National Cyber Emergency Response Team
Government of Pakistan

PKCERT

Pakistan Information Security Framework (PISF) 2025

Essential Incident Response Controls

A. INTRODUCTION

1. Pakistan Information security Framework 2025: **"Essential Incident Response Controls"**, outlines the baseline of information security incident response controls for federal and provincial government ministries, divisions and departments, autonomous bodies, corporations, CERTs and designated CIIs.

2. This framework applies to all organizational functions, systems, and processes involving sensitive data, across all internal and external environments. It establishes the foundation for preparing for, responding to, and recovering from security incidents and disruptions to protect national digital assets, organizational resilience, and public trust.

B. INCIDENT MANAGEMENT

3. The organization shall formulate cyber security incident management policy and procedure for the preparation, detection, response, mitigation, reporting, recovery, remediation and lessons learned.

4. The organization shall maintain classification of cybersecurity incidents based on severity and impact.

5. The organization shall manage incidents using an approved incident response framework that assigns clear ownership and accountability and ensures consistent handling across the incident lifecycle.

6. Organizations, other than service providers, shall perform a needs analysis and feasibility assessment to determine the establishment of a Security Operations Center (SOC) and/or the acquisition of SIEM or other relevant security monitoring solutions.

7. The organization shall maintain incident readiness through clear policies, adequate resources, and skilled teams.

8. The organization shall establish incident response roles and responsibilities, along with the corresponding authority and dependency levels.

9. The organization shall report cybersecurity incidents as follows:

   a) Critical infrastructure incidents: Initial reporting to sectoral regulators/CERTs and nCERT upon verification of incident followed by detailed reporting within 72 hours.

   b) All verified incidents for non-critical infrastructure shall be reported to sectoral regulators/CERTs within 120 hours.

10. The organization shall document incident lessons learned for each security incident and implement corrective actions within defined timelines to prevent recurrence.

C. BUSINESS CONTINUITY PLAN (BCP) (APPLICABLITY TO BE ASSESSED BY RELEVANT CYBER SECURITY STEERING COMMITTEE)

11. The Business Continuity Program shall be governed by appropriate entity designated by cyber security steering committee, with each department nominating a Continuity Focal Person to maintain plans and coordinate response efforts.

12. Based on an annual Business Impact Analysis (BIA) that categorizes critical functions and their interdependencies, the organization shall develop, approve, and implement a comprehensive business continuity plan addressing tiered recovery, backup or alternate sites, remote work arrangements, and supply chain resilience.

13. The organization shall establish and enforce approved recovery and response metrics (recovery time objective (RTO), Recovery Point

Objective (RPO), Mean time to detect (MTTD) and Mean time to response (MTTR)) for critical systems and services to ensure effective detection, response, recovery and minimal data loss consistent with business continuity and operational resilience objectives.

14. Invocation of BCP must follow documented procedure for damage assessment, communications, recovery and restoration with all activities logged.
15. The organization shall conduct annual simulations or exercises to test recovery capabilities, ensure compliance and build resilience with all tests evaluated against defined success criteria.

D. DISASTER RECOVERY PLAN (APPLICABLITY TO BE ASSESSED BY RELEVANT CYBER SECURITY STEERING COMMITTEE)

16. The Disaster Recovery Plan (DRP) shall be activated by the organization upon defined triggers like RTO and RPO.
17. Structured communication during a DR event shall be delivered to all stakeholders using formats and escalation routes aligned with the incident management and response plan, and all activities must be documented.

PKCERT

Safeguarding Pakistan's Cyberspace

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