National Cyber Emergency Response Team
Government of Pakistan

Pakistan Information Security Framework (PISF) 2025

Essential Identity and Access Management Controls

A. INTRODUCTION

1. Pakistan Information Security Framework 2025: **"Essential Identity and Access Management (IAM) Controls"**, outlines the baseline of information security identity and access management controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework governs the management of all user, service, system, and privileged accounts across the organization's technology resources. It covers on-premises, cloud, and third-party environments, including processes for identity governance, lifecycle management, authentication, credential management, and authorization.

B. IDENTITY AND ACCESS MANAGEMENT

3. The organization shall define, document, approve, and implement identity governance processes to ensure accountability, compliance, and secure management of all identities.

4. The organization shall establish and enforce lifecycle processes for the creation, maintenance, and timely deprovisioning of user, service, and system accounts.

5. The organization shall enforce a centralized authentication framework with strong passwords, multi-factor and adaptive methods, supported by session management, monitoring, and standardized tools to ensure secure access aligned with system sensitivity and risk.

6. The organization shall enforce secure credential lifecycle management, including generation, storage, distribution, rotation, review, revocation, and disposal.

7. The organization shall ensure that user access rights are regularly reviewed and are promptly modified or revoked upon role change, transfer, or termination.

8. The organization shall enforce the principle of least privilege through defined access control models, ensuring that all access to systems and data is authorized strictly based on documented business need and formally approved.

9. The organization shall centrally manage all official social media accounts through clearly defined ownership, role-based access controls, and formal content approval processes.

C. PRIVILEGED ACCESS MANAGEMENT

10. The organization shall classify privileged accounts based on business impact and enforce strict governance through approval workflows, dedicated non-shared access, secure vaults, just-in-time elevation, and continuous session monitoring.

11. The organization shall ensure that emergency (break-glass) and third-party privileged access is granted only with enhanced authorization, is limited in duration, and is fully auditable, with privileged activities logged and monitored.

PKCERT

Safeguarding Pakistan's Cyberspace

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