# 1. Approval and Authorisation

Completion of the following signature blocks signifies the review and approval of this Process (signed copy held in safe)

| Name | Job Title | Signature | Date |
|---|---|---|---|
| Authored by:- <Name> | Network/Systems Supervisor | | |
| Approved by:- <Name> | Information Security Officer | | |
| Authorised by:- <Name> | Director of Finance & IT | | |

# 2. Change History

| Version | Date | Reason |
|---|---|---|
| Draft 1.0 | | |
| Version 1.0 | | |
| Version 1.1 | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# 3. Contents

# 4. Definitions in this report

| | |
|---|---|
| Trust | XXX NHS Trust |
| BILLY | Name of the Trust network |
| MS NT | Microsoft Windows NT operating system |
| Filename.EVT | Generic file name for Event Logs files |
| McAffee | Antivirus software on BILLY |
| Cyber Patrol | Internet filtering software on BILLY |
| ACE | Remote authentication program |
| MAX 2000 | Remote dial-in program |
| LAN | Local Area Network |
| WAN | Wider Area network |
| 512 KB | 512 Kilobytes |
| 2 GB | 2 Gigabytes |
| ERR | Error |

# 5. Document referred

| | |
|---|---|
| Helpdesk Procedures | ISMS/HLP/001 |
| Network Server Checklist | Report NSC No.1 |
| Server Performance Monitor | Chart SPM No.1 |
| System Performance Monitor | CHART SPM No.1 |
| Network Servers Checklist | Report NSC No.1 |
| Event Viewer system Logs | Report EVL No.1 |
| Terminal Server user logs | Report TS2 No.1 |
| ACE Server Activity report | Report ASA No.1 |
| User Monitor Access Control | Report UMAC No.1 |
| Proxy Web Server | Report PWS No.1 |
| Weekly Helpdesk Summary | Report WHS No.1 |
| | |
| Details of Reading Servers | Appendix 1 |

# 6. Event logging

Access to the Trust's network services is via a secure log-on process, designed to minimise the opportunity for unauthorised access.

Audit policies for the Trust's network system are set to log users and group management events. These logs are generated as Event Logs. Certain Event Logs may be archived as part of the record retention.

IT Operations uses built in tools on the MS NT system to process the Event Logs. The system itself and applications on the system can generate records of significant events. Event log data is reported to the Event Log Service by part of the system or by application running on the system. The Event Log Service stores the data in a Filename.EVT

Event Logs for performing the checks will be identified and made available to the Administrator.

Administrators log in with a secure password, which is only available to the system users of the IT Operations, who can only access event Logs.

The IT Operations manager will monitor activities on the Trust network servers, audits following events:

- event system log
- event application log
- event security log

Access to event log tools is controlled to prevent any possible misuse or compromise.

Event logs are overwritten as needed. The IT Operations manager decides on the period to which logs can be overwritten.

# 7. Event Analysis

The following interactions are recorded in the Event Logs:

- DATE and TIME
- TYPE – the severity of event
- SOURCE – the component that logged the event
- EVENT ID – a unique number identifying the event that occur
- USER – the name of the user to which the event relates
- COMPUTER – the machine on which the event was logged
- DESCRIPTION – error messages associated with the event

Two of the above fields are important to note for the security of the systems:

1. the event ID and
2. the description

Description field contains unique information about security events. Event IDs are used to identify User/Group Account Changed.

# 8. Event Log Management

The event logs tends to fill up quickly. It is at the discretion of the Network Systems manager to decide which event categories to log.

In general based on the specific information required by the Director of Finance & IT, logging mechanisms will be configured to log minimum number of events to capture that information.

The Trust network system uses MS NT for its core network server's operating system. MS NT includes a utility called Event Viewer that allows the event logs to be viewed. The Network Systems manager controls whether or not to overwrite old events. ***Report EVL and Report TS2*** show two examples of the event viewer on xxxx-2 mail server and xxx-02 terminal server.

