RFC 2350 PROFILE

TLP: CLEAR

FEBRUARY 25, 2026

NATIONAL COMPUTER EMERGENCY RESPONSE TEAM OF PAKISTAN
L-Block, Pak Secretariat, Islamabad, Pakistan.

Table of Contents

1. Document Information

This document is published in accordance with **RFC 2350** to provide official information about the National Computer Emergency Response Team of Pakistan.

1.1 Document Title

RFC 2350 PROFILE

1.2 Date of Last Update

February 25, 2026

1.3 Document Status

Public

1.4 Location of This Document

This document can be found at https://pkcert.gov.pk/d/RFC2350.pdf

2. Contact Information

2.1 Name of the CSIRT

National Computer Emergency Response Team of Pakistan

2.2 Organization

National Computer Emergency Response Team, Ministry of Information Technology and Telecom, Cabinet Division, Government of Pakistan.

2.3 Mailing Address

National CERT
L-Block, Pak Secretariat
Islamabad 44000
Pakistan

2.4 Time Zone

Time Zone: UTC +05:00 (Pakistan Standard Time)
Time Zone DST: Not Observed

2.5 Telephone Numbers

Telephone: +92-51-111-162-378
Fax: +92-51-920-3412

2.6 Email Communication

For general correspondence: info@pkcert.gov.pk
For incident related or technical correspondence: cert@pkcert.gov.pk

2.7 Other Telecommunication

National CERT of Pakistan may be contacted via public channels, including:

LinkedIn Page: https://www.linkedin.com/company/national-cert-pakistan/

Facebook Page: https://www.facebook.com/pkncert

Instagram: https://www.instagram.com/pkcert_official/

2.8 Public Keys and Encryption

PGP key details are provided in section 4.3.

2.9 Operating Hours

Office Hours: Monday – Friday, 08:30 to 16:30 (PKT)
Incident Reporting and Response Hours: +92-51-111-162-378, 24x7, 365 days a year

2.10 Website Information

For obtaining further information about National CERT of Pakistan or reporting incidents, the official website can be found at: https://pkcert.gov.pk

3. Charter

3.1 Mission Statement

The mission of National CERT is to enhance the cybersecurity posture of Pakistan by serving as the national focal point for the prevention, detection, coordination, and response to cyber security incidents, while promoting trusted information sharing and international cooperation.

3.2 Constituency

National CERT constituency consists of underlying CERTs including Federal, Provincial, Government, sectoral, defense and organizational CERTs, public/private organizations and individuals that are designated under the National CERT in accordance with the applicable CERT Rules 2023 published by Government of Pakistan.

3.3 Sponsorship and /or Affiliations

National Computer Emergency Response Team of Pakistan is affiliated with Ministry of Information Technology and Telecom (MoITT), Government of Pakistan and National Telecommunication & Information Security Board (NTISB) under Federal Government of Pakistan.

National CERT is an Operational Member of APCERT.

3.4 Authority

National CERT (www.pkcert.gov.pk) is the National Computer Emergency Response Team under the Ministry of Information Technology and Telecom (MoITT).

The Government of Pakistan, through S.R.O. No. 376(I)/2024 dated 05 March 2024, designated the National Computer Emergency Response Team of Pakistan (National CERT) to provide ICT security services and continuously monitor cyber threats to national security under the “Cyber Security for Digital Pakistan” initiative [7330(2024) Ex. Gaz.]

4. Policies

4.1 Types of Incidents and Level of Support

The National CERT provides incident handling, analysis, and advisory support to its constituents. Incidents are managed through a structured tracking and ticketing system, ensuring a formal audit trail and progressive enrichment of information throughout the incident handling process.

Support is prioritized based on the severity and impact of incident, the affected constituent, the size of the user community and applicable legislative and regulatory frameworks. Cybersecurity incidents covering threats to human safety, critical infrastructure, large-scale service outages, and compromises of sensitive data, are handled on top priority while other incidents are addressed as per the breadth of the impact.

Where applicable, incident management is coordinated with the relevant sectoral CERTs of the affected constituency. All information sharing is conducted in accordance with national policies

and limited to the relevant purpose, ensuring confidentiality, privacy, and integrity throughout the response process.

National CERT responds to the incidents within the following target time frame based on the priority rating of the incident.

Priority	Target Response Time
P1 – High	6 Hours
P2 – Medium	24 Hours
P3 – Low	48 Hours

Target Response Time is the time taken by National CERT to provide first response after an incident is monitored or reported. Recovery times may vary depending on the volume and complexity of incidents.

A number of common incident types along with assigned priority ratings are listed in table below.

Priority	Type of Incident	Affected Sector	Impact Scope	Remarks
P1 – High	Ransomware attack on government systems	Federal/ Provincial Ministries, Critical Infrastructure (Power, Health, Finance)	National	Potential service disruption across multiple departments requires immediate containment, and national-level coordination
P1 – High	APT cyber attack	Defense, Government Communication Networks	National	Requires urgent threat intelligence sharing, cross-sector coordination, activation of emergency/crisis procedures
P1 – High	Compromise of National Digital Assets (CII)	Banking, Telecom, Power, Health	National	Full-scale incident response, data exfiltration prevention, mitigation directives issued
P1 – High	Large-scale data breach	Public sector organizations	Sectoral	Immediate response and coordination with SOCs of affected sector; notifications to stakeholders

P1 – High	Malware/virus outbreak in government network	Federal/Provincial Departments	Sectoral	Network isolation, malware removal, and vulnerability patching required
P2 – Medium	Phishing campaigns targeting government employees	Federal/Provincial Ministries, Public Sector Organizations	Sectoral	Awareness campaigns, email filtering, SOC monitoring, Rules updates
P2 – Medium	Unauthorized access attempts detected	Any government system	Sectoral	Log analysis, access control enforcement, patching
P2 – Medium	Defacement of public facing websites	Government/public websites	Sectoral	Restore site, perform forensic analysis, monitor for repeat attacks
P3 – Low	Missing patches/updates (non-critical)	Any sector	Sectoral	Coordinated patching and remediation; monitoring for exploitation

An incident type not listed in the above table shall initially be assigned a 'High' priority rating. This rating will remain in effect until the initial analysis of the incident is completed, after which the priority may be revised if required.

