Information Security Patch Management Procedure

Section 1 - Procedure

Audience

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

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) The IT Staff of the University have an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, worms and software bugs which could adversely affect the security of a system or the data entrusted on the system. Effective implementation of this procedure will limit the exposure and effect of common malware threats and vulnerability exploitation to the systems within this scope.

Scope

(4) This procedure covers all computers, servers, systems, applications and network infrastructure owned and maintained by the University, and the administrators of all such systems and networks.

(5) This procedure is primarily aimed at system administrators and technical staff, including IT Services staff who are responsible for the ongoing maintenance of ICT services and systems. The scope also extends to anyone else who is similarly undertaking activities governed by this procedure.

Patch Management Procedures

(6) All University owned and maintained computers, computer systems, computer networks and electronic communications devices must be updated with the latest but stable patches released by the respective vendors.

a. A system owner or team must be identified for the overall security management of each system or device.
b. Those responsible for each system, device and application must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.
c. Patches must obtained from a known, trusted source.
d. The integrity of patches must be verified through such means as comparisons of cryptographic hashes to ensure the patch obtained is the correct, unaltered patch.
e. Patches must be tested and assessed before implementation in a production environment to ensure that there is no negative impact as a result.
f. A backup of the production systems must be taken before applying any patch.
g. An audit trail of all changes must be created and documented. The System Owner must verify that the patches

have been installed successfully after production deployment.

h. Production patches must be deployed regularly as per the SLA defined below.

i. System Owners outside of IT Services that manage the security of their own systems are required to use patches in accordance with this procedure.

j. A Request for Change (RFC) ticket must be raised for all patch deployments including emergency updates, critical and operational updates.

k. Refer Information Security Operations Management Procedure for guidelines to be followed for Change Management Process.

SLA with Priority

(7) Patches must be deployed as per below mentioned category classification and SLAs from the time of the patch being released.

Device Type	Potential Business Impact				Compliance	
	Critical	High	Medium	Low	Target	Acceptable Level
Internet Facing	5 days	7 days	30 days	90 days	100%	95%
Non-Internet Facing	7 days	30 days	60 days	90 days	100%	95%
Laptops / Desktops	7 days	10 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 hte 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.

(8) 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 SLA for patch deployment is longer

as shown in the table above in SLA With Priority.

Error Handling and Exception Handling

Error Handling

(9) The System Owner or team is responsible for identifying and rectifying failed patch deployments. Compliance with approved patches must be verified at least on a weekly basis.

Exception Handling

(10) Systems and devices which are not patched via the centrally managed WSUS, SCCM or Satellite services must be updated as per the SLA With Priority as 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 this procedure may result in the effected device or service being removed from the University network.

(11) 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

(12) Implementation and enforcement of this procedure is the responsibility of System Owners. The IT Security Team will conduct random external and internal vulnerability assessments to ensure compliance with this procedure without notice. any system found in violation of this procedure shall require corrective action.

Monitoring and Reporting

(13) All System Owner and teams responsible for the administration 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.

Roles and Responsibilities

(14) System Owner or Team:

a. The System Owner or team is responsible for the overall security management of each system or device that is assigned to them.

(15) IT Security:

a. IT Security are responsible for the following:
    i. Routinely performing compliance checks with the patch management procedure;
    ii. Providing guidance to all groups in issues of security and patch management;
    iii. Ensuring that if something is not secure, it is included on the ICT agenda driving and documenting the status.

Status and Details

Status	Historic
Effective Date	31st March 2017
Review Date	1st July 2018
Approval Authority	Chief Information Officer
Approval Date	28th May 2018
Expiry Date	17th June 2019
Responsible Executive	Anthony Molinia Chief Digital & Information Officer +61 49138713
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"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.

"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.

"System Owner" - An authorised individual who has been allocated responsibility by the University and is held accountable for an ICT resource.