Gathering event log data in mass quantities is not useful and far exceed the ability of an administrator to mange it. The following aspects are for the access control of the Trust network when event logs are produced:

- Minimum log file size. IT Operations use a default 512 KB file size
- Overwrite behaviour when log is full. IT Operations use the option:-overwrite events as needed
- Restrict guest access. IT Operations allow only authorised users access to the event log.

Certain Event Logs may be archived as part of the record retention when required.

# 10. Monitoring system use

Access to the Trust's LAN and WAN are constantly monitored. Initial access to the system and level of access will be authorised by line management on a "need to use" basis. The IT Operations manager will review the systems logs to detect unauthorised or unusual access.

Use of BILLY services are monitored on line for the following:

- Password violations
- Un-authorised data access
- Un-authorised software access
- Misuse of the Trust's Intranet and Internet
- Virus prevention and detection

# 11. Network servers checklist - daily

The following details are checked daily on each BILLY servers for systems availability and security:

- Detecting new viruses
- Data backup failure
- Servers' disk space
- Error messages on the servers' console
- Software and hardware malfunction

Any error or failure on the above list will be reported to the IT Operations manager and the Network Systems manager by email and by the phone whichever the quickest. ***Report NSC and Appendix 1*** show an example of a daily report on the BILLY network servers.

# 12. System performance monitoring - on line

The Trust network servers and the use of its facilities are continuously monitored on line. Success and failure events of the BILLY servers will be recorded on a chart when requested by the IT Operations manager - ***CHART SPM***.

On line monitoring of the servers are for the following purposes:

1. Uptime and reboots:-
   - when service starts
   - when server shuts down correctly
   - when serve shuts down unexpectedly

2. Server crashes:– when a fatal "stop error" occurs

3. Hardware failure:–
   - when event is "warning" – event is a minor failure
   - when event is "error" – event is a severe failure

# 13. Monitoring users and groups - monthly

In order to reduce the impact on the BILLY system's performance, IT Operations decided on the minimum number and type of objects that must audit. Minimum number of accesses is monitored for each type of object each month.

## 13.1 Files and Directories objects

Files and Directories are the most common objects that are monitored by the IT Operations. User Manager in the NT operating systems is used for this purpose.

Following accesses are monitored:

- object's owner
- object's group
- access control list (users and groups)

User manager access control will be generated monthly and reported to the Director of Finance & IT at his request. ***Report UMAC***

## 13.2 Monitoring Audit policy

One of the main policies when monitoring the system in BILLY is the Audit policy. The Audit policy is within the User Manager when objects are established in the NT system.

It is important to monitor the Audit policy in order to prevent a rogue administrator from turning auditing off, performing an inappropriate action, and turning auditing back on.

IT Operations has enabled the following events to Audit:

- Logon and Logoff
- Use of User Rights
- User and Group Management

IT Operations manager only grants administrator access to nominated IT system users.

# 14. Monitoring use of Internet and Intranet

Use of the Internet via the Trust's network and use of the Trust's Intranet are continually monitored to prevent any external threat and misuse of the Trust's system.

## 14.1 Proxy web server

Accessing the Internet websites through the Trust network are filtered by use of a Cyber Patrol for Microsoft Proxy server.

Following categories are defined for filter setting

- Work time
- Leisure time
- Filtered internet access
- Restricted categories – filtered for work or leisure

The Information Security manager is responsible for controlling the access to users and groups.

Event logs on the use of the intranet are produced on line by the system and a report is generated every month to be presented to the Director of Finance & IT. ***Report PWS.***

## 14.2 Intranet server monitoring

Use of the Trust Intranet web pages is controlled through BILLY secure network. Failure to use the Intranet successfully is reported to the Helpdesk.

# 15. Monitoring system use externally

## 15.1 Dial-in system –full access

Access to the BILLY network services is available to users externally. Authorised users access the Trust network services by dial-in to a secure authenticated server.

The ACE program that performs the authentication dialog on the third party clients controls access to the authenticated server.

