East of England Ambulance Service NHS Trust

Electronic Data Backup Policy

Document Reference	POL048
Document Status	Approved
Version:	V7.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Head of IM&T	14 March 2012	IS&T Security & Resilience Manager
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
3.0	December 2015	Approved by Executive Leadership Board
4.0	March 2017	Approved by Executive Leadership Board
4.1	January 2019	Approved by Information Governance Group

Version	Date	Comments (i.e. viewed, or reviewed, amended approved by person or committee)
5.0	March 2019	Approved by Management Assurance Group

Document Reference	
Recommended at Date	Information Governance Group 12 September 2022
Approved at Date	Compliance and Risk Group 17 October 2022
Valid Until Date	October 2024
Equality Analysis	Completed
Linked procedural documents	Information Security Policy IM&T Operational Security Policy
Dissemination requirements	All IT operational staff. Information Asset owners
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups.

This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

Paragraph		Page
1	Introduction	6
2	Purpose	6
3	Duties	6
3.1	IM&T Operational Managers	6
3.2	Information Asset Owners	6
3.3	Consultation and Communication with Stakeholders	6
4	Definitions	6
5	Development	7
5.1	Prioritisation of Work	7
5.2	Identification of Stakeholders	7
5.3	Responsibility for Document's Development	7
6	Schedules and Retention Periods	8
6.1	Media Storage	8
6.2	Backup Operation	8
6.3	Testing	8
6.4	Restoration	8
6.5	Exceptions	9
6.6	Backup Failure Reporting	9
7	Equality Impact Assessment	9
8.1	Dissemination and Implementation	9
8.1	Dissemination	9
8.2	Implementation	9
9	Process for Monitoring Compliance and Effectiveness	10
10	Standards/Key Performance Indicators	10
11	Associated Documents	10

Appendix A	Monitoring Table	11
Appendix B	Equality Impact Assessment	12
Appendix C	Schedule and retention	16

1. Introduction

This policy defines the backup methods and routines for information owned or held by the Trust.

2. Purpose

To ensure the integrity and availability of information, and to allow data essential to the Trust to be restored or recovered as quickly as possible in the event of data loss or corruption on one or more of its computer systems.

3. Duties

3.1 IM&T Operational Managers

Are to ensure that robust, fit for purpose, technical solutions are in place for systems and information within their areas of responsibility to achieve the purpose of this policy.

3.2 Information Asset Owners

To specify the parameters required for backing up information they are responsible for.

3.3 Consultation and Communication with Stakeholders

The schedule and retention periods will be agreed with Information Asset Owners or individual(s) nominated by them. Once agreed the policy will be communicated to them and all operational IM&T staff.

4. Definitions

Backup
The saving of files onto mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive
The saving of old or unused files onto mass storage media for the purpose of releasing on-line storage capacity.

Restore
The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

Rubrik
The solution currently in use in EEAST.

NAS
Network Attached Storage

5. Development

5.1 Prioritisation of Work

This policy has been created to document the procedures in place to ensure the integrity of Trust data so that in the event of data loss it can be recovered in a timely fashion, and that data is useable.

5.2 Identification of Stakeholders

Stakeholders will primarily be Information Asset Owners, although all staff are stakeholders as the policy applies to data held by all staff.

5.3 Responsibility for Document's Development

The development of this document is the responsibility of the IM&T Security and Resilience Manager, in conjunction with other senior technical managers.

6. Schedules and Retention Periods

Data will be backed up, and retained, according to the table in Appendix B. There is no archiving of corporate data beyond these schedules.

6.1 Media Storage

Online storage will be on systems that reside in areas where they are protected from power failures or other electrical anomalies, as far as reasonable, by the use of uninterruptable power supplies; and shall be protected from the risks of environmental hazards and opportunities for unauthorised access.

Offline media will be stored in appropriate storage, i.e. an EN 1047-1 certified fire safe which is located as far as practicable from the servers being backed up.

Archive media will be stored in appropriate storage on a separate site.

6.2 Backup Operation

The IM&T Infrastructure team will operate and monitor all backups. A call will be scheduled on the Service Desk call logging system in line with the schedule as per Appendix B to carry out backup integrity checks.

