PATCH MANAGEMENT POLICY

Overview

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.

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
- Routers and switches
- Databases
- Storage

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 minimized and that the infrastructure is kept patched up to date.

2.3 All 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 This can be caused by viruses and malware exploiting systems or by out of date software and drivers making systems unstable.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 organization's IT infrastructure will be patched according to this policy to minimize vulnerabilities.

4.2. Identifying Patches to be applied

4.2.1 The organization's anti-virus server will be configured to automatically down load the latest virus and spyware definitions.

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

4.2.3 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.

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

4.2.5 Missing patches identified will be implemented as appropriate. Any weaknesses identified will be rectified.

4.2.6 Any system updates/patches for Linux operating systems must be done by the relevant service provider, tested and implemented.

4.2.7 For all updates on Linux operating systems, the Change control process must be followed, to ensure successful completion of update and minimize any problems that might occur.

4.3 Types of Patches

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

TYPE	PATCH
Server/ Computer	Drivers/ firmware
Operating system	Service packs
Application software	Service packs, feature packs
Routers and Switches	Firmware
Printers	Drivers, firmware
Scanners	Drivers, firmware
Anti-virus/ Anti spyware	Data file/ Virus definition update.