The IT Administrator who logs in with a secure password monitors the ACE server. A report is generated to assess the use of the system and to identify possible intrusion by unauthorised users. ***Report ASA***

IT Administrator is responsible to assess the following parameters in the report:

- Access Date/time
- Log-in name
- User/Group name
- Server name
- Secure ID number
- Description

## 15.2 Dial-in system - Email access

Authorised users can access their Trust's email remotely by dial-in to a secure authenticated server. The xxx 2000 program that performs the authentication on the dial-in users controls access to the authenticated server. xxx 2000 access control provides following attributes for the remote dial-in users:

- Authentication
- Authorisation
- Accounting

IT administrators can monitor the success and failure of the users access to the server on line. The Administrator logs in to the server with a secure password to monitor the activities.

# 16. Monitoring fault logs - weekly

All IT related faults including Information Security Incidents are reported to the helpdesk. Faults that are logged with the Helpdesk by different methods must be recorded on the Helpdesk software.

Method of reporting is fully covered in the IT Helpdesk Procedures. Severity of the reports are categorised as:

- Critical
- Urgent
- Normal

Reports are uniquely numbered and assigned to the technical support team to resolve them. The helpdesk administrator monitors reports continuously. Weekly summary of the reports is generated by the Helpdesk software and presented to the Director of Finance & IT. ***Report HDS***

# Chart SPM – Servers Performance Monitor

Shows an example of the servers' performance on line. Chart displays the users activities on the 8 different BILLY servers as well as number of users accessing servers at any one time.

**Chart No.1** - server performance monitor **Date/time created**

# Report EVL – Event Viewer system log

Sample Event Logs IT Administrators accessing the system on the Trust's mail server xxxx-2. Event logs are not held in media libraries or user areas and they must be stored in a secure area separate from development and operational systems for audit purposes when required.

**Report No.1** Event Log on xxxx-2 **date/time created**

# Report TS2 – Terminal Server users logs

Sample Event Logs users log-on and log off to the network on the Trust's Terminal Server xxx-02. Event logs are not held in media libraries or user areas and they must be stored in a secure area separate from development and operational systems for audit purposes when required.

**Report No.1** Event Log on xxx-02 **date/time created**

# Report NSC- Network Servers checklist

**Application:**

1. This is a quick systems checklist to apply on the servers early morning or late evening.
2. This checklist should not be a substitute to full systems check/monitoring procedures.
3. This checklist should be used to complement the on-line monitoring of the Terminal Servers displayed continuously in the IT Ops. Office.
4. Use IT operations network servers checklist in this document –section 2 and 3- to perform this task/report.

**Method:**

During the systems check/monitoring, if error occurs type “ERR” in the checklist table, then write details in the comments column in the error table. Report error if:

- Servers availability
- disk space <2GB
- new virus found while downloading McAffee
- backup failed (tape drive or software)
- error messages appear while logging to servers
- error when h/w & s/w malfunction

.

Example:

**Report No. NSC01** Error checklist table **date:** 25/09/01

| Switch No. | Server | ERR Comments |
|---|---|---|
| 2 | | Disk space =2 GB |
| 2 | | Antivirus s/w download unsuccessful |
| 1 | | Cyber patrol software has failed |
| 2 | | Referenced memory 0x01e19266 could not be read. |

If errors; report to the IT Operations manager and the Network Systems manager then save this document as a log file.

You don’t have to report if there is no error but report must be produced each week for recording and audit purpose.

# Report NSC continued

## Complimentary report Reading servers

**Report No. NSC01** Primary checklist table **date:** 25/09/01

| Server name | Services | Checked Yes / No | | If Error type ERR | Routine checks |
|---|---|---|---|---|---|
| **Switch No.1** | | | | | |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Back up |
| | | | | | Disk space & Back up |
| | | | | | Disk space & Back up |
| | | | | | |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | |
| | | | | | Intrusions check |
| | | | | | Intrusions check |
| | | | | | Disk space, Back up, Inuculan download |
| | | | | | Disk space, Back up, Inuculan download |
| | | | | | |
| | | | | | Services/spooler & test print |
| | | | | | Message monitor |
| | | | | | Message delivery |
| | | | | | Availability& operational |
| | | | | | Disk space & Back up |
| | | | | | Disk space & Back up |
| | | | | | Disk space & Back up |
| | | | | | |
| | | | | | |
| | | | | | Availability& operational |
| | | | | | Availability& operational |
| | | | | | Services/spooler & test print |
| | | | | | Availability& operational |
| | | | | | Availability& operational |