6.3 Testing

The IM&T Infrastructure team will be responsible for testing the ability to restore data from backups on a monthly basis. A call will be scheduled on the Service Desk call logging system.

6.4 Restoration

Users that need files restored must submit a request to the Service Desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

6.5 Exceptions

Where it is deemed appropriate an alternate schedule/system may be used, in which case a local policy will be written and approved.

6.6 Backup Failure Reporting

In the event of a backup failure, as well as remedial action taking place as a priority, failures must be reported to the Service Deliver Manager for Infrastructure and Head of Live Services.

7 Equality Impact Assessment

This is attached in Appendix B

8 Dissemination and Implementation

8.1 Dissemination

This policy will be held in the document library and advertised in line with the Trust policy on dissemination of procedural documents.

It will be circulated within IM&T via the senior management team

8.2 Implementation

Technical implementation is currently in place in line with this policy, current legislation and best practice. IM&T staff will be expected to be experienced in these areas, any training needs will be identified via the PDR process and arranged.

9 Process for Monitoring Compliance and Effectiveness

A service call will be scheduled daily on the Service Desk call logging system to check the automated backups. Success/failure/comments will be noted on the call log, with any failures being escalated through the appropriate technical hierarchy, as well as senior management being informed.

See also Appendix C.

10 Standards/Key Performance Indicators

The scheduled calls on the Service Desk call logging system will be monitored to ensure compliance with section 9 of this policy.

11 Associated Documents

Information Security Policy

IM&T Operational Security Policy

Appendix A: Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Success / failure of scheduled automated backup jobs	Nominated staff on each locality. Note the individual may change on a daily basis dependent on staff levels, etc. Calls will be logged to a group and an individual will pick up that task.	Calls will be logged on the IT call management system to check the backup software in use.	Daily	Log files from the various installations of backup software in use.	Success will be logged on the call management system, exceptions will be reported to senior technical management and an incident raised to identify and resolve the reported issue.	The Service Delivery Manager for Infrastructure and Systems, and the Technical Architect, will undertake subsequent recommendations and action planning for any or all deficiencies and recommendations.	Any changes to be applied will go through the IT Change Control process, and all relevant parties will be informed at all stages, and all documentation will be update accordingly.

Appendix B: Equality Impact Assessment Executive Summary

EIA Cover Sheet		
Name of process/policy	Electronic Data Backup Policy	
Is the process new or existing? If existing, state policy reference number	POL048	
Person responsible for process/policy	IT Security & Resilience Manager	
Directorate and department/section	IM&T	
Name of assessment lead or EIA assessment team members	IT Security & Resilience Manager	
Has consultation taken place? Was consultation internal or external? (please state below):	No	
The assessment is being made on:	Guidelines	
	Written policy involving staff and patients	X
	Strategy	
	Changes in practice	
	Department changes	
	Project plan	
	Action plan	
	Other (please state) Training programme.	

Equality Analysis

What is the aim of the policy/procedure/practice/event?

This policy has been developed as a result of the need to achieve a balance between the legitimate business access needs of authorised staff, and the need to maintain an appropriate level of security; and is designed to ensure that only the specified staff have access to secure areas.

Who does the policy/procedure/practice/event impact on?

Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐
Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐

Who is responsible for monitoring the policy/procedure/practice/event?

IT Security & Resilience Manager

What information is currently available on the impact of this policy/procedure/practice/event?

None

Do you need more guidance before you can make an assessment about this policy/procedure/ practice/event?

No

Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? **No**

Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐
Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐

Please provide evidence:

Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics? **No**

Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐
Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐

Please provide evidence:

Action Plan/Plans - SMART

Specific

Measurable

Achievable

Relevant

Time Limited

Evaluation Monitoring Plan/how will this be monitored?

