Information security policy

Patching software

Version	Date	Who	What
DRAFT	October 2022	Gary Hinson	Template prepared for SecAware

Policy summary

Patching and updating software involves balancing the associated risks and costs, and protecting the organisation's interests through pre-release testing, backups and management authorisation.

Applicability

This policy applies throughout the organisation as part of the corporate governance framework. It is particularly relevant to IT professionals who normally install software patches and updates, plus those who manage and may need to patch or update various other IT systems (including **B**ring **Y**our **O**wn **D**evice, networking and embedded/process control systems) from time to time. This policy also applies to third-party employees working for the organisation whether they are explicitly bound (*e.g*. by contractual terms and conditions) or implicitly bound (*e.g*. by generally held standards of ethics and acceptable behaviour) to uphold our information security policies.

Policy detail

Background

When design flaws and bugs come to light in software, corresponding program changes are usually made by the developers to resolve the problems and are released either as patches (partial code modifications to existing programs) or new versions (generally complete replacement programs). Users of the relevant software choose whether and when to update/patch it, depending on whether they believe the advantages of resolving the flaws and bugs outweigh the costs and risks of changing installed software.

In the case of patches and updates addressing flaws and bugs representing information security vulnerabilities, the possibility of their being exploited typically increases from the time they are discovered until the installed software is patched or updated. However, patches and updates sometimes introduce further flaws, bugs and vulnerabilities, while changes *per se* are risky and costly: this can be important on servers and other IT systems supporting critical business activities. Striking the right balance between delaying the implementation until patches and updates are thoroughly tested, and expediting the implementation to resolve security vulnerabilities, is a risk management decision.

Policy axiom (guiding principle)

With guidance from information security, IT, risk and compliance professionals, the relevant Information Owners ultimately decide whether and when to implement software patches and updates in order to minimise overall risks and costs to the organisation.

Detailed policy requirements

1. Identifying the availability of relevant/applicable patches is a prerequisite for proper patch management. With support from Risk Management and IT, Information Security must maintain a watching brief on various information sources concerning software vulnerabilities, exploits and incidents, and the release of security-related patches.
2. As with other software installations and changes, the normal process for implementing patches involves assessing and testing the patches (including checksum verification, particularly for critical systems), management authorisation for their installation on target systems, and post-installation verification. The nature and extent of assessment, testing and verification should reflect factors such as the criticality of the software and the systems, and the trustworthiness of the organisations providing patches.
3. Delays inherent in the normal implementation process increase the likelihood that unpatched vulnerabilities may be exploited. The associated risks *may* therefore outweigh the advantages of testing and authorisation, hence an expedited patch/update installation process may be appropriate in some cases (*e.g*. routine antivirus signature updates, and security patches for exposed vulnerabilities that are being actively exploited in the wild).
4. Pre-installation backups are strongly advised in case unanticipated problems in the patching process require patches to be reverted (uninstalled). However, routine backups and patch uninstallation scripts *may* be sufficient on non-critical systems.
5. Except for critical systems and servers, the implementation of patches and updates should preferably be automated, for example using Microsoft Update and similar scripted installations requiring a minimum of user interaction on desktops, laptops, tablets and similar devices.
6. Corporate records of installed software should be updated promptly when patches or updates are installed.
7. Special arrangements may be necessary to patch systems that are only occasionally networked. If possible, such systems should be automatically scanned and if necessary quarantined when they attempt to connect to the network, pending their being patched to an acceptable level.
8. Special arrangements and additional controls may be required in the case of patches and updates to systems subject to compliance requirements, such as medical or other systems with health and safety implications, and accredited military systems. We must seek advice and permission from the relevant authorities *before* making changes.

Responsibilities

- **Information Security** owns and is responsible for maintaining this policy and advising generally on information security matters. Working in conjunction with other corporate functions (such as Risk Management, Legal/Compliance and Human Resources), Information Security Management is also responsible for ensuring that functions and people identified in this policy understand their obligations through suitable education, training and awareness activities.
- **Information Owners** are personally accountable for the protection and legitimate exploitation of 'their' information. They have a direct interest in information risk management decisions such as whether and when to deploy patches. They have the ultimate authority to sign-off or reject patches and other changes to IT systems processing 'their' information, acting on behalf of the business.
- **IT** is responsible for managing changes to the corporate and other managed IT systems, including patching.
- **Risk Management** and **Legal/Compliance** are responsible for providing professional advice and guidance in their respective areas of expertise, supplementing that provided by Information Security Management and IT.
- **Help Desk** is responsible for providing general support and advice in this area, liaising with relevant experts as necessary.
- **Workers** are personally accountable for compliance with applicable legal, regulatory and contractual obligations, and conformity with policies at all times.
- **Internal Audit** is authorised to assess conformity with this and other corporate policies at any time.

Further information

For general advice on information security, contact the Help Desk or browse the intranet *Security Zone*. Contact Information Security, IT or Risk Management for more specific advice and assistance.