IT Penetration Testing Policy

TU Dublin Policy on IT Penetration Testing

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 Brendan Jennings, Vice President, Research & Innovation*
Reference number	TSITPTP2025
Version	1.0
Status	Approved
Pre-approval Body/Bodies	UET, ARC
Approved by	Governing Body
Approval date	15th October 2025
Next review date	15th October 2028
Document Classification	TU Dublin Public

2. Introduction / Context

As part of TU Dublin's commitment to safeguarding university data, technology assets, and critical infrastructure, this Penetration Testing Policy establishes the guidelines for performing controlled security assessments of university systems. Penetration testing, a proactive security measure, enables TU Dublin to identify and mitigate potential vulnerabilities within its networks, applications, and cloud services.

The primary goal of this policy is to protect the confidentiality, integrity, and availability of TU Dublin's IT resources by identifying weaknesses that could be exploited by malicious actors. By regularly assessing and fortifying our security defences, TU Dublin strives to create a safe and resilient digital environment for students, faculty, staff, and partners.

3. Purpose

This policy aims to define the cybersecurity requirements related to assessing and testing the effectiveness of the defence of Technological University Dublin's (hereafter referred to as "TU Dublin" or "the University") IT resources and systems by simulating real attack techniques and technologies, to discover unknown security weaknesses that might compromise TU Dublin.

This **Penetration Testing Policy** aligns with the following cyber security framework and controls:

National Institute of Standards and Technology Cybersecurity Framework 2.0

- Identify (ID)
  - Asset Management (ID.AM)
    - ID.AM-05
  - Risk Assessment (ID.RA)
    - ID.RA-01
    - ID.RA-02
    - ID.RA-03
    - ID.RA-04
    - ID.RA-05
    - ID.RA-06
    - ID.RA-07
  - Improvement (ID.IM)
    - ID.IM-02
    - ID.IM-04

4. Scope

This policy applies to all penetration testing activities conducted on the university's IT infrastructure, including but not limited to:

Network Infrastructure
- Internal and external network segments
- Wireless networks
- Firewalls, routers, and switches

Servers and Applications
- Web servers and applications

Endpoints
- Desktops and laptops
- Mobile devices
- IoT devices

Cloud Services
- Cloud-based applications and services
- Virtual machines and storage

Third-Party Services
- Vendor-provided services and applications
- Partner networks and systems

Physical Security
- Access control systems
- Surveillance 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.

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.

Chief Information Security Officer (CISO):
- To authorise penetration testing activities on TU Dublin IT resources and systems.

Business Owners:

- Responsible for planning, coordinating, and executing penetration tests.
- Responsible for providing access to software or systems being tested.
- Responsible for addressing identified vulnerabilities.
- To provide outputs of penetration tests to Information Security Governance Risk & Compliance.

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

Penetration Testing: A controlled, simulated cyberattack on a computer system performed to evaluate the security of the system.

Vulnerability: A weakness or flaw in software, hardware, or procedural controls that could be exploited by a malicious actor to compromise the confidentiality, integrity, or availability of a system.

Threat Actor: Any individual or group that poses a potential risk to an organization's digital assets or operations, including external hackers, malicious insiders, or automated threat mechanisms.

Remediation: The process of identifying and correcting security vulnerabilities and weaknesses to improve the resilience of an IT system.

Confidentiality, Integrity, Availability (CIA): Fundamental principles of information security.

- **Confidentiality:** ensures that information is accessible only to authorized individuals.
- **Integrity:** ensures that data is accurate and unaltered.
- **Availability:** ensures that systems and data are accessible when needed by authorized individuals.

6. Policy Details:

6.1 Policy Overview

The Penetration Testing Policy for TU Dublin outlines the requirements and responsibilities related to conducting controlled penetration tests on the University's IT infrastructure. This proactive approach enables TU Dublin to detect and address vulnerabilities that could pose a risk to the confidentiality, integrity, and availability of university resources.

The policy applies to all systems and applications owned, operated or utilised by TU Dublin and is integral to the University's broader cybersecurity strategy. The policy ensures that all penetration testing activities are conducted in a structured, secure, and ethical manner. This helps to protect TU Dublin from cyber threats while maintaining compliance with regulatory requirements and industry standards.

The objectives of a penetration test are to:

- Identify and document security vulnerabilities within the University's IT environment.
- Assess the potential impact of identified vulnerabilities.
- Provide actionable recommendations for remediation.
- Ensure compliance with relevant regulations and standards.
- Enhance the overall security posture of the university.

