APPENDIX M

Patch Management Policy

1. Introduction

Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software which can disrupt normal business operations in addition to placing the Authority's data at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability. A comprehensive patch management solution is utilised by 'the Authority' to effectively distribute security patches automatically when they are made available. The patch management solution has the ability to evaluate individual computer workstations and servers for vulnerabilities. Patches may then be automatically installed and, when necessary, the affected machine rebooted.

2. Scope

This policy applies to employees (permanent and temporary), contractors, consultants, and other workers. This policy applies to all equipment that is owned or leased by 'the Authority' such as all electronic devices, servers, application software, computers, peripherals, routers, and switches.

3. Policy

Many computer operating systems such as Microsoft Windows, Linux, Mac OS and others include software application programs which may contain security flaws.

Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the network and all computers connected to it. Almost all operating systems and many software applications have periodic security patches released by the vendor that need to be applied. Patches which are security related or critical in nature should be installed.

- In the event that a critical or security patch cannot be centrally deployed by ICT, it must be installed in a timely manner using the best resources available. In the case of non Microsoft desktop operating systems where a centralized deployment is not available then installation should occur in a timely manner by a member of User Support Services or Network, Security, and System Services personnel or the end user.

- Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing or tampering with patch management protections and/or software constitutes a violation of policy.

4. Responsibilities

It is the responsibility of all users to ensure responsible use of computing and network resources. Any attempts to by-pass or disable patch deployment may result in disciplinary action.

IT Services staff are responsible for the overall patch-management implementation, operations and procedures. While safeguarding the network is every user's responsibility, the Technical Support Team will ensure that all known and reasonable defences are in place to reduce network, operating system and corporate software vulnerabilities while keeping the network operating. The Applications Development and Support Team will ensure that individual application systems are kept up to date in line with supplier recommendations. IT Services will ensure that unsupported products are replaced in line with vendors' end of life notifications.

5. Monitoring

Steria Ltd will monitor security mailing lists, review vendor notifications and web sites, and research specific public web sites for the release of new patches. Monitoring will include, but not be limited to, the following:

- Scanning the 'the Authority' network to identify known vulnerabilities
- Using automated tools such as Microsoft WSUS
- Identifying and communicating identified vulnerabilities and/or security breaches to 'the Authority' Information Security Officer and IT Manager
- Subscribing to govcertuk.gov.uk notifications
- Subscribing to notifications and checking web sites of all vendors that have hardware or software operating on 'the Authority' network.

6. Review and evaluation

Once alerted to a new patch, Steria will download and review the new patch within one working day of its release and will categorise the criticality of the patch according to the following:

- Emergency — an imminent threat to 'the Authority' network
- Critical — targets a security vulnerability
- Non Critical — a standard patch release update
- Not applicable to 'the Authority' environment

Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, scheduling, installing and verifying.

7. Risk assessment and testing

Steria will assess the effect of a patch on the corporate infrastructure prior to its deployment. They will also assess the affected patch for criticality relevant to each platform (for example, servers, desktops, printers and so on).

If Steria categorise a patch as an Emergency, it is considered to be an imminent threat to 'the Authority' network and there is a greater risk by not implementing the patch immediately.

The majority of patches will be deemed Critical or Non Critical and will undergo testing for each affected platform before release for implementation. The Technical Support Team will expedite testing for critical patches. Testing of SQL patches will be agreed with the client. Validation of patches against all images should be completed prior to implementation.

All Patches Must go through the Change Management Process.

8. Implementation

Steria will aim to deploy Emergency patches within one working day of availability. As Emergency patches pose an imminent threat to the network, the release may precede testing. In all instances, Steria will perform testing either pre-installation where possible or post-implementation in an extreme emergency situation and document it for auditing and tracking purposes. For all patches a RFC MUST be raised and authorisation MUST be sought from the Infrastructure Manager, the Steria Account Manager, or from the IT Manager in line with the Change Management Policy.

Timeline for releasing Emergency patches Help Desk Priority 1:

Available A = day 0
Submit for testing: <A + 0.5 day
Approval: < A + 0.5 day
Release: < A + 1 day

Timeline for releasing Critical patches Help Desk Priority 4:

Available A = day 0
Submit for testing: <A + 1 day

Approval: < A + 2 days
Release: < A + 3 days

Timeline for Non Critical patches Help Desk Priority 5:

Available A = day 0
Submit for testing: <A + 5 days
Approval: < A + 10 days
Release: < A + 20 days

9. Auditing, Assessment and Verification

Following the release of all patches, Steria will verify the successful installation of the patch and that there have been no adverse effects. The RFC may not be closed on the IT Help Desk until this stage has been completed.

10. Definitions

The Microsoft Windows Server Update Services (WSUS): enables information technology administrators to deploy the latest Microsoft product updates. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.