INFORMATION SECURITY POLICY

# TECHNICAL VULNERABILITY & PATCH MANAGEMENT

| | |
|---|---|
| **ISO 27002** | 12.6.1 |
| Author: | Chris Stone |
| Owner: | Ruskwig |
| Organisation: | TruePersona Ltd |
| Document No: | SP-12.6.1 |
| Version No: | 1.1 |
| Date: | 1st September 2009 |

# Document Control

## Document Storage

**Document Title** Technical Vulnerability & Patch Management

**Document Location** C:\www\Ruskwig\docs\iso-27002\Technical Vulnerability Patch Management - RW.doc

## Version History

| Version No | Version Date | Author | Summary of Changes |
|---|---|---|---|
| 1.1 | 01/09/2009 | Chris Stone | First Issue |
| | | | |

## Approvals

| Name | Title | Date of Approval | Version No |
|---|---|---|---|
| Chris Stone | Head of ICT | 01/09/2009 | 1.1 |
| | | | |

## Distribution

| Name | Title | Date of Issue | Version No |
|---|---|---|---|
| Everyone | Internet | 03/01/2010 | 1.1 |
| | | | |

# Contents

**DOCUMENT CONTROL** 2

**Document Storage** 2

**Version History** 2

**Approvals** 2

**Distribution** 2

**CONTENTS** 3

**0. OVERVIEW** 4

**1. PURPOSE** 4

**2. SCOPE** 4

**3. RISKS** 4

**4. POLICY** 5

4.2 Up to date Inventory 5
4.3 Vulnerability Scanning 5
4.4. Identifying Patches to be Applied 5
4.5 Types of Patches 6
4.6 Roles and Responsibilities 6
4.7 Patching Schedule 7

**5. ENFORCEMENT** 8

**6. DEFINITIONS** 9

# 0. Overview

0.1 The goal of vulnerability and patch Management is to keep the components that form part of information technology infrastructure (hardware, software and services) up to date with the latest patches and updates.

0.2 Vulnerability and patch management is an important part of keeping the components of the information technology infrastructure available to the end user. Without regular vulnerability testing and patching, the information technology infrastructure could fall foul of problems which are fixed by regularly updating the software, firmware and drivers. Poor patching can allow viruses and spyware to infect the network and allow security weaknesses to be exploited.

# 1. Purpose

1.1 This policy defines the procedures to be adopted for technical vulnerability and patch management.

# 2. Scope

2.1 This policy applies to all components of the information technology infrastructure and includes:-

- Computers
- Servers
- Application Software
- Peripherals
- Cabling
- Routers and switches
- Databases
- Storage
- Telephone Systems

2.2 All staff within the IT Department must understand and use this policy. IT staff are responsible for ensuring that the vulnerabilities within the IT infrastructure are minimised and that the infrastructure is kept patched up to date.

2.3 All users of users have a role to play and a contribution to make by ensuring that they allow patches to be deployed to their equipment.

# 3. Risks

3.1 Without effective vulnerability and patch management there is the risk of the unavailability of systems. This can be caused by viruses and malware exploiting systems or by out of date software and drivers making systems unstable.

# 4. Policy

4.1 The organisation's IT infrastructure will be patched according to this policy to minimise vulnerabilities.

### 4.2 Up to date Inventory

4.2.1 The IT Department will maintain an up to date inventory of the components within the organisation's IT infrastructure.

4.2.2 The software and hardware identified will scanned for vulnerabilities and patched according to this policy.

### 4.3 Vulnerability Scanning

4.3.1 All of the hardware and software on the organisation's network will be scanned using a vulnerability scanner to identify weaknesses in the configuration of systems and to determine if any systems are missing important patches, or software such as anti-virus software.

4.3.2 The organisation's network will be scanned at a minimum on a quarterly basis.

4.3.3 Remediation will be undertaken of any vulnerabilities identified.

### 4.4. Identifying Patches to be Applied

4.4.1 The organisation's anti-virus server will be configured to automatically down load the latest virus and spyware definitions and push them to the servers, PC's and tablets running on the network.

4.4.2 Windows patch management tools will be utilised to automatically download the latest Microsoft security patches. The patches will be reviewed and applied as appropriate.

4.4.3 Security weaknesses and software update notifications issued by Computer Emergency Response Teams (CERT) will be monitored on a regular basis and any critical issues affecting the organisation's IT infrastructure will be attacked upon immediately.

4.4.4 Notifications of patches from application and database vendors will be reviewed and the patches applied as appropriate. Where notifications are not automatically sent, the suppliers website will be reviewed on a regular basis.

4.4.5 The websites of the suppliers of servers, PC's, tablets, printers, switches, routers and peripherals will be reviewed to determine the availability of firmware patches.

4.4.6 Missing patches identified as a result of vulnerability scanning will be implemented as appropriate. Any weaknesses identified will be rectified.

