PKCERT

National Cyber Emergency Response Team
Government of Pakistan

National Vulnerability Disclosure Program

Contents

List of Acronyms / Abbreviations

Acronyms	Full Form
MTTR	Mean time to remediation
Cyber Patriot	A person who reports the vulnerability
VDP	Vulnerability Disclosure Program

1. Introduction

The critical role of cybersecurity researchers, ethical hackers, and responsible citizens in safeguarding the nation's digital infrastructure cannot be overemphasized. This National Vulnerability Disclosure Program establishes a standardized framework for the responsible reporting, coordination, and remediation of security vulnerabilities discovered in systems and services operated by federal and provincial government entities. The Program provides a safe, transparent, and legal channel for individuals and organizations to report vulnerabilities in good faith, thereby strengthening Pakistan's overall cybersecurity posture. This program establishes a formal process for reporting, validating, and remediating cybersecurity vulnerabilities.

2. Purpose

This Program aims to enhance national cyber resilience by establishing a transparent, coordinated process for vulnerability disclosure and management. It ensures security researchers, vendors, and government entities can safely report vulnerabilities while maintaining responsible disclosure practices.

- Facilitate responsible disclosure of cybersecurity vulnerabilities.
- Establish a trusted communication channel between researchers and government authorities.
- Define clear procedures and timelines for acknowledgment, validation, and remediation.
- Provide legal protection for good-faith cyber patriots.
- Enhance transparency, accountability, and national resilience against cyber threats.
- Indirectly enhance the cyber defensive posture of Pakistan.

3. Scope

This program covers all public-facing digital systems, services, and applications owned, operated, or managed by the public or private Sector of Pakistan including:

- Websites, citizen service portals, and online forms.
- Application Programming Interfaces (APIs) and mobile applications accessible via the Internet.
- Cloud-hosted services and web-based platforms.
- Internet-exposed email, DNS, and authentication services.
- Any other system or interface that can be directly reached over the public Internet.

The following are out of scope:

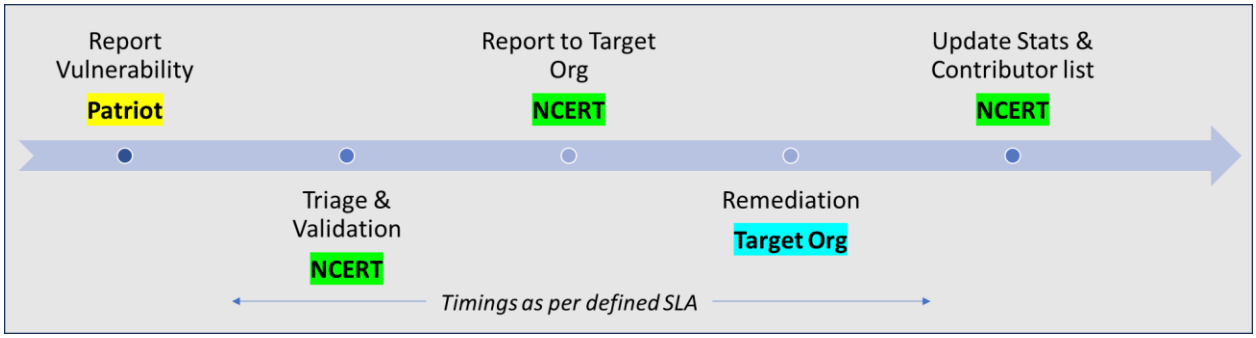
- Isolated or air-gapped systems.
- Social engineering attacks, spam, or physical intrusions.
- Denial-of-Service (DoS/DDoS) attacks.
- Vulnerabilities requiring social manipulation (e.g., phishing, pretexting).

4. Guiding Principles

The program is based on the following principles:

- Good Faith Engagement – Vulnerability reporting shall be conducted ethically and without intent to harm.
- Transparency and Accountability – Both parties shall communicate using defined communication channels.
- Timely Action – Reported vulnerabilities shall be addressed within defined SLA (Annex A).
- Legal Safe Harbor – Cyber Patriots participating in this program and adhering to the terms outlined in this document shall be granted protection from any legal action related to their good-faith vulnerability research and reporting activities.

5. The Work Flow



The figure illustrates the VDP workflow, as explained below.

5.1 Vulnerability Reporting

Cyber Patriots should report a vulnerability through the VDP Portal managed by National CERT Pakistan at https://pkcert.gov.pk/cyber-patriot-program.asp . All the necessary details as per the input form available at the VDP Portal, including affected system details, vulnerability description, reproduction steps, and contact information, must be filled. The Cyber Patriots who wish to stay anonymous can explicitly opt for it while submitting details through the VDP Portal.

Following must be kept in mind with regard to reporting:

- Reports must be clear, specific, and verifiable.
- Reporters should refrain from exploiting or altering any data.
- Vulnerability details are to be kept confidential until official disclosure.
- Vulnerability should be unique, and certification will be awarded to the first valid submission.

5.2. Triage & Validation

Upon receiving a vulnerability report, the National CERT shall issue an acknowledgment within the timeframe specified in SLA (Annex A). Each report will undergo an initial review to verify its authenticity, relevance, and compliance with the defined reporting scope. During the triage phase, the National CERT shall evaluate the report's quality, replicates the findings, and determines the potential impact of the vulnerability. If further technical details are required, the Cyber Patriot shall be contacted to provide clarification or additional evidence.

