East London
NHS Foundation Trust

ICT Housekeeping and Monitoring Policy

Version number :	1.2
Consultation Groups	Information Governance Steering Group, Digital Board and Key Leads
Approved by (Sponsor Group)	Information Governance Steering Group and Digital Board
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

		Page
	Executive summary	4
1	Introduction	4
2	Purpose	4
3	Procedure	4
4	Monitoring	4

Appendices

Appendix A	Housekeeping and Monitoring Procedure Spreadsheet	5

Executive Summary

The following document outlines the process for monitoring that security and other procedures and processes in place in the ICT Department are effectively being carried out on a regular basis. This is to minimize risk to the Trust's data and reputation, and to ensure that disruption from system failures is kept to a minimum.

1.0 Introduction

The Trust uses a number of systems to monitor the various software and hardware devices in use to ensure that they are secure, and that only authorized users are accessing them. Also, these systems are used to monitor performance and help avoid or detect problems when or before they occur.

2.0 Purpose

The purpose of this document is to describe the procedures, systems, frequency and methods of monitoring specific applications and devices on our Trust network to maintain its integrity.

3.0 Procedure

The procedure is described at Appendix A attached. The Assistant Director of IT will ensure the procedure is followed, and the audit sheet regularly updated. Any issues will be escalated to the CIO.

4.0 Monitoring

The Assistant Director of IT will report annually to the CIO on the audit programme. The report will be reviewed by the CIO and submitted to the Digital Strategy Board. Any urgent exceptions should be reported to the CIO as they occur, and any minor exceptions reported at the monthly meeting.

Progress on resolution of any exceptions will be monitored via the monthly meetings within the IT department.

Appendix A

Audit Program									
Audit Entity Risk	**Control Objective**	**Audit Test or Procedure**	**Frequency**	**Number of Users/Devices**	**Performed By**	**Date Completed**	**Document Reference**	**Reviewed By**	**Remarks/Comments**
		· review firewall logs							
Authorization and Access Management									
Access to the network should be appropriately restricted to reduce the risk of security breaches.	Authorization of access to the network (e.g., file and print services, application servers, database servers) is appropriately restricted to reduce the risk of security breaches. The New User request is followed and logged appropriately.	Select a sample of users and obtain applicable authorization forms. Verify and record, through examination of forms, that the access request process · approval by appropriate department manager · approval by IT Management · user is a current employee · new user process is followed by the HelpDesk	Quarterly	5			Authorised Signatory Request		
Access levels should be monitored and granted to only those authorized individuals to ensure that only the appropriate personnel have access to the network.	Ensure level of access is managed on a scheduled basis	Test current user lists for all access levels to determine that only authorized individuals have access and determination of need of access level Check Administrator Groups membership Check for users other than full time employees (PT, contract, external clients/vendors) access level and remote access availability.	Quarterly Monthly Quarterly	5			Authorised Signatory Request		
Hardware and Software									
If software is not upgraded periodically to newer versions the software will not have the latest security upgrades therefore making it more susceptible to unauthorized users.	Ensure awareness and review of latest software patches and reviews are periodically reviewed for upgrades to newer versions which may provide valuable enhancements and increased	Review the patch and software upgrade process using WSUS for Windows as well as for non-MS software eg. Adobe Acrobat Reader.	Monthly	2 per site			Patching & AV Policy		
If Anti-Virus software is not updated on end devices or servers there is considerable risk of virus outbreak, malicious damage or compromised systems	Ensure anti-virus software is updating on the AV Server and end devices. Review logs for activity.	Check the logs on the AV server and update schedules.	Monthly	2 per site					
Back-ups									
If servers/data are not backed up there is considerable risk eg. hardware failure, accidental deletion, inadvertantly overwriting	Ensure backups are completed, all data/servers are backed up, tapes are sent off site as per the schedule.	Review logs, perform sample restores Restore a file Restore a directory Restore an email Restore a mail box Restore a Public Folder item Restore a SQL DB Restore a Virtual Server Restore a Physical Server Check Tape schedule	 Monthly Monthly Monthly Monthly Monthly Monthly Quarterly Quarterly Monthly	n/a					
Change Control Policies									
If change controls procedures and processes are not followed there is a risk that production systems are modified without adequate planning and notification. This could potentially cause outages to critical systems.	Ensure changes to production systems follow the change control process and are fully documented.	Check change control log Check email trails sent to change control panel distribution group Check for approval/rejection emails	Monthly	n/a			Change Control Procedure		

(Original of this spreadsheet can be located on SharePoint.)