REGISTERED No. M - 302 / L.-7646

The Gazette of Pakistan

EXTRAORDINARY
PUBLISHED BY AUTHORITY

ISLAMABAD, TUESDAY, OCTOBER 3, 2023

PART II

Statutory Notifications (S.R.O.)

GOVERNMENT OF PAKISTAN

MINISTRY OF INFORMATION TECHNOLOGY AND TELECOMMUNICATION

NOTIFICATION

Islamabad, the 26th September, 2023

S. R. O. 1394(I)/2023.—In exercise of the power conferred by section 51 read with section 49 of the Prevention of Electronic Crime Act, 2016 (XL of 2016), National Cyber Security Policy, 2021 the Federal Government is pleased to make the following rules, namely:—

CHAPTER-I

PRELIMINARY

1. **Short title, extent, and commencement.**—(1) These rules may be called the Computer Emergency Response Team Rules, 2023.

(2) These rules extend to the whole of Pakistan.

Price : Rs. 40.00

[1913(2023)/ Ex.Gaz.]

(3) These rules shall come into force on such date as the Federal Government may by notification in the Official Gazette appoint in this behalf.

2. Definitions.—(1) In these rules, unless there is anything repugnant in the subject or context,—

(i) "Act" means the Prevention of Electronic Crime Act, 2016 (XL of 2016);

(ii) "artefact" means a piece of data that may or may not be relevant to the response like event logs, files, timestamps;

(iii) "Critical Information Infrastructure" (CII) entails critical elements of infrastructure including but not limited to facilities, systems, networks or processes, information systems, programs or data of critical sectors under the constituencies of CERTs established under these rules;

(iv) "CII CERT" means a CERT responsible for ensuring the security and resilience of CII and responding on its own or assisting NCERT against any kind of cyber threats;

(v) "consequence" means the outcome of an event, being a loss, injury, disadvantage, or unlawful gain;

(vi) "computer security incident" means cyber security incident;

(vii) "critical information" means information, which is declared as critical by any authorized regulator or Government;

(viii) "constituency" means the group of users, sites, networks areas, or Organisations served by a team of a particular CERT;

(ix) "Computer Security Incident Response Team or Computer Emergency Response Team" CSIRT/CERT means one or more teams designated under these rules to respond to any threat against or attack any information system;

(x) "cyber security, data security or information security," means protecting information, data, system, network, infrastructure, and operational technology systems from unauthorized access, use, exposure, disruption, modification, destruction and unintentional or accidental damages.

(xi) "cyber security incident" means an occurrence that results in a real or suspected adverse event in relation to cyber security that violates applicable security policies laws, rules, regulations, directions, guidelines, or security procedures resulting in unauthorized access, unauthorized use of computer resources for processing and storage of information or any changes to data, denial of service or disruption, without authorization;

(xii) "defense CERT" means the CERT managed by the Ministry of Defense, Government of Pakistan;

(xiii) "Director General" means the Director General of the National Computer Emergency Response Team (i.e. National CERT);

(xiv) "functional entity" means an organisation with specific goals and objectives, led by an autonomous body and affiliated, registered, accredited or recognised by the respective regulatory authority;

(xv) "Federal CERT" means the CERT of which deals with Federal Government Division, Ministry, Department or Organisation;

(xvi) "Government CERT" means a CERT that deals with Federal and Provincial CERTs in a manner as prescribed by these rules or notified by MoITT from time to time;

(xvii) "ICT" means Information and Communication Technologies;

(xviii) "incident or event" means any occurrence that actually or imminently jeopardises, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

(xix) "MoITT" means Ministry of Information Technology and Telecommunication;

(xx) "National CERT" means a central entity which deals with all types of Federal, Provincial, sectoral, and defense CERTs in a manner as prescribed by these rules or notified by MoITT from time to time;

(xxi) "NCSP" means the National Cyber Security Policy, 2021 issued by the MoITT as amended from time to time;

(xxii) "Operational Technology Systems" means programmable systems that interact with the physical environment or devices;

(xxiii) "PECA" means the Prevention of Electronic Crime Act, 2016 (XL of 2016);

(xxiv) "Provincial CERT" means the CERT of each Province such as PUNJAB CERT, SINDH CERT, KYBER PAKHTUNKHWA CERT, BALOCHISTAN CERT or any other CERT;

(xxv) "Public Sector Entities (PSE)" means Division, Ministry, Department, Agency, Dependency, Institution and corporation fully or partially owned by the Federal or a Provincial Government;

(xxvi) "risk" means the chance or possibility of harm, injury, damage, or loss;

(xxvii) "risk assessment" means the process of evaluating and comparing the level of risk;

(xxviii) "risk management" for the purpose of these Rules means the application of a management system to risk and includes identification, analysis, treatment, and monitoring;

(xxix) "Sectoral CERT" means those CERTs that fall under Government CERT, CII CERT and Defense CERT;

(xxx) "Security Policy, Information Security Policy or Cyber Security Policy" means documented security processes for protecting information systems and cyberspace.

(xxxi) "SOC" means Security Operation Center established by CERTs or their constituencies under these rules;

(xxxii) "SOAR" means Security Orchestration Automated Response that will act as a part of and subordinate to SOC to provide a solution stack of compatible software programs to robotically collect data about security threats from multiple sources and respond to low-level security events; and (xxxiii) "vulnerability" means the existence of exploitable weakness in hardware or software of information systems that can result in adverse functioning other than the intended function.

(2) The words and expressions used in these Rules but not defined in these Rules shall have the same meanings as is assigned to them in the Act the Electronic Transactions Ordinance, 2002 Pakistan Telecommunication (Re-organization) Act, 1996 or any other relevant law.

