Vulnerability Management Policy

TU Dublin Policy on Vulnerability Management in IT systems.

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH

TU DUBLIN

TECHNOLOGICAL UNIVERSITY DUBLIN

Table of Contents

1. Document Control Summary

Area	Document Information
Author	Information Security Governance, Risk & Compliance
Owner	Chief Information Officer
UET Sponsor	*Dr Dympna O'Sullivan, Vice President, Research & Innovation*
Reference number	TSVMP2025
Version	1.0
Status	Approved
Pre-approval Body/Bodies	UET, ARC
Approved by	Governing Body
Approval date	18th February 2026
Next review date	18th February 2029
Document Classification	TU Dublin Public

2. Introduction / Context

In an increasingly complex and evolving cyber threat landscape, effective management of technical vulnerabilities is essential to the safeguarding of Technological University Dublin's (hereafter referred to as 'TU Dublin' or 'the University') digital infrastructure. The timely identification and remediation of software flaws, misconfigurations, and weaknesses are critical to protecting the confidentiality, integrity, and availability of university systems and data.

This policy establishes a structured approach to vulnerability and patch management, ensuring that known security weaknesses are addressed in a timely and consistent manner. It outlines the roles, responsibilities, and supports the procedures required to reduce the risk of exploitation, meet compliance requirements, and enable a secure operational environment across all TU Dublin IT assets—on-premises, cloud-based, and third-party managed.

3. Purpose

This policy defines TU Dublin's approach to the management of technical vulnerabilities and software patching across all systems and applications. Its purpose is to protect the confidentiality, integrity, and availability of TU Dublin's IT infrastructure by ensuring vulnerabilities are identified, assessed, and remediated in a structured and timely manner.

This **Vulnerability Management Policy** aligns with the following cyber security framework and controls:

National Institute of Standards and Technology Cybersecurity Framework 2.0

- Identify (ID)
  - Risk Assessment (ID.RA)
    - ID.RA-01
    - ID.RA-02
    - ID.RA-03
    - ID.RA-04
    - ID.RA-05
  - Improvement (ID.IM)
    - ID.IM-04
- Protect (PR)
  - Platform Security (PS)
    - PR.PS-02
- Detect (DE)

- Adverse Event Analysis (AE)
  - DE.AE-07

4. Scope

This policy applies to:

- All Information Technology assets (servers, desktops, laptops, mobile devices, applications, cloud services) owned, operated, or managed by TU Dublin.
- Systems connected to the TU Dublin network.
- Third-party providers and vendors with direct network access or providing managed services.
- Internally developed software and systems.

4.1 Roles and Responsibilities

The following roles and responsibilities apply in relation to this Policy:

Governing Body:
- To review and approve the policy on a periodic basis.

TU Dublin Executive and Management Teams:
- To review and approve the policy on a periodic basis.

TU Dublin Vice President of Research and Innovation:
- To ensure the policy is reviewed and approved by the Executive and Management Teams.

TU Dublin Chief Information Officer:
- To review and approve the contents of the policy.

TU Dublin Chief Information Security Officer:
- To oversee and manage the implementation of a successful vulnerability management and remediation program.

Technology Services Management:
- To define and implement standards and procedures which enforce the policy.
- To oversee, in conjunction with data owners, compliance with the policy and supporting standards and procedures.
- To enforce compliance with this policy where technically possible on TU Dublin systems.

Service Owner
- To conduct regular scans to identify vulnerabilities in systems, software and services under their control.
- To assess the risks associated with discovered vulnerabilities.
- To remediate vulnerabilities and reduce risks through patching or other controls in a timely manner.
- Communicate vulnerabilities, risks and mitigations with relevant stakeholders.

Staff/Students/Third Parties:
- To adhere to policy statements in this document.
- To report suspected breaches of policy to the TU Dublin IT Service Desk.

If you have any queries on the contents of this policy, please contact the IT Service Desk.

5. Definitions

Vulnerability: A weakness in a system or application that allows a malicious actor to take advantage of and affect a system or applications confidentiality, integrity, or availability.

Threat: Any circumstance or event that has the potential to exploit a vulnerability and cause harm to a system or organisation.

Risk: The potential for loss or damage when a threat exploits a vulnerability, typically measured by likelihood and impact.

