East of England Ambulance Service NHS Trust

Electronic Data Backup Policy

Document Reference	POL048
Document Status	Approved
Version:	V5.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Head of IS&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
5.0	March 2019	Approved by Management Assurance Group

Document Reference	Directorate: Strategy & Business Development
Recommended at Date	Information Governance Group 9th January 2019
Approved at Date	Management Assurance Group 20 March 2019
Valid Until Date	January 2021
Equality Analysis	31st January 2019
Linked procedural documents	Information Security Policy IM&T Operational Security Policy
Dissemination requirements	All IS&T 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

Appendices

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.

DPM

Data Protection Manager, Microsoft software backup solution. The system in use at EEAS comprises of a large data storage server (NAS) on each site for local backups. Backups are then archived to another site's NAS.

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 Infrastructure and Systems Delivery Manager and Deputy Head of IT

7 Equality Impact Assessment

This is attached in Appendix D

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 – Document Checklist

	Title of document being reviewed:	Yes/No/ N/A	Comments
1.	**Purpose**		
	Are the reasons for the development of the Document stated?	**Y**	
2.	**Definitions**		
	Have all key terms been clearly defined?	**Y**	
3.	**Consultation**		
	Have relevant stakeholders and/or users been consulted with?	**Y**	
4.	**Equality Impact Assessment**		
	Has the Trust Equality Impact Assessment Screening Form been completed and attached by the author and approved by the responsible Executive Director?	**Y**	
5.	**Monitoring**		
	Has the Monitoring Table been fully completed and attached?	**Y**	
6.	**References/Associated Documents**		
	Are key references cited?	**Y**	
	Are linked documents identified where appropriate?	**Y**	
6.	**Approval**		
	Does the Document identify which committee/group will approve it?	**Y**	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	**Y**	
	Does the plan include the necessary training/support to ensure compliance?	**Y**	
8.	**Review Date**		
	Is the review date identified?	**Y**	

Information Governance Lead (or delegated authority)			
This Procedural Document complies with the Policy for the Development of Procedural Documents			
Name		Date	
Clinical Quality Team			
The Procedural Documents complies with the relevant NHSLA standards			
Name		Date	

Appendix B – Schedules and retention periods

Backup profile	Servers	Retention period	Synchromnisation schedule	Recovery point(s)	Additional
Bedford File Servers	EOE-BEAPPS01	60 days	Every 12 hrs	18:00	
	EOE-BEFS01				
	EOE-BEFS02				
	EOE-DCBE02				
Bedford SharePoint Servers	EOE-BESP01	30 days	Every 6 hrs	08:00, 18:00	SQL Backup recovery 20:00
Bedford SQL Servers	EOE-BEAPPS1	30 days	Every 15 mins	20:00	
	EOE-BESDESK01				
	FINASSET				
Bedford Virtual Servers	EOE-BEHYPV01	30 days	SBRP	00:00, 12:00	
Norwich PTS	EOEPTS	30 days	SBRP	20:00	
Norwich Exchange Servers	EOE-EXDB1	90 days	SBRP	20:00	
	EOE-EXDB2				
Norwich Hyper V Servers	EOE-HYPV10	5 days	SBRP	18:00	
	EOE-NRHYPV23				
	EOE-NRHYPV24				
Norwich Cleric SQL	EOE-NRPTSBE1	30 days	Every 1 hr	20:00	
	EOE-NRPTSBE2				
Norwich Data Servers	DOHMOTO	30 days	SBRP	08:00, 12:30, 18:00 (M - F)	
	EOE-FSNR01				
	EOE-FSNR02				
	EOE-NRDATIX01				
	EOE-NROPTIMA01				
	EOE-NRSDESK01				
	EOE-NRWEB06				
	ORMA				
Norwich DC System State	EOE-DCNR01	30 days	SBRP	02:30	

	EOE-DCNR02				
Norwich SQL Servers	DOHMOTO	30 days	Every 30 mins	20:00	
	EOE-DWPRD01				
	EOE-DWPRD02				
	EOE-DWPRD03				
	EOE-DWPRD05				
	EOE-NRCEM01				
	EOE-NRECS01				
	EOE-NRROTAMSTR				
	EOE-NRSDESK01				
	EOE0NRTFS01				
	EOE-NRWEB05				
Formic	EOE-NRFORMIC02	30 days	Every 12 hrs	18:00 (M-F)	
Essex File Servers	EOE-DCES02	60 days	SBRP	20:00	
	EOE-ESAPTS01				
	EOE-ESFS01				
	EOE-ESFS02				
GRS Database Servers	EOE-ESGRSDB01	30 days	SBRP	02:00	
Essex SQL Servers	EOE-ESAV01	60 days	Every 6 hrs	18:00	
	EOE-ESSS01				
Essex Terminal Servers	EOE-ESTSCAD02	60 days	Every 24 hrs	18:00	

*SBRP = synchronises before recovery point

Appendix C - 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 D – Equality Impact Assessment Executive Summary

Executive Summary Page for Equality Impact Assessment:	
Document Reference:	Document Title: **Electronic Data Backup Policy**
Assessment Date:**31st January 2019**	Document Type: **Policy**
Responsible Director: **Director of Strategy and Sustainability**	Lead Manager: **IM&T Security & Resilience Manager**
Conclusion of Equality Impact Assessment: **No impact**	
Recommendations for Action Plan: **None**	
Risks Identified: **None**	
Approved by a member of the executive team:	
YES	**NO**
Name: **Clare Chambers**	Position: **Head of IM&T**
Signature: **Approved via email**	Date: **4th February 2019**