CHAPTER-II

ESTABLISHMENT of CERTs

3. **Types of CERTs.**—CERTs shall be established across Pakistan in three tiers, as under:—

(a) **National Level:** The Central Entity along with its National Computer Emergency Response Team (nCERT) and National Security Operation Center (nSOC).

(b) **Sectoral Level:** Sectoral Regulator(s)/ CERTs (including but not limited to Defence, Telecom, Banking, Finance, Power, and Public sector).

(c) **Organizational Level:** Enterprises, entities, and individual users.

4. **CERT Council.**—(1) There shall be a CERT Council to be established through notification by MoITT which will work as a forum for consultative as well as advising all tiers of CERTs to ensure the effective performance of their roles and functions through assessments and conflict resolution, as assigned under these rules.

(2) The CERT Council shall seek nominations along with justification for establishing CERT from the National CERT, Government CERT, CII, Defence, and all other sectors and recommend to MoITT for approval of the Federal Government.

(3) The CERT Council shall have the following composition:

(i) Secretary, MoITT (Chairman);

(ii) one representative from the Ministry of Defense (Member);

(iii) one representative from the Ministry of Foreign Affairs (Member);

(iv) one representative from National Security Division (Member);

(v) one representative from the Ministry of Interior (Member);

(vi) one representative from Cabinet Division (Member);

(vii) one representative from Telecom Sector CERT (Member);

(viii) one representative from Defense Sector CERT (Member);

(ix) one representative of Government CERTs appointed by the MoITT from amongst the nominations from CERTs for two years (Member);

(x) one representative of Sectoral CERTs appointed by the MoITT from amongst the nominations from CERTs for two years (Member);

(xi) one representative from the Industry appointed by the MoITT for one year (Member);

(xii) one representative from academia appointed by the MoITT for one year (Member);

(xiii) one representative from civil society appointed by the MoITT for one year (Member); and

(xiv) Director General, National CERT (Secretary);

(4) CERT council may co-opt members either on a full-time or temporary basis to seek expert advice and consultation, after approval of the Chairman.

(5) The presence of at least fifty percent of the designated Members of Council (in person or by proxy) shall constitute a quorum at any meeting of Members, with the required presence of Secretary MoITT and a representative from the Ministry of Defence to vote on the issue presented before it.

(6) Chairman CERT Council may constitute sub-committees for different purposes, consultations, and projects as and when required.

5. National CERT.—(1) The National CERT shall be initially established as a project funded by MoITT and executed by a designated entity.

(2) National CERT will have the primary responsibility of coordinating between different CERTs to respond to threats or attacks on any CII systems or critical infrastructure data or widespread attacks on information systems in Pakistan.

(3) National CERT will deal with threats or attacks which could not be successfully responded to by the respective Sectoral CERT.

(4) National CERT will deal with a widespread attack on information systems in Pakistan which involves multiple sectors, including cyber terrorism and cyber warfare.

(5) National CERT shall function on a 24-hour basis on all days of the year including Government gazetted and other holidays.

(6) The contact details including the emergency helpline shall be published on its official website and will be updated regularly.

(7) National CERT shall establish its office in Islamabad and may establish its regional offices throughout Pakistan as and when deem necessary.

6. **Government CERT.**—(1) The Government CERT is responsible for ensuring cyber security and all matter ancillary thereto public sector at the Federal and Provincial levels.

(2) The constituency of the Government CERT includes the Federal and all the Provincial Government CERTs, therefore, it shall oversee and play a coordination role between the National and all Sectoral sectors falling under the Government CERTs.

(3) Government CERT will issue advisory to the Federal and all Provincial CERTs from time to time, not inconsistent with these rules.

(4) All Provincial and Federal CERTs will be under obligation to comply with the advisory of the Government CERT, therefore, will report to the National CERT through Government CERT.

(5) National CERT will serve as the Government CERT until an independent Government CERT is established by MoITT or the concerned Ministry to whom business is allocated.

7. **Critical Information Infrastructure (CII) CERT.**—(1) The CII CERT shall oversee and play a coordination role between the National CERT and various Sectoral CERTs falling under CII, which shall be designated as critical information infrastructure by the concerned Ministry or regulator to whom business is allocated.

(2) CII CERT will be responsible for ensuring security and all matters ancillary thereto CII of Pakistan.

(3) The constituency of CII CERT shall include all the Sectoral CERTs of the sectors designated as critical information infrastructure by the Federal Government.

(4) The concerned Ministry shall designate public or private infrastructure as critical infrastructure in accordance with relevant clauses of PECA and NCSP. The designated infrastructures shall be reviewed on annual basis. Additionally, any infrastructure can be declared CII, depending upon the sensitivity or criticality of the asset, facility, system, network, or process and the impact it has, in case of compromise.

(5) The National CERT may recommend to MoITT or the concerned Ministry to designate any public or private infrastructure as critical infrastructure to whom such business is allocated.

(6) The CII CERT shall develop grading criteria for the classification of public CII and will deal with them in accordance with the provisions of these rule, the Act or NCSP.

(7) The CII CERT shall play a coordinating and/or supporting role to handle security incidents of private sector-based CII Organisations.

(8) The National CERT will serve as a CII CERT until an independent CII CERT is established by MoITT or the concerned Ministry to whom business is allocated.

8. Sectoral CERT.—(1) The Government CERT and CII CERT will be sub-categorized into Sectoral CERTs consisting of the Federal and Provincial Government, Divisions, Ministries, Departments, Local Governments and organisations, regulatory bodies, and various industrial sectors like energy, transport, telecom, and broadcast, respectively.

(2) The Sectoral CERTs will report to the National CERTs through Government or CII CERTs in a manner prescribed by these rules.

(3) The Sectoral CERT is a sector-specific CERT responsible for responding to threats against or attacks on critical information, data, information systems, or infrastructure, or widespread attacks on information systems in its relevant sector.

