Information Security Patch Management Manual

Section 1 - Audience

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

Section 2 - Executive Summary

(2) The University of Newcastle is committed to and is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.

(3) This manual defines the minimum required standards for the management of patch application for University ICT resources.

(4) University 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.

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

Section 3 - Scope

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

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

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

Section 4 - Patch Management

Patch Management Process

(9) All University 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.

(10) The recommended process for patch management is:

a. a System Administrator must be identified for the patch management of each system or device;
b. 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;
c. where possible, a centralised and managed approach should be used to patch or update applications, drivers, operating systems and firmware;
d. patches must obtained from a known, trusted source;
e. patches must be tested and assessed in a non-production environment prior to promotion to a production environment;
f. a backup of production systems must be performed before applying any patch;
g. an audit trail of all changes must be created and documented;
h. the System Administrator must verify that the patches have been installed successfully after production deployment; and
i. a Request for Change (RFC) ticket must be raised for all patch deployments. Refer to the Information Security Operations Management Manual further details on the Change Management Process.

Patch Application Targets

(11) 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.

See: Understanding Red Hat Security Ratings, Adobe Priority and Severity Rating Systems for Security Bulletins, Microsoft Security Updated Severity Rating System and National Vulnerability Database Vulnerability Metrics CVSS.

(12) Note: Systems that are locked down within segregated networks may be still be vulnerable to risks as they are classified above, but the likelihood of exploitation may be reduced. As such, the timeframe for patch deployment is longer as shown in the Patch Applications Target table above.

Error Handling and Exception Handling

Error Handling

(13) 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

(14) 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 University network.

(15) 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 months. In such cases appropriate compensating controls must still be implemented until such time as the patch can be applied.

Patch Enforcement

(16) 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.

Monitoring and Reporting

(17) All System Administrators responsible for the management of systems defined within the scope above are required to compile and maintain monthly reporting metrics that summarise the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk.

Cessation of Support

(18) Applications that are no longer supported by vendors with patches or updates for security vulnerabilities must be updated or replaced with vendor-supported versions.

(19) 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

(20) System Administrator:

a. the System Administrator is responsible for the operational management and protection of each system or device that is assigned to them; and
b. 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.

(21) The Information Security Team are responsible for the following:

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

Status and Details

Status	Historic
Effective Date	18th June 2019
Review Date	18th June 2021
Approval Authority	Chief Information Officer
Approval Date	17th June 2019
Expiry Date	17th January 2023
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Level of risk" - Magnitude of a risk or combination of risks, expressed in terms of the combination of their consequence and likelihood.

"ICT resources" - All information and communication technology resources and facilities.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.