6.2 Policy Details

The following details establish the procedural guidelines, prerequisites, and approval requirements for conducting penetration tests within TU Dublin's technology ecosystem:

Authorization and Approval:

- All penetration testing activities on TU Dublin IT resources and systems must be authorized by the Chief Information Security Officer (CISO) or delegate.
- All penetration testing activities should be approved by the relevant business owner before commencement to minimise potential service disruption.
- If penetration testing has the potential to disrupt a production service, the proposed test should be submitted for assessment in line with the Technology Services Change Management Policy.
- Only qualified and approved third-party vendors or in-house security or infrastructure personnel are permitted to conduct penetration tests. These personnel must possess skills and competency required to perform the tests in a controlled manner.

Scope of Testing:

- Each penetration test must clearly define the scope, objectives, and boundaries to prevent unintentional disruptions or impacts to live operations. Scope documentation must include specific IP addresses, systems, or applications to be tested and any required exclusions or limitations.
- Third party service and software providers should conduct regular penetration testing on their services and provide the university with detailed reports.

Testing Methodologies:

- Penetration testing will follow standardized methodologies, such as those outlined by the Open Web Application Security Project (OWASP) or the National Institute of Standards and Technology (NIST).
- All penetration testing activities must comply with relevant laws and regulations including GDPR.
- A risk assessment should be conducted prior to penetration testing to identify potential impacts on operations.
- Testing activities will encompass various attack vectors, including vulnerability scanning, exploitation, and post-exploitation to assess the risk associated with any identified vulnerabilities. Vulnerabilities should be scored according to the Common Vulnerability Scoring System (CVSS).
- A communication plan should be established to inform relevant stakeholders before, during, and after penetration testing.

Confidentiality and Data Protection:

- Data gathered during penetration testing must be handled in accordance with TU Dublin's Data Protection Policy. All findings are to be stored securely, with access restricted to authorized personnel only.
- Sensitive data exposed during testing, whether intentionally or inadvertently, must be reported and remediated in compliance with TU Dublin policies.

Reporting and Remediation:

- At the conclusion of each test, a detailed report outlining discovered vulnerabilities, risk levels, and recommended mitigation actions will be provided to relevant stakeholders.
- It is the business owner's responsibility to action the recommended mitigation actions. Remediation actions should align with TU Dublin's Vulnerability Management Policy.
- Third party service and software providers should provide detailed remediation plans when vulnerabilities are identified in their systems.

Record-Keeping and Audit:

- Records of all penetration testing activities, including scope, findings, and remediation actions, will be retained for auditing and compliance purposes.
- Regular audits will be conducted to ensure that penetration tests are performed in compliance with this policy and that all identified vulnerabilities have been addressed effectively, including retesting and remediation validation activities.

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 are encouraged to report any suspected violations of this procedure 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.

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 Information Security Policy
- TU Dublin Acceptable Usage Policy
- TU Dublin Password Policy
- TU Dublin Data Protection Policy
- TU Dublin Remote Access Policy
- TU Dublin Cloud Services Policy
- TU Dublin Vulnerability Management Policy
- NIST Cybersecurity Framework (CSF) 2.0

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

The Penetration Testing Policy is a critical component of TU Dublin's commitment to safeguarding its digital infrastructure and sensitive information. By establishing a formal basis for identifying and addressing vulnerabilities. TU Dublin proactively reduces the risk of cybersecurity incidents that could impact the University's operations, reputation, and stakeholders.

This policy reinforces TU Dublin's dedication to maintaining the confidentiality, integrity, and availability of its IT resources and ensuring a safe digital environment for students, staff, faculty, and partners. Ongoing adherence to this policy, along with regular review and updates, will ensure that TU Dublin's cybersecurity practices remain robust, adaptive, and aligned with evolving industry standards and threats.

9. Appendix

10. Document Management

10.1 Version Control

VERSION NUMBER	VERSION DESCRIPTION / CHANGES MADE	AUTHOR	DATE
0.2	*Initial Draft*	*ISGRC*	*14/04/2025*
0.3	*TSMT Review*	*ISGRC*	*08/05/2025*
0.4	*HEAnet Review*	*ISGRC*	*21/05/2025*
0.5	*Draft*	*ISGRC*	*28/05/2025*

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
0.5	*10th June 2025*	*University Executive Team*
0.5	*30th September 2025*	*Audit & Risk Committee*
1.0	*15th October 2025*	*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 both 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-IT-Penetration-Testing-Policy-TSITPTP2025_v1.0.pdf" once released.

10.6 Document Classification

This document is classified as TU Dublin Public and is available to all.