NHS
East London
NHS Foundation Trust

Security and AV Patching Policy

Version number :	2.1
Consultation Groups	Information Governance and IT Leads
Approved by (Sponsor Group)	Information Governance Steering Group
Ratified by:	Quality Committee
Date ratified:	20 February 2019
Name of originator/author:	Server Manager, Usman Malik
Executive Director lead :	Chief Digital Officer
Implementation Date :	February 2019
Last Review Date	February 2022
Next Review date:	February 2025

Services	**Applicable**
Trustwide	x
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	**Date**	**Author**	**Status**	**Comment**
1.0				
2.0	20/02/2019	Asim Mir	Expired	
2.1	08/02/2022	Usman Malik	Live	Updated with new AV and patch software tools

CONTENTS

1 Introduction 4

2 Duties 4

3 Process 4

4 Desktop Patching………………………………… 4

5 Patch Testing, Release and Problem Reporting 4

6 Accelerated Patch Release 5

7 Laptops and Devices not Connected directly to the Trust Network 5

8 Patching of Servers 5

9 Patching of Routers and Switchers 5

10 Antivirus Guidelines 5

11 Scheduled Scanning of Files 6

12 Containment of Virus Incidents 7

13 Scanning of Email for Threats 7

14 Monitoring 7

1. Introduction

The increased use of electronically stored information in the Trust increases the risk of data being copied, modified, hidden or encrypted, accessed by unauthorized persons, stolen or destroyed. Unless systems are appropriately secured, there is an increased risk that they will be used to mount attacks against other organizations, potentially damaging the reputation of the Trust.

It is essential that those who administer and manage IT facilities to do so within the policy frameworks concerning data protection and information governance.

This document forms the Trust's Security Patching Policy in support of its Information Security Policy. Compliance with this Policy will ensure that consistent controls are applied throughout the Trust to minimize potential exposure to security breaches.

2. Duties

This Policy is primarily aimed at systems administrators and technical support staff who are responsible for the development and maintenance of IT.

Applicability extends to those Trust staff undertaking activities governed by this Policy.

It is the personal responsibility of each person to whom this Policy applies to adhere fully with its requirements.

The IT Server Manager and IT Network Manager will ensure that this policy is implemented and utilized by the IT technical team

3. Process

All Trust systems that connect to the network, including routers and switches, are to be protected both from malicious code and hacking attacks which exploit software vulnerabilities through the deployment and installation of security patches.
Critical security patches must be installed universally across applicable devices, as they become available, in accordance with this Policy.

4. Desktop Patching (Microsoft Operating Systems)

The IT Server Manager will ensure that all desktop computers connected to the Trust network have up to date patches applied.

This is facilitated by using a deployment tool called Desktop Central Manage Engine, which is updated automatically and updates devices on a regular basis via automated task sequences.

5. Patch Testing, Release and Problem Reporting

The IT Server Manager is responsible for ensuring all Microsoft patches are thoroughly tested before being released via the centrally provided patching service each month.

Patches that cause problems will not be deployed and an alternative solution will be sought. Automated task sequences are currently scheduled to run 24/7 due to the high volume of devices on the network, otherwise Trust connected devices are in danger of not applying critical fixes in a timely fashion with the setting on the device to Auto Download and install.

6. Accelerated Patch Release

When an exploit to vulnerability is published prior to the roll-out of a patch, an assessment will be carried out by the IT and Telecoms Infrastructure Development Manager to determine whether a reduced testing period and early deployment is considered necessary.

Where the risk of system compromise is considered to be greater than deployment of a partially tested patch, a decision by the Associate Director of IT will be taken to release the patch early.

7. Laptops and devices not connected directly to the Trust network

All laptop computers will be subscribed to the centrally provided patching service.
It is the responsibility of the end user to ensure that all computers that are not directly connected to the Trust network are periodically connected to the network to ensure they are fully patched and up to date. Once the patching tool has been successfully deployed onto the endpoint, patching can be done over a personal WiFi connection for the most critical updates such as Microsoft security fixes. Other updates unique in their deployment to the Trust will need to be connected to the network to receive said updates, either by physically being on-site connection or over the Trust's approved VPN solution, Cisco AnyConnect.

8. Patching of Servers

It is the responsibility of the IT Server manager to ensure all Trust servers have security patches applied within two working weeks of the patches being released. An automated means of patch deployment will be used to fulfil this requirement although time schedules are to be chosen by the administrators. This is to control of any potential impact.

9. Patching of Routers and Switches

The IT Network Manager will subscribe to appropriate security alert e-mailing lists and proactively monitor appropriate web sites for notification of any vulnerabilities affecting routers and switches.

Where vulnerabilities are found to apply to network devices, advice will be sought from the third party network support contractor to determine whether it is feasible to use a work- around solution rather than apply a patch immediately. Where possible the application of patches will be deferred until the next available scheduled maintenance slot. However, where deferment is not advisable, a risk assessment will be carried out and remedial action will be taken, following local procedures which are designed to minimise disruption.

10. Antivirus Guidelines

The Trust has a site license for up to 10,000 installations of Sophos virus protection software for PCs and laptops.

Deployment of Anti-Virus Software

Sophos Central Console:

Hosted by vendor.
https://cloud.sophos.com/manage/login

Required AD Accounts:

All required accounts were created by local staff and the details were stored in KeePass.

Software Subscriptions were left at the default / recommended setting.

Endpoints:

The endpoint list was set by policies whereby a task sequence is initiated whenever a device is joined or re-joined to the network. Local files and registry is queried to confirm existence of existing Antivirus (AV) software and if none is found to be present, an install takes place.

Updating:

Each device is able to update its Antivirus over any Internet connection inside or outside the Trust to ensure it is always updated whenever a device has an active Internet connection.

Policies:

Enforce web, application, device, data and anti-ransomware policies with ease, thanks to seamless integration within the endpoint agent and the management console.

Web Control Category-based web filtering that is enforced both on and off the corporate network

Application Control Point-and-click blocking of applications by category or by name

Device Control Managed access to removable media such as USB sticks and mobile devices. All unencrypted and unapproved (whitelisted) devices are blocked from USB access.

Data Control Data loss prevention (DLP) using prebuilt or custom rules

Message Relays:

In order to reduce the amount of network activity caused by endpoints on a Trust site, reporting to Sophos Central Console message relays were created on all local SUMs. Endpoints on a site with a local SUM will relay messages to Enterprise Console via the local SUM. This also reduces the amount of connections to Sophos Central Console and thus improves the responsiveness.

11. Scheduled Scanning of Files

Daily server scans of local data volumes are set to run overnight, these scans terminate after 8 hours to prevent overrun into normal working hours. Daily scans on endpoints commence each day at 12pm.

12. Containment of Virus Incidents

The IT department will take appropriate action to contain virus infections and assist in their removal. In order to prevent the spread of a virus, or to contain damage being caused by a virus, the IT department may remove a suspect computer from the network or disconnect a segment of the network.

Infected machines will be cleaned or reimaged before reconnection to the network.

13. Scanning of Email for Threats

An NHS Mail email Gateway is deployed to provide virus scanning and malware detection.

The Trust benefits from scanning on the national NHS mail relays as there is an arrangement of a 24/7 security team that can implement changes to gateways quickly as required.

14. Monitoring

The IT Server Manager will ensure all hardware is monitored and that patches have been correctly applied. Automated reporting of the patching compliance of PCs in the Domain will be regularly undertaken. The IT Server Manager is responsible for confirming the patch compliance of all Trust systems, and taking prompt remedial action where systems are found to be not fully up to date.