4.2 Co-operation, interaction and disclosure information

The National CERT cooperates with national and international CSIRTs, government entities, law enforcement agencies, service providers, and other relevant stakeholders to facilitate effective incident response and information sharing. All cooperation activities are conducted in accordance with national policies, legal requirements, and international best practices. Information shared during these interactions, is classified as per NCERT's information classification scheme. Accordingly, entity-level incident-related information is classified as 'CONFIDENTIAL' and is provided only to authorized parties, while non-sensitive or aggregated data that is used to develop advisories and other information intended for mass communication to broader audiences, is classified as 'PUBLIC'.

Information is shared on a need-to-know and best-effort basis, subject to applicable laws and regulations. National CERT follows the Traffic Light Protocol (TLP) for information handling to control the disclosure and redistribution of information.

4.3 Communication and Authentication

National CERT encourages encrypted communication for sensitive incident reporting. Following are details of National CERT's PGP key:

PGP Key ID: 53CE7031670000B1
PGP Key Fingerprint: B326677FA10AD35C18658C3753CE7031670000B1
PGP Public Key URL: https://pkcert.gov.pk/d/pgpkey.txt

4.4 Confidentiality and Data Protection

The National CERT ensures that all information received from reporters or stakeholders is handled securely and used solely for incident response, advisory, and mitigation purposes. All activities comply with national privacy laws and regulations, ensuring that personal and organizational data are protected and not disclosed without proper authorization.

Information is retained only for the duration necessary to manage incidents and fulfill legal obligations; disclosure to third parties is conducted strictly in accordance with national policies and international cooperation agreements.

5. Services

5.1 Incident Response (Triage, Coordination, and Resolution)

National CERT performs initial triage of reported incidents to assess validity, severity, and potential impact. Incidents are prioritized based on their assessed severity and impact.

National CERT coordinates incident response activities with relevant stakeholders, including affected organizations, service providers, and national or international CSIRTs, in accordance with applicable laws and confidentiality requirements.

National CERT provides support to its constituents with respect to organizational and technical aspects of reported incidents and assists them in incident containment, mitigation, and recovery.

5.2 Proactive Activities

These are activities aimed at preventing, mitigating, and preparing for incidents:

1. Developing security baselines, standards, best practices, and guidance for constituents. The relevant information is published on 'Knowledge Base' section of NCERT's official website.

2. Promoting education, awareness, and training programs for different audiences, including academia and research institutes. The relevant information is published on 'Advisories' and 'Capacity Building' sections of NCERT's official website.
3. Collaborating with industry partners and public/private organizations to promote innovation and local development of cybersecurity tools and solutions. The relevant information is published on 'CIE Partners' section of NCERT's official website.
4. Supporting audit and compliance through its Cybersecurity Auditing Firm Registration Program. The relevant information is published on 'Audit Firm Registration' section of NCERT's official website.
5. Operating national vulnerability disclosure program. The relevant information is published on 'Vulnerability Disclosure Program/Cyber Patriot Program' section of NCERT's official website.
6. Operating national cyber solutions registry to support and promote indigenous development of security tools. The relevant information is published on 'National Indigenous Cyber Solutions Registry (NICSR)'.
7. Supporting Sectoral CERTs, organizations, and institutions to develop their incident management capabilities, baselines, and benchmarking through joint exercises.
8. Providing predictive and fused cyber analysis based on situational awareness, trends, and vulnerabilities.

5.3 Responsive Activities

These are activities triggered after an incident is reported or detected:

1. Providing incident response, vulnerability, and artefact analysis, including forensic investigations.
2. Disseminating information about reported vulnerabilities and mitigation strategies to constituents, partners, and trusted collaborators.
3. Supporting incident reporting across a broad spectrum of sectors, including government, military, telecom, finance, and academia.
4. Operating automated systems to collect, correlate, analyze, and share computer and network security information.
5. Providing on-site incident response capability to federal-level constituents and law enforcement agencies.
6. Collaborating with national and international CERTs, forums, and expert groups for information sharing and coordinated response.
7. Responding to security incidents with coordinated monitoring, analysis, and mitigation, following established prioritization and severity criteria.

6. Incident Reporting

Organizations and individuals may report cybersecurity incidents to National CERT through any of the channels listed below:

Email: cert@pkcert.gov.pk

Incident Reporting Form: The Form is available here https://pkcert.gov.pk/report-incident.asp

Phone: +92-51-111-162-378

When reporting an incident, please include:

- Organization name and contact details
- Description of the incident and its impact
- Date and time of detection (with time zone)
- Affected systems and services
- Any supporting logs or evidence (if available)

7. Disclaimers

National CERT provides its services and information on a best-effort basis. Reasonable efforts are made to ensure accuracy and timely dissemination; however, National CERT does not guarantee the completeness or correctness of the information and shall not be held responsible for any direct or indirect loss arising from its use.

Users are advised to exercise due diligence when acting on the information provided.

The official website of NCERT may contain links to external sites not under NCERT's control; NCERT is not responsible for the content, availability, or reliability of such sites, nor does the inclusion of links imply endorsement.

8. Additional Information

This RFC 2350 document may be updated periodically. The latest version will be available on the official website of National CERT. For verification or international coordination, National CERT may be contacted through officially published channels only.