(4) The constituency of a Sectoral CERT includes underlying functional entities affiliated/registered/accredited/recognised by the respective Government or sectoral regularity authority.

(5) The local government CERTs shall fall under the respective Provincial CERTs or as determined by the competent authority of the respective Provincial CERT.

(6) The Sectoral CERT shall maintain the list of its constituents and update/review the list as and when required.

9. Federal CERT.—(1) The Federal CERT will function as a Sectoral CERT, therefore, will report to the National CERT through Government CERT.

(2) The constituency of a Federal CERT includes the Federal Government subjects enumerated in the Federal Legislative list and other public sector bodies not limited to autonomous and semi-autonomous Organisations.

10. Provincial CERT.—(1) The Provincial CERT will function as a Sectoral CERT, therefore, will report to the National CERT through Government CERT.

(2) The constituency of a Provincial CERT includes provincial departments or authorities including but not limited to autonomous and semi-autonomous organisations under the administrative control of the Provincial Government.

(3) Provincial CERT will be responsible for ensuring the security of all digital assets developed, occupied, and deployed by relevant provincial public sector entities.

(4b) The Provincial Government may establish a new or designate an existing Public Sector Entity of the Province as a Provincial CERT which shall be duly notified by the Concerned Provincial Government.

CHAPTER-III

CERT WORKING MECHANISM

11. Functions of CERT.—In particular, and without prejudice to the generality CERT may have the following functions under the relevant area of work:

(a) **Proactive** functions such as:—

(i) collect Information on emerging, or new threats;

(ii) advanced threat analysis;

(iii) issuance of alerts, warnings, and situational awareness;

(iv) vulnerability management;

(v) conduct infrastructure security assessments;

(vi) provide guidelines on security configurations to CII;

(vii) coordination of cyber incidents response activities; and

(viii) any other function as assigned from time to time under these rules or required to cater to the matters falling under their role of responsibilities within the domains of cyber security.

(b) **Responsive** functions such as:—

(i) incident reporting;

(ii) incident response and recovery;

(iii) incident investigation, analysis and adequate remedial measures shall be taken;

(iv) Forensic and malware, analysis and take necessary steps;

(v) issuance of lessons learnt report to all concerned; and

(vi) any other function as assigned from time to time under these rules.

(c) **Sustenance** functions for its mandated objectives, functions, and services such as:—

(i) partnerships, MOUs, etc;

(ii) continual optimization;

(iii) technology development and implementation;

(iv) skill development, research, and training;

(v) security engineering;

(vi) process optimization and SOP refinement; and

(vii) any other function assigned from time to time under these rules.

12. Services provided by a CERT.—(1) Proactive Services: The CERT shall provide the following proactive services to its constituents to improve the infrastructure and security processes of constituents before any incident is detected or occurs. By providing proactive services, CERTs will help to avoid the incidents and reasonably minimize their negative impact:—

(a) **Announcements**: The CERT shall disseminate security-related information (advisories, guidelines, newly found vulnerabilities, etc.) among its constituencies. Such announcements shall be issued by email signed with an electronic signature or shall be shared via secure web portals or encrypted applications;

(b) **Technology Watch**: The CERT shall disseminate information on the latest trends, forecasts, R&D, high-potential inventions, and the potential impact on existing systems, as and when required;

(c) **Security Audits and Infrastructure Assessments:** The CERT shall conduct periodic security audits and infrastructure assessments to identify existing vulnerabilities in the infrastructure and shall recommend mitigation measures accordingly. The service will aim at establishing trust in ICT transactions, systems, and infrastructures;

(d) **Secure Configuration and Maintenance:** The CERT shall provide guidelines on security configuration to assist the constituencies in hardening their systems to minimize the attack surface and reduce the residual risk;

(e) **Development of Secure Solutions:** Indigenous security solutions will be developed, supported, or recommended by CERT to ensure protection against malware, possible threats, and vulnerabilities found in foreign or 3rd party products, as and when required. The CERT will also develop a vulnerability discovery platform for its internal use;

(f) **Intrusion Detection and Malware Analysis Services**: The CERT shall provide intrusion detection services upon request to help its constituents detect cyber hygiene, ongoing attacks, or intrusions and to initiate the incident handling process as soon as possible. The CERT will establish an expert malware analysis centre with advanced analysis capabilities; and

(g) **Inclusion of Academia:** The CERT will engage academia for its voluntary assistance and in this regards the Universities be encouraged to produce cyber security experts and the National/Provincial CERTs and CII should sponsor, the interns in this regard.

(2) **Responsive Services:** The CERT shall provide the following responsive services to its constituents to respond to requests for assistance from constituencies, reports of incidents, and tackling threats made or attacks against the systems.

(a) **Incident Management:** The CERT will provide support for incident handling, analysis, and response upon request, to its constituents through a tracking and ticketing system after defining Incident Scoring and Priority Levels During the incident handling phases, the ticket will be enriched with information, ensuring a formal audit trail and log of the incident. A joint team consisting of members of the National CERT and the sectoral CERT of affected constituents for incident management shall provide incident handling capability by monitoring, analysing, and responding to the incident;

(b) **Vulnerability Management:** The CERT will provide support for vulnerability handling, analysis, and response upon request, to its constituents after defining the vulnerability's severity Levels. A joint team consisting of members of the National CERT and the sectoral CERT, technical experts, and affected constituents for vulnerability management shall provide vulnerability handling capability by monitoring, analysing, and responding to the vulnerability; and

(c) **Artefact Handling**: The CERT will provide forensic artefact handling services upon request, to its constituents by conducting forensic analysis, reverse engineering, run time and comparative analysis, etc.

(3) **Security Quality Management**: The CERT will provide the following security quality management services to its constituents which consist of services that improve an organisation's overall security.

