Maynooth University
National University
of Ireland Maynooth

Patch Management Policy v1.3

Policy Owner:	Information Security
Creation Date:	5th January 2021
Review Date:	N/A
Version:	1.3
Scope:	This policy applies to all systems and services owned and managed by Maynooth University.
Related Policies:	Information Security Policy
Consultation:	HEAnet ICT Security Services, IT Services, Computer Science, Electronic Engineering & Library
Approved by:	University Executive
Approval Date:	9th March 2020

Revision History

Version	Date	Comment
1.0	17.6.19	Original Release
1.1	28.01.20	Updated following additional consultation
1.2	02.03.20	Updated to reflect input from University Executive
1.3	05.01.21	Added ‘Approved by’ and ‘Approval Date’ following internal audit

Next Review Date: 2022

Table of Contents

1 Relevant Information

Maynooth University has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems onsite, offsite and inclusive of systems and services supplied by the third parties. Patch management is an area of systems management that involves acquiring, testing and installing multiple patches (software updates/code changes), to an administered computer system. The system administrator ensures that patches are installed properly, and all associated procedures are documented. Effective implementation of this policy reduces the likelihood of IT system compromise from a malicious threat actor or threat source.

2 Definitions

Vulnerability - Weakness in system or application that allows attackers or abusers to an take advantage and affect the system/application confidentiality, integrity or availability

Patch - Is a code or software update that covers/solves a certain vulnerability

IT Systems – Workstations, Servers (physical and virtual), System Components, Firmware, Networks (including hardwired, Wi-Fi, switches, routers, etc.), Mobile Devices, Hardware, Software (databases, platforms, etc.), Applications and cloud services.

3 Purpose of the Policy

This document describes the requirements for maintaining up-to-date operating systems security patches, software and firmware version levels on all the systems and services owned and managed by Maynooth University and on services provided by the third parties.

4 Scope of the Policy

This policy applies to:

- Workstations, servers, networks, hardware devices, software and applications owned and managed by the University. This includes third parties supporting Maynooth University's IT Systems.
- Systems that contain University data owned and managed by University's IT department.
- Third party suppliers of IT systems and services.

5 Policy

5.1 General

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the Maynooth University's network shall be regularly maintained by applying critical security patches within **thirty (30) days** after release by the vendor. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

5.2 System, Utility and Application Patching

A regular schedule shall be developed for security patching of all Maynooth University's systems and devices. Patching shall include updates to all operating systems as well as office productivity software, data base software, third party applications, and mobile devices under the direct management of Maynooth University's IT department.

Most vendors have automated patching procedures for their individual applications. There are a number of third party tools to assist in the patching process. Maynooth University's should make use of appropriate software management tools to support this process across its many different platforms and devices.

5.3 Patching Exceptions

Patches on production systems (e.g. servers, enterprise applications and systems in departments used for teaching purposes) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing. Deviations from normal patch schedules shall require Head of Department authorization.

System with a low risk factor (no university data, not connected to the Internet) can be dealt with on a best effort basis.

Systems with a high risk factor (contains university data and/or connected to the internet) must be patched as per this Patch Management Policy.

5.4 Patching Procedures

Procedures established and implemented for patch management shall be:

- Evaluated regularly;
- Documented and well understood by support staff;
- Automated and regularly monitored wherever possible; and
- Applied in a timely and orderly manner based on criticality and applicability of patches.

5.5 Document Management and Compliance

Maynooth University's change management and update procedures for IT Systems should include documented procedures and evidence of practice. To demonstrate compliance with this policy, Maynooth University needs to show it has taken all the necessary steps to secure the University's IT systems. This includes but is not limited to:

- Minutes of change management meetings relating to IT Systems
- Records of system updates and applied patches

6 Review and Reporting

The Policy will be reviewed and updated, on-going basis, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

7 Contact

Maynooth University Information Security Manager
Email: informationsecurity@mu.ie
Telephone: +353 1 708 6388