Patch: A code or software update that resolves a specific vulnerability.

Exploit: A software program that takes advantage of a vulnerability or security flaw.

Third Parties: Third Parties are defined as any individual consultant, contractor, subcontractor, vendor, or agent not registered as a TU Dublin employee, or student but who will require access to specific elements of TU Dublin's IT infrastructure, and/or data.

6. Policy Details:

6.1 Policy Overview

This Vulnerability Management Policy defines TU Dublin's approach to managing technical vulnerabilities and applying software patches across systems, applications, and infrastructure.

The policy ensures that all known vulnerabilities — whether in operating systems, third-party software, or internally developed applications — are identified, assessed, prioritized, and remediated in a timely and controlled manner, based on their risk and severity.

The key objectives of this policy are to:

- Minimise the risk of security breaches caused by unpatched vulnerabilities.
- Ensure a consistent and structured process for vulnerability management.
- Establish clear responsibilities for patching and remediation activities.
- Define patching timeframes based on industry-standard CVSS severity ratings.
- Provide guidelines for handling exceptions where patching is not immediately feasible.
- Promote secure development and responsible vulnerability disclosure practices.

This policy is a critical component of TU Dublin's overall Information Security Framework and supports compliance with best practices and regulatory requirements.

The Chief Information Security Officer (CISO) has the ultimate responsibility for vulnerability management and remediation in TU Dublin.

6.2 Vulnerability Management

6.2.1 Vulnerability Assessment

TU Dublin is committed to proactively managing vulnerabilities across all information systems to protect institutional data and technology assets. The university adopts a structured vulnerability management approach encompassing the following key principles:

- **Asset Awareness:** All IT assets must be identified and maintained in an up-to-date inventory to support vulnerability management efforts.

- **Regular Assessment:** Systems must be regularly assessed for vulnerabilities using appropriate tools and threat intelligence from trusted sources.
- **Risk-Based Prioritization:** Identified vulnerabilities must be prioritized based on severity, potential impact, and business context using a risk-based approach.
- **Continuous Improvement:** Vulnerability management effectiveness must be reviewed through metrics, reporting, and ongoing improvement initiatives.
- **CVSS (Common Vulnerability Scoring System)**: A risk-based approach using CVSS scoring and business context is used to prioritize remediation. This is a standardized framework for rating the severity of vulnerabilities, ranging from 0.0 (None) to 10.0 (Critical).
- **Timely Remediation:** Vulnerabilities must be remediated within defined timeframes aligned with their severity as detailed in the table below. Where patching is not immediately feasible, appropriate compensating controls must be applied.

Severity Rating	CVSS Base Score	Remediation Schedule
Critical	9.0 -10.0	7 days
High	7.0 – 8.9	14 days
Medium	4.0 – 6.9	30 days
Low	0.1 – 3.9	90 days

- All critical TU Dublin IT assets and applications must be scanned for vulnerabilities and on a schedule appropriate for the risk profile of the assets or regulatory needs.
- Approved scanning tools must be used to conduct vulnerability scanning.
- Scans should be conducted after significant changes (e.g., new system deployment, patching, configuration changes).
- Newly deployed or significantly modified applications should be scanned prior to release.

6.2.2 Patch Management

- All managed systems must be kept up to date with security patches in accordance with remediation schedules.
- Automatic patching should be enabled where available to ensure timely automatic updates. All other systems must be patched in accordance with defined schedules.
- Standard patch windows should be defined and communicated, with procedures in place for expedited or emergency patching in response to active threats.
- Personal and unmanaged devices must maintain up-to-date operating systems and software to access university resources.

6.2.3 Exceptions to Patching

If patching cannot be completed within prescribed timeframes, the IT Exception process must be followed, including:

- Formal approval by the CISO or delegated authority.

- Documentation of alternative risk mitigations.
- Recording of exceptions in the risk register.

6.2.4 System Hardening

In addition to vulnerability mitigation practices, systems and applications must be hardened to reduce exposure. Hardening measures may include service restrictions, access controls, network isolation, conditional access and enhanced monitoring.

- All hardening actions must be documented and validated.
- All servers and systems must be hardened, patched, have relevant security applications and tools installed, before being used in a production environment.
- All server and systems must have a vulnerability assessment completed before being used in a production environment.