# Report NSC continued

## Complimentary report Other Servers

**Report No. NSC01** Primary checklist table **date:** 25/09/01

| Server name | Services | Location | Yes | No | If Error type ERR | Routine checks |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# IT Operations Network Servers Checklist

**A- Primary checklist - daily**

| Action | Process |
|---|---|
| **Servers availability** | Use the 2 multi-switches in the comms. room to check all servers. Make sure servers on BILLY, TJE and BILLY3 domains are operational.<br><br>If you are in a remote site:<br>Use PING to verify response to the servers IP address or<br>use ControlIT to perform the task.<br><br>**Other servers and comms. devices can be checked independently. Thy are:** |
| **Anti-virus monitor check** | check that the Real-Time Monitor is running by clicking on the Green icon in the bottom left hand corner. If this just makes the icon disappear or if the icon is not there do the following:<br>Click on Start/Programs/InoculateIT for Windows NT/InoculateIT Realtime Monitor |
| **Updating Antivirus software** | 1.Ensure that you have internet access.<br>2. Goto OXO-2<br>3. Click on Start/Programs/InoculateIT for Windows NT/AutoDownload manager<br>4.Click on the traffic light style icon<br>5. After 4 hours check on the Anti-virus realtime monitor |
| **E-mail checks** | 1. Daily checks using the monitor pages at: http//<br>2. (note that this password will have to be manually changed when you do the BILLY administrators password)<br>3. Here you can see the incoming and outgoing messages and they can be refreshed as necessary |
| **Undeliverable messages** | there should be no messages that block on OXO-3 as they are reported to Mail Admin.<br><br>1. However if there is then go to OXO-3.<br>2. In Explorer goto c:\Program Files\Mail Essentials\outgoing or incoming; in there you can see by directory the messages and can delete the offending item.(Pick that up by viewing the Mail Essentials monitor on OXO-3 itself). |
| **Tape backup success check** | Go to machine console and click on : Start/Programs/ArcserveIT for Windows NT/ArcserveIT Manager/Job Status<br><br>Make sure backup is successfully completed. on the following server:<br><br>Data-1, Data-2, Data-3, OXO-2, OXO-12, TJE-4, Energy-1, Web-2, TJE-4, |

| | |
|---|---|
| **Tape Change** | There are 9 tapes on BILLY servers which must be changed daily:<br>Data , mail, energy, TJE and web servers<br>Full procedure in detail is on Information Backup procedures |
| **Drive space checking** | Goto each machine in turn and using Explorer check to freespace on each drive c: and d: drives.<br>If disk space less than 2 GB on Data servers and Mail servers report it |
| **Ziggy Print Server** | Two print services available in BILLY. Following routines to follow if they fail to operate:<br>1. Click on Start/Settings/Control Panel/Services<br>2. Stop the Remote Procedure Call RPC (Locator)<br>3. Stop the Spooler<br>4. Start the Spooler<br>5. Start the Remote Procedure Call RPC (Locator)<br>6. Close Services<br>7. Close Control Panel |
| **Dial In Monitoring,** *Check every Mondays* **Dial In problems** | This facility is provided via the Max box and NHS_MAN_2.<br>To monitor the dial-in point: TELNET xxx.xxx.xxx.xx and use the password: Ascend. It'll appear in the sessions box how many users are actually dialed in and what Ids' they are using.<br><br>As well as above.<br>check out using ControlIT or at the console NHS_MAN_2. There are differing routes depending upon whether the complaining user is Secure dialIn or not.<br><br>When reported, Tech support must dial-in from office to identify the problem:<br>1. if external, check& fix config. on local m/c<br>2. if internal check & fix comms. And server config.<br><br>To check the users configuration click on:<br>1. The icon labeled Ascend<br>2. Access Control Manager<br>3. Edit Users<br>4. Find the user in question and check config |
| **SecureId dial in users** | As above<br>To check the users configuration click on:<br><br>1. Click on the icon labeled ACE<br>2. Database Administration<br>3. User menu<br>4. Edit User<br>5. find the user and check config |
| **Checking Comms Routes** | WAN Communications to xxxxxxx, xxxxxxxxx, xxxxxxxxx and the NHSnet could fail externally, if so:<br>Find BT SIN number and call BT when comms. fail.<br>*Fault calls to BT must be logged in BT files as well the Helpdesk* |