(a) **Risk Management**: The CERT will use knowledge of the environments and information collected via the responsive (incident, vulnerability, and artefact handling) and proactive (intrusion detection and security assessments) services to build a snapshot of situational awareness of the country as a whole and the individual constituency. This snapshot of overall risk will be used in the risk management process;

(b) **Business Continuity and Disaster Recovery**: The CERT will dispense requisite support in the cyber-security aspects of the business continuity and disaster recovery management processes to its constituents upon request;

(c) **Security Consulting**: The CERT shall provide security consultancy services to its constituents on its own and upon request;

(d) **Awareness Building**: The CERT will disseminate awareness materials and security advisories, and arrange seminars, conferences, and competitions at multiple levels for public awareness. The CERT will arrange Hackathons, Capture-The-Flag events, Cyber Drills, War Gaming, etc on annual basis;

(e) **Education/Training**: The CERT shall have qualified HR with cyber security training; or courses from globally recognized cyber security programmes or any other programmes as advised by the CERT Council. The CERT will offer short and long-term technical training programs leading to certifications and qualifications in various domains of information, communication, and cyber security on regular basis. The CERT will undertake training in a Cyber-range with the formulation of red and blue teams to simulate realistic environments;

(f) **Screening and Product Evaluation**: The CERT will conduct supply chain product screening and evaluation for its constituents on tools, applications, or other services to ensure the security of products under their use or being procured and their compliance with national or organizational standards and /or security best practices. The service will aim at establishing trust in ICT applications, products, systems, etc; and

(g) **Partnerships and Collaborations:** The CERT will establish and maintain partnerships, collaborations, and/or MoUs with relevant bodies, forums, and CERTs to improve the quality of services.

(4) **Service Monitoring:** The CERT will monitor service delivery (e.g. incident management, vulnerability management, artefact handling, etc.) to review the efficiency and effectiveness of its service. The CERT will identify, devise, and monitor the most important key performance indicators (KPI) to evaluate the quality and performance of services. The indicators will be relevant to the CERT's key mission objectives and weighted according to the importance of the services to which they relate. The CERT will also conduct an annual assessment of the Capability Maturity of its constituents as per the Capability Maturity Model as enumerated under Annex-A. Following is the non-exhaustive list of the most important KPIs for service delivery which will be used for statistical analysis as well as will be used for implementing appropriate actions for improvement.

(a) response times for service events e.g. incident, vulnerability report, or priority scheme, etc;

(b) level of information provided for service events (short-term);

(c) time-to-live for service events;

(d) level of information provided in the longer term (reports, summaries, announcements); and

(e) total time required to close the ticket (time to resolve an event).

13. Essential components of a CERT.—The CERT shall consist of four components called (i) Security Operations & Compliance Centre (ii) Coordination & Capacity Building Center (iii) Technology Development Team (iv) Supporting Labs.

(1) **Security Operation and Compliance Center**. The center will be established 24x7 to monitor the CII of constituents followed by a strict audit & compliance regime. The CERT team will deploy a SOC with state-of-the-art proactive and preventative defence in-depth cyber security measures. The Centre will provide its services in the following 2x domains:—

(a) **Governance, Risk and Compliances (GRC)**: The GRC service will include:—

(i) **Policy Regulations and Standards**: Development of policies, regulations, and standards at the National level in diverse domains of information, telecom, and Cyber Security with the support of subject matter experts in relevant domains.

(ii) **Risk Management**: It shall conduct information security risk analysis activities for existing and new systems, and business processes and evaluate the threats and attacks against constituent assets and systems; and

(iii) **Audit & Compliance**: 'Audit Framework' will be developed which will provide guidelines against which the designated audit teams will conduct organizational infrastructure audits. The respective frameworks will also serve as respective baselines against which the constituents will be assessed.

(b) **Operations & Monitoring**: The services will develop a resilient National Cyber posture by adopting a mechanism to monitor ongoing threats to Pakistan's Digital Landscape. Operations & Monitoring will include:—

(i) **Incident Management**: Receiving, triaging, and responding to requests and reports and analyzing reported incidents and events. SOC Center will use the results of vulnerability and artefact analysis to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. The findings of the activity will be shared with "the Coordination Center" which will correlate activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Perform vulnerability scanning of Cyber Space to identify risks.

(ii) **Security Operations & Orchestration**: A state-of-the-art SOC will be established on a 24x7 basis to monitor constituencies and CIIs through coordination and interfacing with their relevant CERTs. SOAR will also be part of SOC which will provide a solution stack of compatible software programs that will be used to collect data about security threats from multiple sources and respond to low-level security events without human assistance. Major functions will include:—

(1) alerts and warnings;

(2) Security Information and Event Management (SIEM) for event collection, normalization, and correlation activities;

(3) honeynets lure in attackers and study attack vectors before they can materialize threats against network resources;

(4) for Vulnerability Handling and Analysis, vulnerability assessment tools will help the SOC team in finding vulnerabilities for further security analysis;

(5) exploitation framework to be used by SOC offensive team to perform penetration testing and aid in IDS signature development.

(6) application security tools to scan security vulnerabilities in applications. This information will be shared with software development teams to remediate the vulnerabilities; and

(7) a low-maintenance auto-discovering network monitoring platform supporting a wide range of device types, platforms, and operating systems

including Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp, etc.