6.2.5 Software Development Vulnerability Management

Security vulnerabilities in applications developed by or on behalf of TU Dublin must be:

- Assessed promptly upon discovery or notification.
- Prioritized and remediated based on risk and impact.
- Tracked throughout the software development lifecycle.
- Addressed in accordance with secure development practices and frameworks.

6.2.6 Third-Party Vulnerability Disclosure

If TU Dublin identifies vulnerabilities in third-party software, the university will:

- Notify the vendor in a responsible and confidential manner.
- Allow reasonable time for resolution prior to any public disclosure.
- Ensure that all communications and actions align with responsible disclosure principles.

6.3 Monitoring

TU Dublin reserves the right to monitor all TU Dublin IT resources, information assets, content and data at all times.

TU Dublin reserves the right to log any required TU Dublin data, concerning systems access, including data relating to unauthorised access attempts which may warrant investigation.

TU Dublin may also log all changes made to TU Dublin systems and applications.

6.4 Violation of Policy

Contravention of TU Dublin policies may lead to the removal of access to TU Dublin services and resources and may lead to disciplinary action in accordance with the TU Dublin Staff Disciplinary Procedures or Student Disciplinary Procedures if applicable.

Users should report any suspected violations of this policy to the TU Dublin IT Service Desk. On receipt of any such notice, (or whereby the University otherwise becomes aware), of any suspected breaches of this procedure or its policies, the University reserves the right to suspend a user's access to the University's services and resources.

Where a valid business case exists exceptions to this policy may be approved by Technology Services in line with the IT Exception Policy.

6.5 Change Process

This policy will be reviewed every three years or after any change to TU Dublin applications, IT environment or business processes that would affect the application of this policy.

7. Related Documents

This policy should be read in conjunction with the following University policies, and users, and third parties should ensure compliance with these policies in addition to this policy:

- TU Dublin Penetration Testing Policy
- TU Dublin Data Protection Policy
- TU Dublin Acceptable Usage Policy
- TU Dublin Information Security Policy
- TU Dublin IT Exception Policy
- TU Dublin Data Classification Policy
- TU Dublin Remote Access Policy
- TU Dublin Cloud Services Policy
- TU Dublin Patch Management Procedure

The above is not an exhaustive list and other TU Dublin documents may also be relevant.

For further information on IT related queries please contact the IT Service Desk.

8. Conclusions

Effective vulnerability and patch management is essential to maintaining the security and resilience of TU Dublin's IT environment. By following this policy, TU Dublin ensures that technical vulnerabilities are identified, assessed, and remediated in a timely manner, reducing the risk of security incidents and protecting the University's information assets.

9. Appendix

10. Document Management

10.1 Version Control

VERSION NUMBER	VERSION DESCRIPTION / CHANGES MADE	AUTHOR	DATE
0.1	*Initial Draft*	*ISGRC*	*14/04/2025*
0.2	*Draft*	*ISGRC*	*27/04/2025*
0.3	*TSMT Review*	*ISGRC*	*08/05/2025*
0.4	*HEAnet Review*	*ISGRC*	*24/07/2025*
0.5	*Draft*	*ISGRC*	*12/08/2025*
0.6	*Addition of CISO repsonsibilites*	*ISGRC*	*03/02/2026*

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
0.5	*25th November 2025*	*UET*
0.6	*3rd February 2026*	*Audit &Risk Committee*
1.0	*18th February 2026*	*Governing Body*

10.3 Document Ownership

Accountability for defining, developing, monitoring and updating the content of this document rests with the Office of the Vice President of Research and Innovation.

10.4 Document Review

The Chief Information Officer is accountable for reviewing this document in consultation with relevant stakeholders. This document should be approved by the Vice President of Research and Innovation, the University Executive Team and Governing Body.

10.5 Document Storage

This document will be stored on the TU Dublin content management systems under the Policies and Forms media folder / Technology Services sub-folder. The file will be called: “TU-Dublin-Vulnerability-Management-PolicyTSVMP2025_v1.0.pdf” once released.

10.6 Document Classification

This document is classified as TU Dublin Public and is available to TU Dublin staff, students and third parties.