POLICY SUMMARY

The purpose of this Patch Management Policy is to provide guidance in line with HMG and private sector best practice for the implementation of an organisation wide Anti-Virus and Malware Policy. Ensuring that the applicable and relevant anti-virus and malware security controls are set in place in line with the Department for Health, the wider NHS, health and social care and HMG requirements.

The Trust monitors the implementation of and compliance with this policy in the following ways:
Continual monitoring by ICT Services

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Essex MH&amp;LD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is
Director of Information Technology and Telecommunication
CONTENTS

1.0 OVERVIEW
2.0 ROLES & RESPONSIBILITIES
3.0 MONITORING
4.0 REVIEW AND EVALUATION
5.0 IMPACT, RISK ASSESSMENT AND TESTING
6.0 IMPLEMENTATION
7.0 AUDITING, ASSESSMENT AND VERIFICATION
1.0 OVERVIEW

1.1 Patch Management is the ability to implement patches in a timely manner using strategies and plans as appropriate to ensure systems and services continue to be available and secure for the purposes of the business function(s) they provide.

1.2 Patching (sometimes also known as a “fix”) is a technique used to correct a problem (often known as a “bug”) in a computer program. This is typically done by obtaining a repair program from the vendor which the original computer program was purchased from.

1.3 Patches can be summarised into two categories –

   - **Functional**
   - **Non-Functional**

1.4 **Functional** - This typically involves correcting features or functionality of a computer program. Functional patches may involve changes to the “look and feel” of certain areas of a product or areas that may not work as intended but which do not affect the overall security of the application.

1.5 Customer requirements for functional patch deployment should be directed to the ICT Service Desk in the first instance.

1.6 **Non-Functional** - These types of patch are released for several purposes, many of which are security related. The focus of this policy will therefore only consider these patches where they are released to repair or mitigate a specific security vulnerability found in a system in live service.

1.7 The severity of the vulnerability generally dictates the timescale for availability, ultimately leading to deployment and subsequent correction of the vulnerability.

1.8 The addition of the patch will not usually affect functionality or have effects to users of systems or services; however, this should be confirmed via Pre-deployment testing and/or post implementation testing, where systems have clinical impact or use.
2.0 ROLES AND RESPONSIBILITIES

2.1 ICT is responsible for the overall patch management implementation, operations, and procedures. While safeguarding the network is every user’s responsibility, the Cyber Team ensures all known and reasonable precautions are in place to reduce network vulnerabilities while keeping the network operating.

2.2 ICT will manage the patching needs for:
   - All IT infrastructures on the network and associated components owned or managed by EPUT
   - All applications owned or managed by EPUT

2.3 ICT will be responsible for routinely assessing compliance with the patching policy and will provide guidance on issues of security and patch management.

2.4 ICT will have responsibility, on behalf of all system owners for the implementation, management and enforcement of patching for the system

3.0 MONITORING

3.1 ICT will monitor NHS Digital CareCERT notifications, security mailing lists, review OEM notifications and Web sites, and research specific public Web sites for the release of new patches. Monitoring will include, but not be limited to -

   - Scanning EPUT’s infrastructure to identify known vulnerabilities.
   - Identifying and communicating identified vulnerabilities and/or security breaches to the EPUT IT Security Manager.
   - Monitoring notifications, and Web sites of all vendors that have hardware or software operating on EPUT’s network

4.0 REVIEW AND EVALUATION

4.1 Once alerted to a new patch, ICT will download and review the new patch within three days of its release. ICT will categorise the criticality of the patch according to the following:

   - Emergency — an imminent threat to EPUT’s network.
   - Critical — targets a security vulnerability
   - Not critical — a standard patch release update
   - Not applicable to EPUT’s environment

4.2 Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the impact, risk, testing, scheduling, installing, and verifying.
5.0 IMPACT, RISK ASSESSMENT AND TESTING

5.1 ICT will assess the impact of a patch to the corporate infrastructure prior to its deployment. The team will also assess the particular patch for criticality relevant to each platform (e.g., servers, desktops, printers, etc.).

5.2 If ICT categorises a patch as an Emergency, the team considers it an imminent threat to EPUTs network. Therefore, EPUT assume greater risk by not implementing the patch prior to testing.

5.3 Patches deemed Critical or Not Critical will undergo testing against operating system and core software before release for implementation. Testing will be via deployment to a predefined list of UAT machines, it is the UAT member’s responsibility to ensure all systems are tested on behalf of the department and report any issues to ICT immediately. If no response is received from the UAT members, ICT will assume that the patches have been tested successfully and will proceed to release.

5.4 ICT will expedite testing for critical patches relating to servers and other core infrastructure equipment in a test environment. The testing will cover hardware compatibility, Operating Systems and core software.

6.0 IMPLEMENTATION

6.1 ICT will deploy Emergency patches within 1 day of availability. As Emergency patches pose an imminent threat to the network, the release may precede testing.

6.2 The timeline for releasing critical patches is as follows:

- Available \( A = 0 \)
- Submit for testing \( A + 3 \) working days
- Approved \( A + 10 \) working days
- Release \( A + 14 \) working days

6.3 ICT will obtain authorisation for implementing Critical patches via the standard request for change process.

6.4 Patches will be released to servers and core infrastructure utilising maintenance windows enabling reboots out of hours and where agreed with the relevant system owners.

6.5 For new devices, each platform will follow hardening procedures at point of provisioning to ensure installation of the most recent patches.
7.0 AUDITING, ASSESSMENT AND VERIFICATION

7.1 Following the release of all patches, ICT will verify the successful installation of the patch and that there have been no adverse effects.

7.2 Any system found in violation of this policy will require immediate corrective action.

END