NHS
East London
NHS Foundation Trust

Server Backup Policy

Version number :	1.2
Consultation Groups	Information Governance Steering Group, Digital Board and Key Leads
Approved by (Sponsor Group)	Information Governance Steering Group, Digital Board and Key Leads
Ratified by:	Quality Committee
Date ratified:	13th November 2019
Name of originator/author:	Usman Malik
Executive Director lead :	Paul Calaminus
Implementation Date :	November 2019
Last Review Date	September 2019
Next Review date:	September 2022

Services	Applicable
Trustwide	x
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
1.0	07/01/2013	Daniel Woodruffe	Final	Revisions
1.1	22/03/2016	Asim Mir	Final	Revisions
1.2	23/09/2019	Usman Malik	Final	Revisions

Contents

1. Introduction

The purpose of this backup policy is as follows:

- To safeguard the information assets of the Trust.
- To prevent the loss of data in the case of accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes should such events occur.
- To manage and secure backup & restoration processes and the media employed within these processes.

2. Process

Responsibility for maintaining a full set of up to date backups resides with the IT Server Manager. Any issues with maintenance of a complete set of backups will be escalated to the Assistant Director of IT. The IT department provides policy-based, system level, network-based backups of all centrally hosted systems. Backup policies are implemented on a per system basis that define:

- **Selections:** what information is to be backed up on systems.
- **Priority:** relative importance of information for purposes of the ordering of backup jobs.
- **Type:** the frequency and amount of information to be backed up within a set of backup jobs.
- **Schedule:** the schedule to be used for backup jobs.
- **Duration:** the maximum execution time a backup job may take prior to its adversely affecting other processes.
- **Retention Period:** the time period for which backup images created during backup jobs are to be retained.

3. Definition of Retention Period

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed on centrally hosted systems during the time period defined by system backup policies.
Backup retention periods are in contrast to retention periods for information defined by legal or business requirements.

System backups are not meant for the following purposes:

• To archive data for future reference
• To maintain a versioned history of data

4. Default Schedule of Backups

Unless a system supporting an application or business function requires a custom schedule, systems will be backed up using a default schedule of monthly full backups and subsequent differential incremental backups prior to the next full backup.

During backups, point-in-time images of information stored in active, permanent storage (e.g. hard disks) will be copied to magnetic tape or other media.

Full backups will back up all files specified within a system's backup policy, regardless of when they were last modified or backed up. Differential/incremental backups will back up all files that have changed since the last successful incremental or full backup.
The media containing a system's monthly full backup and full set of subsequent differential- increment backups will comprise its full backup media set.

Through use of full backups and subsequent differential-incremental backups, backup windows (time period required to perform backups of one or more systems) will be minimized as will be the number of media required to store the backups. This will assist in ensuring good system performance for business processes. Restores will require a longer period of time as the last full backup and all differential-incremental backups that have occurred since the last full backup are required. However, due to the frequency of backups, at most one set of tapes would be required in the event of a complete system failure. Thus, this policy works to minimize the time required to backup systems (the common case) while limiting the potential time required to perform a full system restore in the event of a system failure.

The IT department will schedule backup windows for systems so as to minimize disruption to business functions and ensure accomplishment of the monthly full, weekly – daily – differential - incremental policies described above.

5. Storage Locations and Retention

5.1 Period of Backups

Unless a system supporting an application or business function requires a custom retention period, IT will maintain 4 weeks of full and incremental backups.

After a successful full backup, a copy of the full backup's images will be made and stored in a secure, off-site media vaulting location permanently for disaster recovery purposes.

This will ensure that no more than one month of information would be lost in the event of a disaster in which centrally hosted systems and backup images (stored in two Trust locations) are destroyed.

5.2 Backup Verification
The IT Server Manager will ensure that on a daily basis, logged information generated from each backup job will be reviewed for the following purposes:

- To check for and correct errors
- To monitor duration of the backup job
- To optimize backup performance where possible

The IT Server Manager will identify problems and take corrective actions to reduce any risks associated with failed backups. Test restores from backup tapes for each system will be performed at least every two months. Problems will be identified and corrected. This will work to ensure that both the tapes and the backup procedures work properly.

IT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes. This forms part of the Housekeeping & Maintenance Policy.

5.3 Systems Management

IT will ensure on an on-going basis that all elements of its backup system are documented and maintained in such a manner as to ensure:

- The integrity and confidentiality of data copied during backup and restore operations
- Appropriate access to data maintained within the backup system
- Recoverability in the face of system failure or disaster
- Optimal performance
- Stability

This documentation will be reviewed every two years and revised in the event of any changes to procedures or software.

Elements of the backup system requiring on-going systems management include, but are not limited to:

- Client software
- Hardware drivers
- Server software
- Network connectivity & communications
- Storage devices (e.g. tape library)

5.4 Media Management

Media will be clearly labeled and logs will be maintained identifying the location and content of backup media.

Backup images on assigned media will be tracked throughout the retention period defined for each image. When all images on the backup media have expired, the media will be re-incorporated amongst unassigned (available) media until reused. Periodically and according to the recommended lifetime defined for the backup media utilized, IT will retire & dispose of media so as to avoid media failures. This information can be found out from the backup management console. Additionally, a label of first use will also be utilised.

5.5 Storage, Access, and Security

All backup media must be stored in a secure area that is accessible only to designated IT staff or employees of the contracted secure off-site media vaulting vendor.
Backup media will be stored in a physically secured location when not in use.
During transport or changes of media, media will not be left unattended.

5.6 Retirement and Disposal of Media

Prior to retirement and disposal, the IT Server Manager will ensure the following:

- The media no longer contains active backup images or that any active backup images have been copied to other media
- The media's current or former contents cannot be read or recovered by an unauthorized party

With all backup media, the IT Server Manager will ensure the physical destruction of the media prior to disposal.

5.7 Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration of information will be made through a ticket logged with the help desk.
As the restoration of information has security consequences including:

• Possible escalation of privileges by parties authorized to access information
• Access by non-authorized parties. The IT and Telecoms Infrastructure Development Manager will carefully verify that the request for restoration of information is authorized by the owners of the information prior to performing the restoration.

The IT department will additionally ensure that the information restored is restored to a file system location with access controls appropriate to the information being restored.

5.8 Degradation of Service

Should a failure or defect of the backup system threaten the recoverability of a computing system or its information, the IT department will take immediate actions to correct the situation.
Additionally, IT will attempt to warn all users and owners of applications & information of the failure or defect and the potential scope of information loss.
IT will work with those warned to mitigate potential or actual risks until such time as full-service can be restored.

6. Disaster Recovery Considerations

As soon as is practical and safe post-disaster, the IT department will:

- Restore existing systems to working order or obtain comparable systems in support of defined business processes and application software.
- Restore the backup system according to documented configuration so as to restore server systems.
- Obtain all necessary backup media to restore server computing systems
- Restore server computing systems according to the priority of systems and processes as outlined for restoration and recovery by:
- The Trust's DR Plan
- The point-in-time direction of the Trust's board

7. Associated Documentation

Housekeeping and Maintenance Policy