(c) **Cyber Threat Intelligence:** A cyber threat intelligence system shall be established to monitor the cyber security hygiene of affiliated constituents and keep CERT updated with situation awareness of our cyber frontiers. The service, upon request, will also be provided to desiring constituencies subject to technical, operational, and administrative grounds. Said system will also perform the following functions, both onsite and offsite, for constituencies and critical network infrastructure owners:—

(i) to address malware and worm detection, anomalies in egress and ingress traffic, and hygiene of the *.gov.pk domains, government departments, and critical network infrastructure owners will share important gateway traffic-related details e.g. Traffic Type, capacity, bandwidth, congestion, etc. with the CERT for early detection and situational awareness with respective CERTs. In this regard, the following essential details from session data will be shared by participating agencies:—

(1) autonomous system number (ASN)

(2) ICMP type and code

(3) packet length

(4) protocol

(5) sensor identification and connection status (location of the source of the data)

(6) source and destination IP

(7) source and destination port

(8) TCP flag information

(9) timestamp and duration information

(10) any additional information to find anomalies

(ii) in the next phase, the participating constituency will share statistics and malicious content, activity, alerts, etc. received from deployed (whether on-premises or cloud or hybrid, etc.) security mechanisms within six months of joining the program;

(iii) data received will be securely retained for at least three years until and unless it is allowed for further retention or earlier erasing on a case-to-case basis and will be destroyed after approval from a competent authority. Statistical results, analysis, studies, alerts, etc. generated from the received data will however be retained as per the internal policy of CERT;

(iv) the CERT will notify or share only specific results from the data shared by specific constituent stakeholders and constituencies. Generalized notifications, alerts, announcements, etc. will only be publicized after stripping any information that may attribute data to contributing constituency;

(v) for the provision of advanced detection and prevention services following capabilities will be added as per timelines to be defined by the CERT after taking the viewpoint of constituencies as well as taking stock of current cyber hygiene:—

(1) active and passive network traffic analysis and scan for possible intrusions;

(2) monitor, analyze, correlate and escalate network Intrusion Events;

(3) develop appropriate responses; protect, detect, respond; and

(4) conduct incident management and forensic investigation.

(vi) the solution will assist in NOC and SOC monitoring, resultantly, CERT will have an organized mechanism to pro-actively defend its constituents against incidents and intrusions, regardless of source, time of day, or attack type; and

(vii) establish a process for building and managing a catalogue of known exploited vulnerabilities within a certain timeframe (e.g., 30 days, 2 weeks, etc.).

(2) **Coordination & Capacity Building Centre.**—

(a) **Coordination Centre**: The Coordination Centre will be the focal point of contact for other CERTs (Government CERT, CII CERT, Federal, provincial, and other Sectoral CERTs) and the Capacity Building Centre for respective constituents. The Centre will have the following functions to perform and services to provide:—

(i) **Vulnerability Discovery and Management:** A Vulnerability Disclosure Program (VDP) will be established that will perform the following functions related to Cyber Threat Intelligence/Vulnerability Management.

(1) Develop, maintain, and operate a Vulnerability Disclosure Platform;

(2) Assess and advise mitigation activities (in collaboration with provincial/sectoral CERTs) and monitor ongoing threats.

(3) Gather Cyber Threat Intelligence about threats and threat actors from different data sources deployed/ functional at (public, private, defence, and other sectors and advise implementation of Security Information and Event Management (SIEM) & Security Orchestration, Automation, and Response Centre (SOARC) at constituent's level). The information gathered from these sources will be used to mitigate cyber-attacks.

(4) Vulnerability management including Triage Route and Track Vulnerability Reports.

(ii) **Hardware/Software Assessment (Whitelisting):** This service will assist constituents of the CERT in the procurement and acquisition of software and hardware that are security tested for CERT Supporting Labs (Forensics & Screening) and subsequently approved by the Coordination Centre. Designated teams will also formulate hardening guidelines for hardware and software before deployment; and

(iii) **Coordination and Liaison with National/ International Agencies**: This service will coordinate with sectoral and international CERTs as well as with other agencies to leverage expertise in the field of cyber security and liaise on matters that could affect Cyber security.

(b) **Capacity Building Centre**: The Capacity Building Centre will run a Cyber Security training and awareness program through the implementation of a National Cyber Security Strategy, the provision of Analytic and Planning Support data, establishing liaison with Academia and Research Institutes, Public-Private/ International Agencies-partnerships and publications of Research and whitepapers. The Centre will provide services to constituents of CERT through the following sub-sections:—

(i) **Development of Virtual Training Environment:** VTE setup will be established for capacity building along with a Digital Repository of Digital Assets and their Owners at the National level;

(ii) **Training and Awareness Programmes**: Each will liaison with Academia and Research Institutes and build Public-Private/International Agencies-partnerships for information security, capacity-building training/certifications, and Cyber Security awareness programmes; and

(iii) **Advisories**: Information Dissemination. The centre will immediately disseminate cyber alerts on various identified Cyber Security risks followed by detailed advisories and white papers for dissemination to constituents of CERT.

(3) **Technology Development Team:** The team will focus on researching Advanced Persistent Threats (APTs), Nation State Actors, and the Tools, Techniques, and Procedures (TTP) employed by various adversaries. The team will develop a collection of synchronized, real-time capabilities, to discover, define, analyse, and mitigate cyber threats and vulnerabilities. These capabilities will enable the Cyber Incident Response team to disrupt and neutralize cyber-attacks as they occur more readily. The team may also support the conduct of capture-the-flag competitions.