# IT Operations Network Servers Checklist continued

### B- Secondary checklist - ad-hoc or weekly

| | | |
|---|---|---|
| **Mail Content Checking** | Internet Mail is sent via OXO-3 for both The Trust and Logistics staff; whilst incoming mail for the Trust comes via the Notes server OXO-7. The messages (both incoming and outgoing) that go via OXO-3 can be content checked for sexually explicit language in the subject line and body of the message. Whilst this list currently employed is not exhaustive it may need to be expanded. To expand this goto ControlIT or the OXO-3 console and:<br>1. Click on Start/Programs/GFI Mail Essentials/Mail Essentials Configuration<br>2. Click on the Content Ch. Tab<br>3. In the bottom right hand corner of the dialogue box ensure that <default profile> is selected and click on the settings button.<br>4. Add the criteria in each of the following areas; “Block mails with word or phrase in body”; or “Block mails with word or phrase in subject”<br>5. To exit click Close/Apply/OK<br>This method does not apply to EU and Human Right regulations (too complicated to apply, does not apply only to sexually explicit language) | **Ad-hoc** |
| **Illegal Software**<br><br>Only on IBA and data servers | System Administrators MUST do a regular trawl for inappropriate/illegal software. This must be done on each of the Data servers and must include both shared and user directories. There should be no need for any runnable software in these directories and as such should be tracked and stopped.<br>This can be done by:<br><br>1. Open Explorer on the relevant machine<br>2. Highlight the route of the D: drive<br>3. Select the Tools menu<br>4. Choose Find from the menu<br>5. In the Find dialogue box ensure the checkbox “include subfolders” is checked<br>6. In the Named field type in : *.exe;*.bat;*.com<br>7. click on the Find Now button<br>8. You will then after processing find a list of all software that accords with this search criteria.<br>9. Right click on each item in the list and check out Ownership etc to hang the user responsible<br>10. a copy of the list to the guilty persons might be sent to line-manager and HR.<br><br>Must be discussed with user first | Only when servers performance change sharply |

| | | |
|---|---|---|
| **Mail Attachment Blocking/ Filtering** | Internet Mail is sent via OXO-3 for The Trust; whilst incoming mail for the Trust comes via the Notes server OXO-7. The messages (both incoming and outgoing) that go via OXO-3 can be checked for potentially damaging mail attachments. Currently we are trapping attachments of type: exe; vbs; com; bat. To expand this goto ControlIT or the OXO-3 console and:<br><br>1. Click on Start/Programs/GFI Mail Essentials/Mail Essentials Configuration<br>2. Click on the Content Ch. Tab<br>3. In the bottom right hand corner of the dialogue box ensure that <default profile> is selected and click on the settings button.<br>4. Click on the Attachment Options button<br>5. Click on the Add button to increase the number of attachments that are to be blocked.<br>6. To exit click Close/Apply/OK<br><br>Also check other file formats noted by Anti-virus software vendors (does not only apply to exe, vbs, com, bat) | Should do any time new viruses noted |
| **Assigning user to new Proxy server** | 1. Add them to the group A-PROXY-ACCESS<br>2. Amend users Internet Explorer settings by choosing from the Tools menu Internet Options<br>3. Choose the Connections Tab<br>4. Select the LAN Settings button<br>5. In the proxy server area in the address field type in “TJE-7” and the port = “80”<br>6. Click on the Advanced button<br>7. Make sure the box is checked for: “Use the same proxy server for all protocols | **Ad-hoc** |
| **Adding people to the Helpdesk as techy types** | 1. Goto TJE-4<br>2. Goto The HelpDesk database<br>3. Edit the table: D2n Passwords by adding the details of the person required<br>4. Goto User Manager for Domain<br>5. Add the details of the users BILLY account to the Helpdesk group<br>6. Synchronize the Servers of the domain | **Ad-hoc** |
| **Battery re-conditioning** | All Dell PowerEdge 4300 machines need to have the battery for the RAID controller reconditioned every 6 months. This process takes 8 to 14 hours and therefore must be done out of hours. There is an added complication in that all heavy hard disk throughput must be finished before this can be done i.e. OXO-2 mail delivery etc must be minimal normally after 22:30 at night. To do this:<br>1. goto each machine in turn and click on Start\Programs\Dell Perc 2\FAST\Open\View\Controller View<br>2. Right Click on the PERC 2<br>3. Choose Properties<br>4. Click on the button labeled “Recondition” | **Could be done at weekends** |
| **TJE-4(SQL** | This machine uses Microsoft SQL Server 7. It provides the back- | **Ad-hoc** |