Who **IT Security & Resilience Manager**

How **Reports from IT operational staff**

By **Email \ Service Desk reporting system**

Reported to **Head of Live Services**

Appendix C Schedule and retention

Server Name	Server Type	Backup Type	Data Size to backup	Frequency	Retention Period(s)
EOE-NRPTSBE1	Windows Server	SQL Backup	500Gb	Daily	1 Month
EOE-NRSYSLOG01	Windows Server	D:\	50Gb	Twice a day	1 Month
EOE-NRDC01	Windows Server	Bare Metal Recovery	100Gb	Daily	1 Month
EOE-NRDC01	Windows Server	System State (includes AD)	100Gb	Daily	1 Month
EOE-NRDC02	Windows Server	Bare Metal Recovery	100Gb	Daily	1 Month
EOE-NRDC02	Windows Server	System State (includes AD)	100Gb	Daily	1 Month
EOE-NRDC03	Windows Server	Bare Metal Recovery	100Gb	Daily	1 Month
EOE-NRDC03	Windows Server	System State (includes AD)	100Gb	Daily	1 Month
EOE-NRECS01	Windows Server	SQL Backup	2000Gb	Daily	1 Month
EOE-DWPRD03	Windows Server	SQL Backup	100Gb	Daily	1 Month
EOE-NRPRD01	Windows Server	SQL Backup	1500Gb	Daily	1 Month
EOE-NRPTS01	Windows Server	E:\Logs	200Gb	Twice a day	1 Month
EOE-NRPTS02	Windows Server	D:\Data	200Gb	Twice a day	1 Month
EOE-NRPTS02	Windows Server	E:\Data	200Gb	Twice a day	1 Month
EOE-NRPTS02	Windows Server	E:\SQL Backups	200Gb	Twice a day	1 Month
EOE-NRPTS02	Windows Server	F:\Data	300Gb	Twice a day	1 Month
EOE-NRPTS02	Windows Server	SQL Backup	500Gb	Daily	1 Month
EOE-NRTFS01	Windows Server	SQL Backup	300Gb	Daily	1 Month
EOE-NRWEB05	Windows Server	SQL Backup	200Gb	Daily	1 Month
EOE-NRPTS01	Windows Server	SQL Backup	400Gb	Daily	1 Month
EOE-ESFILE01	Windows Server	\\EOE-ESFILE01.eaamb.nhs.uk\EEAST	3000Gb	Daily	1 Month
EOE-NRFORMIC02	Windows Server	E:\FormicShareBackup_EOE-NRFORMIC01	250Gb	Daily	1 Month

EOE-ESDC01	Windows Server	Bare Metal Recovery	100Gb	Daily	1 Month
EOE-ESDC01	Windows Server	System State (includes AD)	100Gb	Daily	1 Month
EOE-ESDC02	Windows Server	Bare Metal Recovery	100Gb	Daily	1 Month
EOE-ESDC02	Windows Server	System State (includes AD)	100Gb	Daily	1 Month
EOE-ESSYSLOG01	Windows Server	D:\	100Gb	Daily	2 Months
EOE-ESAPP01	Windows Server	C:\	40Gb	Daily	2 Months
EOE-ESAPP01	Windows Server	SQL Backup	50Gb	Daily	2 Months
EOE-ESEDM01	Windows Server	SQL Backup	200GB	Daily	2 Months
EOE-BEDC01	Windows Server	Bare Metal Recovery	100Gb	Daily	1 Month
EOE-BEDC01	Windows Server	System State (includes AD)	100Gb	Daily	1 Month
EOE-BEDC02	Windows Server	Bare Metal Recovery	100Gb	Daily	1 Month
EOE-BEDC02	Windows Server	System State (includes AD)	100Gb	Daily	1 Month
EOE-BEAPPS01	Windows Server	C:\inetpub	25Gb	Daily	2 Months
EOE-BEAPPS01	Windows Server	D:\Planet	5Gb	Daily	2 Months
EOE-BESYSLOG01	Windows Server	D:\	100Gb	Daily	2 Months
EOE-BEAPPS01	Windows Server	SQL Backup	150GB	Daily	1 Month

	Number of mailboxes	Total Data size as of 04/10/2022
Email	7301	20.8TB
	Number of	
OneDrives	OneDrives	Total Data size as of 04/10/2022
	7076	7.5TB