(4) **Supporting Labs.** The functions and services of CERT will be supported by Forensics Lab and Screening & Evaluation Lab. The Forensics lab will provide and extend 24x7 support to the Incident Management team. The Screening & Evaluation Lab will conduct screening and evaluations of Hardware and Software before their procurement and/or deployment and/or operationalization of systems at the constituent's premises. These services will be provided as per relevant certification programmes or standards that are applied by the CERT or relevant authorities. Details of services of both labs are as under:—

(i) **Digital Forensics Lab**: Digital Forensics Lab will perform the collection, preservation, documentation, and analysis of evidence from a compromised system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents provide a provable chain of custody that is admissible in a court of law under the rules of evidence. Relevant staff performing this function may also have to be prepared to act as expert witnesses in court proceedings as per PECA 2016. Forensics Lab will be capable to perform forensics analysis on all types of devices and equipment including networks (firewalls, switches, routers, gateway devices, data leakage prevention, etc.), Systems (OS, platforms, etc.), Applications (desktop, iOS, Android, etc.), Hardware (PC, Servers, Smartphones, USBs, data storage, etc.), IoT and other such devices; and

(ii) **Screening and Evaluation Lab**: Such setup will screen information systems from bugs, malware, hardware implants etc. Based upon the criticality and sensitivity of the information system to be decided by respective CERTs on their risk-based approach, the screening & evaluation lab will conduct supply chain product screening and evaluation on equipment, tools, applications, or other services to ensure the security of the IT and IT security and/or sector-specific products and their conformance to the national or organizational standard and /or security best practices. Tools and applications reviewed can be open source, locally or foreign vendor-developed, or third-party commercial products.

14. **Support Infrastructure.**—(1) The competent authority of respective CERTs shall ensure that the following parameters are in place and infrastructural support is established to allow CERT to fulfil its mandate, roles, and responsibilities:

(a) financial Support by allocating appropriate funds to the relevant budget head;

(b) human resources by hiring industrial professionals having relevant expertise. HR employed for CERT will be security-wise cleared at the time of hiring and with regular security clearances of employees conducted every two years through to applicable rules & regulations;

(c) support of administrative infrastructure shall be provided in the form of transport, appropriate office premises, and other required utilities;

(d) hardware support infrastructure shall be provided in the form of IT systems, management systems, lab infrastructure, coordination support systems, and all such tools and techniques that may be deemed essential for the delivery of its functions and services along with its regular updates and patch management mechanism;

(e) software support infrastructure shall be provided in the form of necessary operating systems, purpose-specific applications, security assessment tools, forensic applications, and all such tools and techniques that may be deemed essential for the delivery of its functions and services along with its regular updates and patch management mechanism;

(f) communication support infrastructure in the form of high bandwidth internet connections, point-point links, enterprise-level links, connectivity with its constituents for situational awareness and intrusion detection, connectivity with ISPs, IXPs, Telecom Operators, CII, etc. All such connectivity and communication links may be deemed essential for the delivery of its functions and services along with its regular updates and patch management mechanism; and

(g) any other aspect deemed essential.

CHAPTER- IV
NATIONAL CERT

15. **Functions and Services of National CERT.**—(1) The National CERT may adopt the same structure as CERT to offer a full range of functions and services as discussed in Chapter III.

(2) The National CERT shall act as a National coordination body and will provide a full range of its services upon request.

(3) The initial baseline capability criteria shall be developed by respective CERT teams and will be finalized and updated as per National CERT's recommendations.

(4) The National CERT shall establish necessary information and cyber security infrastructure through physical separation between highly sensitive systems dealing with critical infrastructure and through logical separation between other such systems. Confidentiality, Integrity, and Availability of infrastructure, communications, and operations along with stringent access control and authorisation protocols on a need-to-know basis will be ensured.

(5) Other than the Sectoral CERT, the National CERT will provide a subset of its services to the following stakeholders upon request:—

(a) individuals and home users

(b) intermediaries, organisations, companies, SMEs, etc

(c) internet and Domain Service Providers (ISPs), telecom service and other service providers etc

(d) third-Party vendors of IT & ITSec products and services

(e) academia, Research, and Development Organisations

(f) international CERTs, Forums, and expert groups

16. **Responsibilities of the National CERT.**—(1) Develop a national infrastructure for coordinating a response to any threat against or attack on any critical infrastructure, information systems, critical infrastructure data, or widespread attack on information systems in Pakistan.

(2) Develop a capability to support incident reporting across a broad spectrum of constituencies and sectors within Pakistan including government, military, critical services and infrastructures, telecommunication, commercial, academic, banking, finance, etc.

(3) Provide incident response, vulnerability, and artefact analysis, infrastructure security assessments, forensic investigations, law enforcement investigations, system screening, product evaluations, and all related activities.

(4) Disseminate information about reported vulnerabilities and share relevant mitigation strategies with appropriate constituents, partners, stakeholders, and other trusted collaborators through a national-level cyber alert system.

(5) Provide an automated process for collecting, correlating, analysing, and sharing a computer and network security information across the Federal Government and important constituencies.

(6) Provide on-site incident response capability to federal-level constituents and support federal law enforcement and investigation agencies.

(7) Provide fused, current, and predictive cyber analysis based on situational awareness of cyber hygiene and reporting of security incidents.

(8) Help Sectoral CERTs, organisations, and institutions within Pakistan to develop their incident management capabilities, baselines, and benchmarking methods.

(9) Develop and publish security standards, security best practices, and guidance in information, communication, and cyber security domains.

(10) Promote or undertake the development of education, awareness, and training materials and programs appropriate for a variety of different audiences, academia, and research institutes.

(11) Collaborate with other CERTs and international forums and bodies for information sharing, participation in cyber drills, and support for cyber/computer security incidents.

(12) Identify and maintain a repository of CSIRT capabilities and points of contact within Pakistan.

(13) Establish an integrated risk management process for identifying and prioritizing protective measures regarding cyber-security.

(14) Work towards adopting a coherent approach for embedding cybersecurity as an integral part of government policies across all domains to tackle vertical domains of cybersecurity.

(15) Such other functions and objectives relating to cyber security may be assigned to the National CERT from time to time.

17. **Cooperation and Coordination.**—(1) The National CERT shall begin cross-border cooperation for multilateral engagements such as association with regional CERTs including Asia Pacific Computer Emergency Response Team (APCERT), Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT), and membership with global entities Forum of Incident Response and Security Teams (FIRST), etc.

(2) Other sectors for establishing liaison are:

(a) organisations within and outside Pakistan engaged in specific areas in protecting and responding to cyber security incidents;

(b) investigation, enforcement, security, intelligence, and forensics organisations;

(c) academia, industry, service providers, and research and development institutions; and

(d) policymakers for cyber-security aspects of the business continuity and disaster recovery management processes for critical information infrastructures.

18. **Critical Information Infrastructure (CII).**—(1) The National CERT will recommend the designation of public or private infrastructure as critical infrastructure to the relevant authority, as and when required.

(2) The National CERT shall develop a grading criterion for the classification of public CII and will provide the services according to the obtained ranking of CII.

(3) The National CERT shall play a coordinating and/or supporting role for private sector-based CII organisations which have their infrastructure for handling security incidents.

19. **Compliance with the National CERT.**—(1) The National CERT may call for information and give direction to Public Sector Entities (PSE), service providers, intermediaries, data centres, private organisations, and any other persons/organisations deemed necessary through Sectoral CERT.

(2) The National CERT may develop an information sharing and aggregation framework, and issue associated SOPs/advisories for compliance from Government. CERT/CII CERT and Sectoral CERTs.

(3) The Government CERT/CII CERT and Sectoral CERTs shall seek compliance from their respective constituency with the SoPs, advisories, and directives issued by the National CERTs.

CHAPTER-V

SECTORAL CERTs

20. **Responsibilities of Sectoral CERT.**—(1) The Sectoral CERT will collect, and compile required information from its constituents and will share related information with the National CERT to issue a non-compliance report bi-annually for the information of The Prime Minister of Pakistan.

(2) The Sectoral CERT shall establish a SOC as a mandatory component of the CERT, with state-of-the-art proactive and preventative defence-in-depth cyber security measures, to monitor and interface with their underlying respective functional entities/organisations/licensees.

(3) The Sectoral CERT may take initiatives regarding the capacity building of its cyber security staff and may issue associated SOPs/advisories to their underlying respective functional entities/organisations/licensees.

(4) The Competent Authority of the respective Sectoral CERT will be responsible for ensuring compliance (Rule 19) with the -National CERT SOPs/advisories.

(5) Before launching a CERT by any organization, 5 members of the organisation must attend the CERT course / training from the authorised training provider.

21. **Functions and Services of Sectoral CERT.**—(1) The Sectoral CERT may adopt a similar structure CERT to offer a range of functions and services (discussed in Chapter III).

(2) Additional services provided by the Sectoral CERT differing from those of the National CERT include:

(a) sharing of specific information and in-depth knowledge with the relevant sector

(b) enlisting point of contact for the sector-specific constituency;

(c) close coordination with vendors in the sector;

(d) provide expertise in a specific sector such as hardware and systems;

(e) sector-specific conferences, workshops, training, and exercises;

(f) the creation of uniform frameworks for audit documentation at the sectoral level;

(g) faster sectoral communication channel;

(h) sector-specific recommendations.

22. **Compliance with the Sectoral CERT.**—(1) The Sectoral CERTs shall notify the following processes and seek compliance from each underlying functional entity and share it with the National CERT at least bi-annually or upon request:

(a) information security policy;

(b) data and asset classification within sectors/organisations;

(c) role and responsibilities of applications and systems custodians in their respective sectors;

(d) vulnerability assessment/penetration testing of all websites, portals, and Information Systems;

(e) risk or security assessment and whitelisting of all applications/systems used/deployed;

(f) Software Development Lifecycle (SDLC) Audit and periodic code reviews to ensure that applications continue to be secure;

(g) Information Security Audit of Information Systems and controls;

(h) issuance of SOPs for patch management, anti-virus/malware, access privileges, acceptable configuration, endpoint management, and security hardening of systems/devices;

(i) assurance of data privacy in case citizen/consumer data is stored and processed;

(j) prevention or detection of intrusion against critical systems;

(k) analysis, assessment, and prioritization criteria of events/incidents;

(l) event classification and triage mechanisms and reports;

(m) recovery and remediation records;

(n) Audit and compliance reports;

(o) Disaster Recovery and Business Continuity Plan;

(p) Incident Response Plans;

(q) Post-Incident Reports;

(r) the head of the functional entity shall designate an "Information Security Officer" from the senior management of the respective organization, who will coordinate security policy compliance efforts across the organization and interact regularly with Sectoral CERT;

(s) the designated Information Security Officer shall submit details on outcomes of implementing plans of the previous year and plans for the following year to Sectoral CERT; and

(t) non-Compliance with the afore-mentioned clauses will be dealt with through provisions, as mentioned in Chapter VI.

23. **Functional Entity.**—(1) To fulfil the requirements mentioned in Section 21 and to ensure a structured mechanism, in accordance with best information security practices, the competent authority of the functional entity is advised/required to:

(a) align its IT goals with business goals;

(b) introduce a well establish Governance structure with an empowered Information/Cyber security unit/wing;

(c) allocate sufficient funds to procure required technology and hire adequate human resources;

(d) introduce a compliance framework and formulate KPIs for reporting at the highest level;

(e) establish an Incident Management Group under the competent authority and define an escalation ladder with a list of contact persons to be contacted during the incident;

(f) identify and implement an Information Security Management System (ISMS) within the organisation;

(g) designate an "Information Security Officer" from the senior management, who will coordinate security policy compliance efforts across the organisation and interact regularly with Sectoral CERT.

CHAPTER-VI
OPERATIONAL SOPs

24. **Point of Contact.**—(1) All functional entities and the Sectoral CERTs shall designate a Point of Contact (PoC) to interface with the National CERT. The information relating to a Point of Contact shall be sent to the National CERT in the format specified by it and shall be updated from time to time.

(2) The point of Contact for Sectoral CERT will be nominated by the competent authority of the respective sector regulator and will be a Cyber Security Expert.

(3) All communications from/to the National/Government/CII CERT/Sectoral CERTs seeking information and providing directions for compliance shall be sent to the said Point of Contact.

25. **Reporting of Incidents.**—(1) Any individual, organisation, or private sector entity, not falling under any Sectoral CERT, affected or that may be affected by cyber security incidents may report directly to the National CERT through an established communication channel.

(2) The functional entity will summarily report incidents to their respective Sectoral and the National CERT within 'one hour of being identified by their respective CSIRT/CERT/IT department. Reporting will be with their best estimate at the time of notification and will report further updated information as it becomes available.

(3) After analysing the severity, impact, scale and resolution of the incident, sectoral CERT will submit a post-incident report to the National, Government, and CII CERT within a reasonable time of occurrence.

(4) The method and format of incident reporting will be devised by the National CERT under the prescribed format of information sharing. The National CERT will define the impact and severity assessment matrix for a description of incidents. The incident reporting form will provide the details of incident details such as observations e.g. IP address, malicious code, malicious URL, or any other items and actions sought against the observations e.g. website takedown, notification of possible compromised host, analysis of malicious code, an indicator of compromise extraction, etc.

26. **Compliance.—**(1) **Directions for Compliance;** In pursuance of its mandated roles and functions, as provided in PECA and NCSP with a view to augment the National Cyber Security, DG National CERT shall designate an officer to issue directions or advisory to the functional entity through Sectoral CERTs. Such directions or advisories for compliance shall be issued by email signed with an electronic signature or shared via secure web portals or encrypted applications. The functional entity shall comply with such directions or advisories and shall report to National CERT, within the time and the manner as provided in the direction or advisory.

(2) Dealing with Non-compliance;

(a) in case of non-compliance with any directions by any Service provider, intermediaries, data centres, corporate body and any other person, the concerned officer of the Cybersecurity department shall submit a non-compliance report to the Director General National CERT providing details of such non-compliance within two days from the date of expiry of such directions;

(b) on receipt of a non-compliance report, as specified in clause (a) of sub-rule (2) the DG of National CERT will issue a notice to the concerned functional entity to furnish the reasons for non-compliance within three working days; or

(c) in case of no or unsatisfactory response from the functional entity against the notice issued by the DG National CERT, the case shall be submitted to the CERT Council. Simultaneously, a non-compliance report will be shared with the competent authority of the constituent after seeking a response for reasons of non-compliance;

(d) based on the non-compliance report or where the CERT Council deems appropriate or where the severity of the cyber security incident affects or threatens to affect a government infrastructure or offences related to critical infrastructure under PECA, an authorised designated officer of National CERT will report the matter with investigation and law enforcement agency for appropriate action.

(3) **Periodical Reports:** The National CERT will draft, issue and publish a biannual report containing incidence reported/managed as well as compliance status for the information of the Prime Minister of Pakistan.

Annex A
National CERT Capability Maturity Model

Tier	Level	Description
1	**Startup**	• Core CERT functions and services (i.e. Announcements, Alert & Warnings, Security Audits or Assessments incident Reporting, and Awareness Building) are provided in limited government and military constituencies. • Support incident reporting across limited government and military sectors. • Supporrt conduct of incident, vulnearability, and artefact analysis, infrastructure security assessments, forensic investigations, system secreening, and product evaluations in limited government and military sectors. • Initiate contact with other CERTS.
	Formative	• Regular contact with other CERTs, trust relationships are cultivated and membership is applied for international forums. • All core CERT fuctions and services are provided in limited government and military constituencies. • Core CERT service processess are documented and repeatable with consistent results. • Risks to national and economic security are identified and risk value is calculated. • Data protection through detection tools and monitoring prodedure is in place. • Analysis capabilities by incident response role in limited government and military constituency. • Resiliency and recovery capabilities applied to incidens impacting business and operations.
2	**Established**	• CERT is recognised as the national Point of Contact in the national and international CERT community. • Sets of defined and documented standard processes are established and maintained for core CERT community.

		• Additional added value CERT services may be initiated and are repeatable and provide consistent results. • Risks to national and economic security are identitied, documented, and managed in a standard well-defined process. • This incident management process (preparation, analysis, containment & post-incident) is defined, documented and followed. • A continuity and disaster recovery plan is defined, documented and followed.
3	**Managed**	• CERT has an official mandate in certain national reposnibilites and has full recognition in the national & international CERT community. • Using process metrics, management can effectively control the core CERT processes. Offered CERT services are defined and processes documented, providing consistent and quality results. • Risks to national and economic security are identified and proactively monitored periodically. • The continuous monitoring program is established to detect threats in realtime. • Response time and impacts of incidents are monitored and minimized.
	Optimized	• CERT has a full official mandate for all National CERT responsibilities across all constituencies and stakeholders. • CERT has trust relationship with its consituencies, stakeholders, and peers. • CERT services are mature and focus on improving the performance of the process through incremental and innovative technological changes/improvements. • Cybersecurity risks are continously monitored and incorporated into national and economic security. • Formulated standard and poicies are operationalized in all constituencies and stakeholders of CERT. • Detection and monitoring solutions are continously learning behaviours and adjusting detection capabilites.

[File. No. 3-2/2023-Legal]

IZAZ-UL-HAQ SHAH,
Deputy Secretary.

PRINTED BY THE MANAGER, PRINTING CORPORATION OF PAKISTAN PRESS, ISLAMABAD.
PUBLISHED BY THE DEPUTY CONTROLLER, STATIONERY AND FORMS, UNIVERSITY ROAD, KARACHI.