### 4.5 Types of Patches

4.5.1 The following patches will be implemented on the different information infrastructure types.

| Type | Patch |
|---|---|
| Server / Computer | BIOS, firmware, drivers |
| Operating System | Service packs, patches, feature packs |
| Application Software | Service packs, patches, feature packs |
| Router and Switches | Firmware |
| Anti Virus / Anti Spyware | Data file/Virus definition update |
| Printers | Driver, firmware |
| Scanners | Driver, firmware |

### 4.6 Roles and Responsibilities

4.6.1 The employees detailed below will be responsible for patch management.

| Role | Responsible Officer | Comments |
|---|---|---|
| Patch identification | System Owners and System Administrators | Responsible for identifying patches for the application systems which they own or administer. |
| Technical Patch Administration | Technical Team Manager | Responsible for patch approval and ownership of all technical updates including:-<br>• Operating systems<br>• patches for PC's and servers<br>• Antivirus and antispyware<br>• Firmware<br>• Printer drivers. |
| Technical Release Administration | Technical Team Manager | Responsible for the planning, building, testing and deploying new hardware or software. |
| Application Patch Administration | System Administrators | Responsible for patch approval and ownership of all application updates. |
| Application Release Administration | System Administrators | Responsible for the planning, building, testing and deploying new application software. |
| Vulnerability & Security scanning | Security Manager | Responsible for scanning the components on the network for security weaknesses and missing patches. |
| Change Manager | Change Approval Board | Responsible for the assessment and approval of major ICT infrastructure changes or the introduction of new hardware or software. |

### 4.7 Patching Schedule

4.7.1 The organisation's ICT infrastructure will be patched according to this schedule.

4.7.2 PC's & Tablets

4.7.3 PC's and tablets should be patched according to the schedule below.

| Time | Action |
|---|---|
| Daily | • Microsoft critical updates, and security updates configured to be approved for rollout as they are released.<br>• Anti-virus and spyware definitions configured to be installed automatically as they are released. |
| Weekly | • New software releases reviewed and approved as required. |
| Monthly | • Check that drivers are up to date. |
| Quarterly | • Review vulnerability scans and remediate as required. |
| Six monthly | • Check for BIOS updates. |

4.7.4 Windows Servers

4.7.5 Servers should be patched according to the schedule below.

| Time | Action |
|---|---|
| Daily | • Anti-virus and spyware definitions will be configured to be installed automatically as they are released. |
| Weekly | • Critical security patches reviewed and approved as required. |
| Monthly | • Public facing servers – apply all outstanding patches. |
| Quarterly | • Apply all outstanding patches.<br>• Check that drivers are up to date.<br>• Review vulnerability scans and remediate as required. |
| Six monthly | • Check for new printer drivers.<br>• Check for BIOS updates. |

4.7.6 Sun Servers

4.7.7 Sun servers should be patched according to the schedule below.

| Time | Action |
|---|---|
| Weekly | • Critical security patches reviewed and installed as required. |
| Quarterly | • Apply latest rollup patch.<br>• Review vulnerability scans and remediate as required. |

4.7.8 Printers, Peripherals, Switches, Routers and Storage

4.7.9 Printers, peripherals, switches and routers and storage should be patched according to the schedule below.

| Time | Action |
|---|---|
| Annually | • Check for new firmware updates. |

4.7.10 Telephone System

4.7.11 The telephone system should be patched according to the schedule below.

| Time | Action |
|---|---|
| Annually | • Apply important software updates. |

4.7.12 Application software and databases

4.7.13 Application software and databases should be patched according to the schedule below.

| Time | Action |
|---|---|
| Monthly | • Critical security patches reviewed and installed as required. |
| Quarterly | • Apply latest software patches. |

# 5. Enforcement

5.1 If any member of IT staff is found to have breached this policy, they may be subject to disciplinary action.

5.2 Users who systematically breach this policy by failing to allow the equipment that they use to be updated, may be subject to disciplinary action.

# 6. Definitions

6.1 The following patch management terms are used within this policy.

| | |
|---|---|
| Patch or fix | A release of software that includes bug fixes or performance-enhancing changes. |
| Security Patch | A broadly released fix for a specific product, addressing a security vulnerability. |
| Hotfix | A single package composed of one or more files used to address a problem in a product. |
| Driver | Software required by the operating system to make a piece of hardware function. |
| Service release or service pack | A release of software that bundles together several patches and/or updates to provide a clear benchmark or level of release (e.g. Service Pack 1). |
| Critical Update | A broadly released fix for a specific problem, addressing a critical, non-security related bug. |
| Update | A release of software that adds new functionality to an earlier version. |
| Version or build | Software that has a numeric or named attribute denoting its maturity or age (e.g Version 5.6.1). |