| | | |
|---|---|---|
| **Server)** | end database to several items for both Purchasing and IT. All connectivity should be using ODBC/DAO to gain access to the info in the databases details of which are embedded in the global.asa files on the Web Server(Web-2). All data is extracted using SQL Server Stored Procedures so minimal network traffic is passed. There shouldn't be need for any database work unless any other projects are created apart form that detailed above in setting up users. | |

# Example – Report Weekly Helpdesk Summary

Report shows the summary of all calls made to the Helpdesk in different categories during one week.

**Report No. 1** Weekly Helpdesk Summary **date/time created:**

| Report Category | Monday | Tuesday | Wednesday | Thursday | Friday | Unfixed | Unclaimed |
|---|---|---|---|---|---|---|---|
| Add/Delete/Amend Users | | | | | | | |
| BT Fault | | | | | | | |
| BT Faults | | | | | | | |
| BT Faults | | | | | | | |
| BT request | | | | | | | |
| change to BILLY setup | | | | | | | |
| E-mail | | | | | | | |
| Hardware | | | | | | | |
| ISDN - No Connection | | | | | | | |
| ISDN Line Closed | | | | | | | |
| National Database | | | | | | | |
| Other | | | | | | | |
| Password change/problems | | | | | | | |
| Printing Problem | | | | | | | |
| Problem re:software use | | | | | | | |
| Request for new hardware | | | | | | | |
| Request for new service | | | | | | | |
| Software error | | | | | | | |
| Software query | | | | | | | |
| Unable to Access Billy | | | | | | | |
| User file problems | | | | | | | |
| User fixed | | | | | | | |
| Virus | | | | | | | |
| Web page request | | | | | | | |

# Report ASA – ACE Server Activity report

Report shows the users activity to access the ACE server externally using a secure dial-in method. Report is generated to monitor unauthorised user access (intrusion –if any)

**Report No.1** ACE Server Activity report **Date/time created**: 03

| **Date** | **Time** | **Current User/Client (Group)** | **Affected Token ID** |
|---|---|---|---|
| | **Description** | **(Site) Server** | |
| | **Affected User Name** | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Report PWS – Proxy Web Server

Shows a sample of the report generated to monitor access to the Internet using BILLY servers.

**Report No.1** proxy web server **date/time created**

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Report UMAC - User Manager Access Control

Shows a sample of a user manager access control for BILLY. Report generated to monitor files and directories objects' owner.
Note this sheet also contains the location of the profile and user directories as used by the system.

**Report No.1** user manager access control **date/time created**

| Login Name | Full Name | Description | User Directory | Profile Directory |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Appendix 1 – Details of Site 1 servers

| Switch No.1 | | Switch No.2 | |
|---|---|---|---|
| **Server name** | **Services** | **Server name** | **Services** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Other Servers**

| Server name | Services | Location |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |