socket stops working) to critical (the entire building is physically destroyed).

This document describes the most likely “disasters” and the suggested resolution. The disasters and resolutions are necessarily general. In some cases, elements of a large disaster are covered as separate disasters themselves. For example, the loss of the building would include the loss of all servers. The loss of each server is covered as a separate disaster with its own list of impacts.

In most cases, the best resolution is to remove the underlying problem. For example, if a server stops working, the best solution is to fix the server. The resolutions listed here apply only when fixing the underlying cause is not possible or will take too long.

Note: With the “disasters” that affect access to the building, this disaster recovery plan forms part of the Business Contingency and only covers the computing aspects. It is assumed that the company will provide alternative buildings, hardware and software to continue the business.

6.1 An individual PC is not working

Resolution:

(a) Use another PC if possible. Have the broken PC repaired or replaced as appropriate.

6.2 A stand-alone PC for instrument control is not working

Resolution:

(a) Find a spare PC and load the necessary instrument control software onto it from the installation media. For validated applications, requalification would be required.

6.3 A computer virus infects the UK computer network

Impact:

(a) This varies greatly depending on the virus in question. It may potentially include loss of service, breach of security and/or destruction of data. The resolution below applies only to "serious" infections.

Resolution:

(a) All computers identified as affected should immediately be isolated from the network (including servers, if they are infected).

(b) Machines should not be reconnected until they have been disinfected and had their anti-virus software suitably updated.

(c) If the virus propagates by use of a software flaw for which a patch is available, the patch should also be installed.

(d) In the event of a serious infection, the other company sites should be notified.

(e) Depending on the seriousness of the problem, it may be appropriate to disconnect the UK LAN from the Internet (to prevent further infection entering from the Internet and/or to prevent the virus spreading to other company sites).

6.4 A single hard drive fails on one of the servers

Impact:

(a) This will not usually prevent the server in question from functioning. However:

  (i) Performance will be reduced.

  (ii) Should a second hard drive fail, this will disable the server, potentially causing loss of data.

For these reasons, the problem needs to be corrected in a timely manner.

Resolution:

(a) As soon as possible, the failed drive replaced. (This does not require the server to be shut down.) The RAID system can then regenerate the contents of the failed drive. Performance will be reduced but the server will still be usable while the regeneration is in progress.

(b) Note that the server will not be able to tolerate the loss of another hard drive until after the regeneration process has successfully completed.

(c) If the fault cannot be repaired quickly, it would be advisable to perform a tape backup.

6.5 Multiple hard drives fail on a single server

Impact:

(a) This will disable the server until corrected. (Impacts and resolution are listed separately for each server.)

(b) All data since the last backup are likely to have been lost.

Resolution:

(a) The failed drives should be replaced as soon as possible, and data restored from backup. If this will take too long, see the additional resolutions for each server as listed in the appropriate section.

6.6 A single power supply fails on a server

Impact:

(a) Minimal immediate impact. However, if the other power supply fails as well, this will disable the server. Thus, the failure needs to be corrected in a timely manner.

Resolution:

(a) Arrange for the immediate replacement of the failed power supply unit. (The server does not need to be shut down to perform the replacement.)

6.7 Both power supplies fail on a server

Impact:

(a) The server will be unavailable. Impacts and additional resolution are listed separately for each server.

Resolution:

(a) Arrange for the replacement of both power supplies as soon as possible.

(b) Once this is done, the server may or may not operate normally. If necessary, restore from the most recent backup tapes to bring the server back to normal operation.

6.8 The Server [name] is unavailable

Impact:

(a) Automatic network configuration of PCs by DHCP will not occur.

(b) DNS services will be unavailable.

Resolution:

(a) DHCP and DNS services can be provided from another server temporarily.

6.9 The Server [name] is unavailable

Impact:

(c) Most network drives will be unavailable.

(d) Printers will be unavailable.

(e) [Project management software] will be unable to perform most operations on UK projects.

Resolution:

(b) Data can be restored from backup to another server. User login scripts would need to be reconfigured for the new location.

(c) Another server can be set up to provide print services. Individual user profiles would need to be reconfigured for the new location.

6.10 The Internet is unavailable

Impact:

(a) All email services will be unavailable. (Email will continue to be delivered, but UK staff will be unable to access it from the UK LAN. Users with local email caching enabled can still read their existing email and compose and send new messages, but these will not be delivered until the problem is rectified.)

(b) The [document management software] will be unavailable.

(c) The [project management software] will be unavailable.

(d) The [data management software] will be unavailable.

(e) The [accounting software] will be unavailable.

(f) Automatic antivirus updates will no longer occur.

Resolution:

(a) It is impossible to access email without some kind of Internet connection. Another company site can be instructed to check the UK mailboxes for high-priority emails if necessary.

(b) Important documents can be retrieved from [document management software] on a machine with Internet access and the VPN client software and copied onto a temporary folder on the network fileserver.

(c) Unless some kind of temporary Internet access can be brought into the company buildings, there is no way to access [project management software], [data management software] or [accounting software]. Urgent instructions will have to be sent to other company sites by telephone if necessary.

(d) Antivirus updates can be manually downloaded on a machine with Internet access, and manually installed on each PC.

6.11 The building loses mains power

Impact:

(a) The network switch and servers will continue to operate normally until the UPS battery runs out. After this, all servers will be unavailable. The impacts of server unavailability are covered separately for each server.

(b) All PCs will cease to function; any data stored on them will be unavailable. (Laptops will continue to function until they run out of battery power.)

(c) Access to the Internet will not be possible once the UPS battery runs out.

Resolution:

(a) If possible, it is preferable that the servers be cleanly shut down before the UPS battery runs out.

(b) If time allows, a differential backup should be attempted before the UPS battery runs out. There will not be time for a full backup.

(c) No further resolution is possible without a power source.

(d) [Company name] has an emergency generator callout contract. This is described in the local Freezer Disaster Recovery SOP.

6.12 The building is physically inaccessible; computer equipment still functioning

Impact:

(a) Minimal immediate impact if the servers are still functioning. However, if the building is at risk of damage, it would be advisable to attempt to recover data over the VPN.

(b) It will not be possible to change the tapes in the drives to continue normal backup operations.

Resolution:

(a) As much data as possible should be recovered from the building over the VPN. If necessary, replacement hardware can be obtained to store this.

6.13 The building is destroyed

Impact:

(a) All servers will be unavailable. The impacts of server unavailability are covered separately for each server.

(b) Any data stored on the servers since the last backup have now been lost. This should not exceed 24 hours during the week.

(c) Any data stored on individual PCs have now been lost.

Resolution:

(a) New servers will have to be obtained. Data can be restored from the most recent backup tapes. Significant reconfiguration may be required.

6.14 The off-site backup tapes are destroyed/lost

Resolution:

(a) If necessary, a new off-site storage location should be found.

(b) A new set of backup tapes should be created. Perform an immediate full backup, move this to off-site storage, and then continue the normal backup cycle.

7.0 [Revision History]

Note:

This document has been redacted. Sensitive information has been replaced with [red text in square brackets].

"SOP" stands for "Standard Operating Procedure", a kind of formal document.