

Technology Services Guideline: Physical Environment

1. Introduction

The protection of the physical environment is a critical component of Technological University Dublin's information security strategy. A lack of physical access control and security measures can undo the most careful technical precautions. Technological University Dublin is committed to ensuring the safety of its employees, contractors, and assets and takes the issue of physical security seriously. This guideline sets out the main activities and precautions that should be taken to enable a physical security regime.

This **Physical Environment Guideline** aligns with the following cyber security framework and controls:

National Institute of Standards and Technology Cybersecurity Framework 2.0

- Identity Management, Authentication, and Access Control (PR.AA)
 - PR.AA-06

2. Definitions

Physical Environment: Any physical space within the organization's premises, including offices, data centres, labs, and storage areas.

Assets: Physical and digital resources owned or managed by the organization, including equipment, data, and infrastructure.

3. Physical Environment Guidelines

This section outlines the key principles and standards for enabling a secure and safe physical environment from an information security perspective.

1. Access Control

- Implement access control measures such as key cards, biometric scanners, or security codes to restrict entry to sensitive areas.
- Maintain a log of individuals who access restricted areas and review access logs regularly.
- Ensure that visitors to sensitive areas are escorted by authorized personnel at all times.

2. Physical Security Measures

- An assessment of perimeter vulnerability should be conducted for all sensitive areas.
- A building should have appropriate control mechanisms in place for the classification of information and equipment that is stored within it.
- Surveillance cameras and alarm systems should be installed in critical areas to monitor and deter unauthorized access.
- Conduct regular security audits to identify and address vulnerabilities in the physical environment.
- Ensure that all security measures comply with relevant laws and regulations.

- Staff working in secure areas should confirm that all unknown persons present are authorized to access those areas.
- Keys to all secure areas housing IT equipment and lockable IT cabinets should be held centrally by an authorised authority.
- Where breaches occur, or an employee leaves, all identification and access tools/passes (e.g., badges, keys) should be recovered from the employee, and any door/access codes should be changed immediately.
- All general computer equipment should be located in suitable physical locations that limit the risk of theft.
- Computers handling sensitive data should be positioned to eliminate the risk of the data being seen by unauthorized people.
- All on premise servers should be located in Technological University Dublin data centres.
- Paper-based (or similar non-electronic) information in an open office should be protected by the controls for the building and via appropriate measures such as:
 - Filing cabinets that are locked with the keys stored away from the cabinet
 - Locked safes
 - Stored in a secure area protected by appropriate access controls

3. Environmental Controls

- Maintain appropriate environmental controls such as temperature, humidity, and air quality to protect sensitive equipment and data.
- Implement fire suppression systems and conduct regular fire drills to ensure preparedness in case of emergencies.
- Ensure that electrical and network infrastructure is properly maintained and protected from physical damage.
- Business-critical systems should be protected by an Uninterruptible Power Supply (UPS) to reduce the operating system and data corruption risk from power failures.
- Network cables should be protected by conduit and, where possible, avoid routes through public areas.

4. Asset Management

- Keep an inventory of all physical assets and conduct regular audits to ensure accuracy.
- Label and secure all equipment, especially those containing sensitive data.
- Implement procedures for the secure disposal of obsolete or damaged equipment.
- Procedures should be in place to ensure the inventory is updated as soon as assets are received or disposed of.
- All IT Assets should be securely marked and have a unique asset number allocated to it. This asset number should be recorded in the IT Asset inventory.

4. Summary

Protecting the physical environment is crucial for Technological University Dublin's information security. By following these guidelines, we ensure the safety of our employees, contractors, and assets. Regular audits, training, and adherence to procedures help maintain effective security measures. By following these guidelines, we can collectively contribute to a secure and resilient physical environment, safeguarding our valuable resources and supporting the overall mission of Technological University Dublin.

Document Control Summary

Area	Document Information
Author	Information Security Governance, Risk & Compliance
Status	Approved
Approved by	David Robinson – Chief Information Officer
Approval date	25 th April 2025
Document Classification	TU Dublin Public