A member of:
Association of UK University Hospitals

Sussex Partnership
NHS Foundation Trust

# IT Patching Policy

| | |
|---|---|
| POLICY NUMBER | TP/CO/102 |
| POLICY VERSION | V1.0 |
| RATIFYING COMMITTEE | Information Governance Security Assurance Group |
| DATE RATIFIED | November 2019 |
| NEXT REVIEW DATE | November 2021 |
| DATE OF EQUALITY & HUMAN RIGHTS IMPACT ASSESSMENT (EHRIA) | N/A |
| POLICY SPONSOR | Chief Digital Information Officer |
| POLICY AUTHOR | IT Infrastructure and Operations Manager |

## EXECUTIVE SUMMARY:

This policy highlights the patching requirements to ensure the security of trust information. The objective is to ensure that all devices and applications are patched in accordance with the latest patch releases. It applies to all devices and applications used by Trust staff.

**If you require this document in another format such as large print, audio or other community language please contact the Corporate Governance Team on: 0300 304 1195 or email: policies@sussexpartnership.nhs.uk**

# Table of Contents

# BODY OF THE DOCUMENT

## 1.0 Introduction

### 1.1 Purpose of policy

- The purpose of this document is to define the policy for patching all server, client devices and applications used by Sussex Partnership NHS Foundation Trust.

### 1.2 Definitions

| | |
|---|---|
| **Trust** | Sussex Partnership NHS Foundation Trust |
| **End User** | The person utilising the Trust systems |
| **IT systems include** | |
| | • Servers (physical and virtual)<br>• Workstations<br>• Firmware<br>• Networks (including hardwired, Wi-Fi, switches, routers etc.)<br>• Hardware<br>• Software (databases, platforms etc.)<br>• Applications (including mobile apps) |
| **SCCM** | Microsoft System Centre Configuration Manager – is a systems management software used to deploy patches across Trust managed devices. |
| **Phase** | • Phase 0 (Initial Test machine)<br>• Phase 1 (Key test users - <5 machines)<br>• Phase 2 (Whole CDIO department)<br>• Phase 3 (Trust wide key systems users)<br>• Phase 4 - Trust Wide |
| **CAB** | Change Advisory Board, approving requested changes to the trust it environment, assists in the assessment and prioritisation of changes. |

### 1.3 Scope of policy

The scope of this document is limited to systems hosted and managed by the Trust IT department including systems hosted as part of the IT contract held with Daisy Data Centre Solutions.

### 1.4 Principles

The Trust has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems on and off site which includes systems and services

supplied by third parties. The Trust has an obligation to provide appropriate and adequate protection of all IT estate whether it is IT systems on premise, in the Cloud or systems and services supplied by third parties.

## 2.0 Policy Statement

The effective implementation of this policy reduces the likelihood of compromise which may come from an internal or external malicious threat.

## 3.0 Duties

- The Trust IT department will manage the patching needs for the Windows and Linux estate that is connected to the Trust domain. It is responsible for routinely assessing compliance with the patching policy and will provide guidance to all the stakeholder groups in relation to issues of security and patch management.
- Change Advisory Board (CAB) is responsible for approving the monthly and emergency patch management deployment requests.
- The End User has a responsibility to ensure that patches are installed and the machine is rebooted when required. Any problems must be reported to the IT helpdesk.
- Third Party Suppliers will ensure security patches are up-to-date for IT systems which are being designed and delivered by third party suppliers prior to going operational. Once the IT systems are operational, third party suppliers must ensure vulnerability patching is carried out.

## 4.0 Procedure

All patching will follow an agreed implementation process;

- Patch released and available in SCCM
- 1-3 days - Deployed to Phase 0
- 4-5 days – Deployed to Phase 1
- 9-13 days – Deployed to Phase 2
- 18-21 days – Deployed to Phase 3
    - 2nd phase of Microsoft patches released and available in SCCM
    - 2nd phase deployed to Phase 3
- 28 days – Deployed to Phase 4

## 5.0 Equality and Human Rights Impact Analysis (EHRIA)

- An impact analysis is deemed unnecessary.

## 6.0 Monitoring Compliance

- The IT department will monitor the deployment of Microsoft and application patches on a monthly basis utilising the SCCM tool.
- On a yearly basis the Trust will undertake the Cyber Essentials Plus certification to identify any gaps in patching levels and rectify these as part of the certification process.

## 7.0 Reference documents

- Third party – Daisy Patching Policy