PKCERT

National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Physical Security Controls

NTISB

A. INTRODUCTION

1. Pakistan Information security Framework 2025: **"Essential Physical Security Controls"**, outlines the baseline of physical security of information security system and infrastructure for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all organizational systems, networks, communication channels, and supporting technologies used to transmit, process, or store information. It covers employees, third parties, and any other entities with access to organizational systems, ensuring physical security of digital assets across the enterprise.

B. PHYSICAL SECURITY CONTROLS

3. Organizations shall define, document, approve, and implement cybersecurity requirements for the physical protection of information and technology assets.

4. The cybersecurity requirements for physical protection of information and technology assets shall include at least the following:

a) Authorized access to sensitive areas and assets within the organization (e.g., data center, sensitive information processing facilities, security surveillance center, network cabinets)

b) Implement robust facility access controls, monitoring, and surveillance, including entry/exit records, with secure storage and protection of access records.

c) Secure destruction and re-use of physical assets that hold classified information (including documents and storage media)

5. The organization shall establish controls to ensure that storage media used for Confidential or Secret information is removed or securely handled before devices are sent outside organization for repair.

PKCERT

Safeguarding Pakistan's Cyberspace

info@pkcert.gov.pk
www.pkcert.gov.pk