NHS Lothian

Digital & IT

Procedure for Re-approving systems used by NHS Lothian

April 2020

Author(s): Information Governance

Owner: Filip Horvat

Version No: 1:3

Status : Trial Version

Release Date: 17/04/2020

1. Document History

1.1. Document Location

This document is only valid on the day it was printed.

The source document can be found at the following location:

1.2. Revision History

Date of this revision:17/04/2020

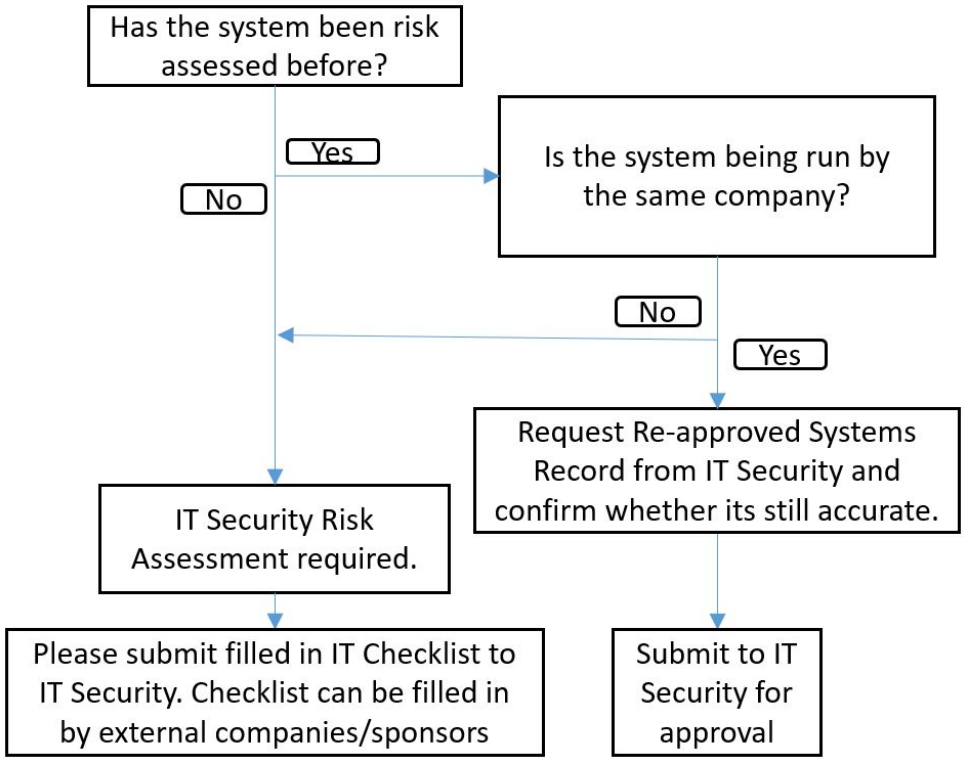
Date of next revision:

Revision Date	Version	Summary of Changes	Revised By
28/02/2020	Draft V1.0	Creation of discussion draft	
10/03/2020	Draft V1.1	Minor changes to wording	Filip Horvat, Carol MacKenzie, Pamela Linksted
03/04/2020	Draft V1.2	Flowchart adjusted	Filip Horvat
17/04/2020	Trial Version for R&D	Minor adjustments made	Filip Horvat, Martin Clunie
24/04/2020	Trial Version for R&D	Name of the document changed. Further minor adjustments.	Filip Horvat, Martin Clunie, Carol MacKenzie
26/08/2020	Trial Version for R&D	Name of the document changed to Re-approved Systems Procedure.	Filip Horvat

Creating and developing an inventory of safe systems

This document describes the procedure for Re-approving systems used by NHS Lothian Research and Development on a frequent basis.

The purpose of this arrangement is to create approval process of systems that have already been assessed. Where the setup and use of the system is consistent with that approved previously, further risk assessment would not be required. Failure to provide accurate details will result in approval being delayed.



Step 1.
Determine whether the service/system in question has been risk assessed before. This can be done by contacting IT Security Project Manager filip.horvat@nhslothian.scot.nhs.uk or in his absence by emailing Lothian.ITSec@nhs.net.
Please include as much detail as you can (job reference number, name of the project, name of original requestor, date of assessment, etc.)

Step 2.
Where the system has been risk assessed before, IT Security will issue you with a Re-approved System Record containing basic information about the service/system gathered during the last assessment. Confirmation is required that the Re-approved System Record is accurate for this subsequent use of the system and if not accurate, any differences noted. You can do this by forwarding the document onto the company/service in question and asking them to confirm compliance. The document will need to be signed by the member of staff requesting the service.

Step 3.
Forward the signed Reapproved System Record to IT Security.

Step 4.
IT Security will confirm if you can proceed with using the product.
IT Security will need to perform risk assessment taking in to account any changes that occurred since the last assessment. Additional information may be required.

Example of **Preapproved System Record**

Author/s: Information Governance
Release: 17/04/2020
Version: Trial Version
Owner: Filip Horvat

General Information		**Define any differences.**
Company:	Generic Company Inc.	
Product:	Generic Product	
Product Description	Web based file transfer tool.	
Data management		
Data Type:	CT Scans	
Retention Period:	Generic Company Inc. retention standards are currently 15 years for clinical trial data and TMF, however this is extending prospectively to 25 years once the EU Clinical Trial Regulation is fully implemented.	
Data accessed by:	Generic Company Inc.	
Technical Detials		
Service supported by:	Generic Company Inc. Charlotte, NC 28214 Wildwood Drive HelpDesk@ Generic Company.com (+1 848-275-1234).	
Infrastructure managed by:	Generic Company servers managed by AWS (Amazon Web Services).	
Infrastructure location:	US West availability zone.	
Data transfer between NHS Lothian and external infrastructure:	Transfer to external agency via encrypted link. 256-bit SSL encryption on all data traffic.	

Procedures and technological standards:	Generic Company standards are aligned to ISO 27001 requirements. POL-GL-QA-001 - Data Privacy Policy, POL-GL-IT-008 - Password Policy, GL-IT-W012 - Security Auditing Procedure, GL-IT-009 - Security Vulnerability Assessment Procedure and GL-GO-012 - Security System Training are among those governing policies and procedures.	
Data Destruction:	Media will be destroyed in accordance with IM-RM-005 Imaging Media Destruction, a certified destruction service allowing for required auditability and traceability.	
Penetration testing results:	No penetration information available.	

Reference number of the previous assessment:

Please confirm that supplied information is accurate and that any changes to the system have been highlighted.

Name of the contact confirming the accuracy of the record on behalf of the company:

Position within the company:

NHS Lothian requestor name:

Signature:

Date: