Information Technology Patch Management Policy

Document Information

Version Number	1.0
Last Update	15/10/2022
Author	Matthew Coutts
File Name	Information Technology Patch Management Policy
Document Title	Information Technology Patch Management Policy
Document Owner (Role Position)	Global Head of Enterprise Technology, Risk and Cyber Security
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Comments	Approved By
1.0	20/10/2022	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver
1.0	20/10/2022	20/10/2022	Matthew Coutts

1. Purpose

All employees performing roles of system or application administrators managing TEG ICT services and systems. This manual also applies to contractors, vendors and others managing TEG ICT services and systems.

2. Executive Summary

TEG is committed to and is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.

This manual defines the minimum required standards for the management of patch application for Company ICT resources.

Company System Administrators have an obligation to provide appropriate protection against malware threats, such as viruses, trojans, and worms, and software bugs which could adversely affect the security of a system, or the data stored or processed by the system.

Effective implementation of these minimum standards will help limit the Company's exposure to common malware threats, vulnerability exploitation, and the effects of software bugs.

3. Scope

This manual covers all computers, servers, systems, applications and network infrastructure owned or maintained by the Company, regardless of the location, and the administrators of all such systems and networks.

This manual is primarily aimed at System Administrators and technical staff, including IT Services staff, who are responsible for the ongoing maintenance of Company ICT services and systems.

This manual also extends, as far as practicable, to third parties who manage ICT services and systems on behalf of the Company, or who manage services and systems that are used to store or process Company information assets. The minimum standards defined in this manual should be included in any relevant supplier relationship agreements.

4. Patch Management

Patch Management Process

All Company owned or maintained computers, computer systems, computer networks and electronic communications devices must be updated with the latest stable patches released by the respective vendors.

The recommended process for patch management is:

- a System Administrator must be identified for the patch management of each system or device;

- those responsible for each system, device and application should monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities;
- where possible, a centralised and managed approach should be used to patch or update applications, drivers, operating systems and firmware;
- patches must obtained from a known, trusted source;
- patches must be tested and assessed in a non-production environment prior to promotion to a production environment;
- a backup of production systems must be performed before applying any patch;
- an audit trail of all changes must be created and documented;
- the System Administrator must verify that the patches have been installed successfully after production deployment.

Patch Application Targets

The following are the maximum timeframes within which a patch must be deployed once released by a vendor. The timeframes vary depending on the potential attack vectors and the potential business impact should the service become unavailable.

System or Device Type	Potential Business Impact				Compliance	
	Critical	High	Medium	Low	Target	Acceptable Level
Internet Facing	48 hours	14 days	30 days	90 days	100%	95%
Non-Internet Facing	7 days	30 days	60 days	90 days	100%	95%
Laptops / Desktops	7 days	30 days	60 days	90 days	100%	95%
Network Devices	Within 30 days			90 days	100%	95%

Category Definitions to be considered for Patch Deployment

Rating	Red Hat, Microsoft & Adobe Rating	Typical CVSS Score	Description
Critical	Critical	10	A vulnerability whose exploitation could allow code execution or complete system compromise without user interaction. These scenarios include self-propagating malware or unavoidable common use scenarios where code execution occurs without warnings or prompts. This could include browsing to a web page or opening an email or no action at all.
High	Important	7.0 – 9.9	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. This includes common use scenarios, where a system is compromised with warnings or prompts, regardless their provenance, quality or usability. Sequences of user actions that do not generate prompts or warnings are also covered.
Medium	Moderate	4.0 – 6.9	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations. The vulnerability is normally difficult to exploit.
Low	Low	<4.0	This classification applies to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.

Error Handling and Exception Handling

Error Handling

The System Administrator is responsible for identifying and rectifying failed patch deployments. Compliance with approved patches must be verified at least on a weekly basis.

Exception Handling

Systems and devices that are not patched via the centrally managed WSUS, SCCM or Satellite services must be updated as per the timeframes in the Patch Applications Target table above. Where this is not possible exceptions must be obtained from the CIO and appropriate compensating controls must be implemented to mitigate the risk. Failure to align with these minimum standards may result in the effected device or service being removed from the Company network.

Note: Exceptional cases may be considered including, but not limited to, where the impact of applying a patch (downtime etc.) is higher than the impact of not applying the patch, e.g. taking down a system running a compute job for a number of weeks. In such cases appropriate compensating controls must still be implemented until such time as the patch can be applied.

Patch Enforcement

Implementation and enforcement of these minimum standards is the responsibility of the System Administrator. The Information Security Team will conduct random external and internal vulnerability assessments to ensure compliance with these minimum standards without notice. Any system found in violation of these minimum standards shall require corrective action.

Cessation of Support

- Applications that are no longer supported by vendors with patches or updates for security vulnerabilities must be updated or replaced with vendor-supported versions.
- Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities must be updated or replaced with vendor-supported versions.

Roles and Responsibilities

<u>System Administrator:</u>

- the System Administrator is responsible for the operational management and protection of each system or device that is assigned to them; and specifically,
- System Administrators must test and deploy patches to each server, endpoint, network device, and application that falls within the scope of their management in accordance with the requirements of this Manual.

The Information Security Team are responsible for the following:

- routinely performing compliance checks with the minimum standards defined in this manual;
- providing guidance to all groups in issues of security and patch management; and
- ensuring that if patch application falls outside of the defined timeframes, that an incident is logged in the Company's IT Service Management tool for actioning.