Once triage is complete, in the validation phase, a detailed technical and risk assessment shall be conducted to confirm the vulnerability's accuracy and severity. This process may include collaboration with the affected organization to ensure accurate validation and impact analysis. The validated vulnerability shall then be categorized by severity level as per SLA (Annex A), enabling timely coordination and prioritization of remediation actions.

5.3. Report to Target Organization

Report of confirmed vulnerability will be shared with the concerned target organization for remediation. Concerned Provincial CERT/ Sectoral CERT will also be kept in loop.

5.4. Remediation by Target Organization

The Target Organization will be responsible for remediating the vulnerability in SLA (Annex A). Necessary assistance and support will be provided by the concerned Provincial/ Sectoral CERTs, as deemed appropriate.

5.5. Statistics and Contributor List Update

After remediation, the status of the vulnerability will be updated in the vulnerability database as "Fixed", along with the relevant details. Moreover, the Cyber Patriot who reported the vulnerability will be included in the Contributor List, which is publicly available on the VDP Portal. The technical details of the vulnerability and the name of the Target Organization will not be publicly disclosed. Certificates will be issued to the cyber patriot.

6. Authorized Research & Safe Harbor

Cyber Patriots acting in good faith within the scope of this Program are authorized to identify and report vulnerabilities. Individuals acting in good faith and within the boundaries of this Program shall not be subject to criminal, civil, or regulatory action under applicable Pakistani laws, including the Prevention of Electronic Crimes Act (PECA) 2016, provided that:

- They do not cause harm, access unauthorized data, or disrupt services.
- They report discovered vulnerabilities directly and confidentially through the VDP Portal.

• They cease testing immediately after confirming the vulnerability.
• They do not publicly disclose the vulnerability.

7. Legal & Compliance

This Program complies with national cybersecurity legislation, data protection laws, and international standards for responsible vulnerability handling. Safe harbor applies only to research conducted within defined scope and in good faith.

8. Roles & Responsibilities

National CERT oversees Program implementation, vulnerability triage, and national coordination. Provincial/ Sectoral CERTs shall also be involved in validation and remediation processes, as needed. Target organization must apply timely patches and confirm to National CERT.

- Cyber Patriot: Submit vulnerabilities responsibly and confidentially, provide sufficient detail, and avoid exploitation or public disclosure at any stage.
- National CERT Pakistan: Manage the VDP portal, oversee submission triage, coordinate with relevant agencies, and maintain comprehensive records and performance metrics. Ensure effective communication with target organizations and continuous follow-up on remediation progress until closure.
- Provincial CERTs/ Sectoral CERTs: Provide necessary support and assistance to Target Organization in their jurisdiction, to remediate vulnerabilities and also keep National CERT informed.
- Target Organization: Validate, mitigate, and patch the reported vulnerability within defined SLA (Annex A), while keeping National CERT in the loop.

9. Transparency, Metrics & Governance

The National CERT shall ensure accountability and continuous improvement through transparent reporting and performance measurement. Annual transparency report (excluding the identification of target organizations and technical details of vulnerabilities) will include:

- Number of vulnerabilities reported and resolved.
- Average acknowledgment, validation, and resolution times.
- Recognized contributors and researchers.
- Systemic improvements achieved through the VDP process.

Performance metrics shall cover the total number of reports received, acknowledgment efficiency, validation accuracy, and mean time to remediation (MTTR). The National CERT will review the Program's effectiveness annually and issue necessary updates to maintain alignment with national cybersecurity objectives and evolving threat landscape.

10. Confidentiality and Data Protection

All submitted information shall be:

- Treated as confidential,
- Stored securely within government infrastructure, and
- Accessed only by authorized personnel for remediation purposes.
- Personal data of Cyber Patriots shall not be disclosed if explicitly requested.

Annex A – Service Level Agreements (SLAs)

The severity level of a vulnerability, when viewed from the National CERT perspective, is determined by its scope of impact across the national cybersecurity ecosystem, rather than the technical severity or local disruption it may cause to a single organization. While a vulnerability may be severe for an individual entity such as a complete network compromise, ransomware encryption, or a data breach, it is considered lower in severity for National CERT if its effects are confined within that organization and do not extend to other sectors, critical infrastructure, or government systems.

Conversely, when a vulnerability affects or threatens to affect multiple organizations within the same sector (for example, a coordinated phishing campaign across financial institutions or an outage impacting several healthcare providers), National CERT categorizes its impact as Medium. At Medium impact level, Provincial CERTs/ Sectoral CERTs coordinate the response, while National CERT maintains oversight to ensure containment and to evaluate cross-sector implications. Only vulnerabilities that transcend sectoral boundaries or have a potential national security or critical infrastructure impact are classified by National CERT as High and Critical.

Impact Category	Acknowledgement by NCERT	Triage/ Validation & Reporting by NCERT	Remediation by Target Organization
Critical	24 Hrs.	≤3 Days	≤7 days Provincial CERT/Sectoral CERT & National CERT in support.
High	48 Hrs.	≤5 days	≤15 days Provincial CERT/Sectoral CERT in support.
Medium	3 days	≤10 days	≤30 days
Low	7 days	≤15 days	≤60 to 90 days