Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

NATIONAL CYBER SECURITY POLICY 2025

2025 - 2026

MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION

Government of Pakistan

PKCERT

Table of Contents

Background

1.1 INTRODUCTION

Information and Communication Technologies (ICTs) have played a key role in revolutionizing the world, making it truly a Global Village within the last decade. The innovation in Information and Communication Technology is redefining the dimension of socio-economic development in the world, resulting in commercial, economic, cultural, and social opportunities for users of Cyberspace.

This unprecedented growth has ushered in a new era, marked with easy and low-cost access to highly interconnected networks around the globe. With the developments in the ICTs, and reliance on Broadband infrastructure, in particular, the Internet has taken center in today's modern world. The world is now increasingly interconnected and people have unprecedented access to information and knowledge.

To harness the benefits of ICT technologies and the Fourth Industrial Revolution (4IR), Pakistan has also adopted the path of Digital Transformation.

The increased use of information and communication technologies enhanced global connectivity, mobility, and versatility of digital services exposes information assets to a host of new and evolving Cyber Security threats. The Fourth Industrial Revolution has made these assets highly valuable. However, with the organic growth and proliferation of the Internet, some worrisome trends in the use of cyberspace have also emerged. The concerns over safety and security potentially impede the objective of accelerated development and affect the confidence of people in using applications and services offered to traverse cyberspace.

The rise in incidents related to malicious use of ICTs in cyberspace is affecting the integrity and the civil rights protections guaranteed by the state, level-playing field, transparency, and the socio-economic equilibrium by posing security and financial risks to the whole spectrum of users including Individuals, Businesses, Sectors, and States and could potentially impose serious barriers to achieving development goals in various economic sectors.

1.2 REVIEW OF PAKISTAN'S CYBER SECURITY LANDSCAPE

In order to ensure the online safety of the citizens of Pakistan and to ensure the security of the digital systems, various initiatives are already in place by different federal & provincial bodies and sectoral regulators under the enactments such as the Electronic Transaction Ordinance, 2002 (covering only electronic financial transactions and records), Investigation for Fair Trial Act (IFTA) – 2013, Pakistan Telecommunication (Re-Organization) Act - 1996 and Prevention of Electronic Crime Act (PECA) 2016 which cover some but not all aspects of information and Cyber Security. In addition, the State Bank of Pakistan (SBP) issues guidelines on Cyber Security for the financial sector, and the PTA has notified the Telecom Computer Emergency Response Team (CERT). However, the inter-departmental coordination and holistic approach to address the Cyber Security challenges and their emerging trends requires a special focus on a national level.

With regards to setups responsible for Cyber Security in the country, only the selective Cyber Security Incident Response Teams (CSIRTs) are operational at the organizational level in the public, private, and defense sectors. However, there is a need to enhance existing legislative and institutional frameworks, and strengthen the principal, organization, mandated for national Cyber Security. The legal framework, structures, and processes related to Cyber Security need to be constantly monitored, assessed, and improved.

To undertake academic research, National Center for Cyber Security was established in 2018. The HEC has also formulated new academic degrees that include BS, MS, and Ph.D. Cyber Security and MS Systems Security programs. However, the demand and supply gap for digital skills in general and Cyber Security, in particular, is ever-increasing, which underscores the importance of upskilling the existing resources.

In the absence of an indigenous national ICT and Cyber Security industry, Pakistan relies heavily on imported hardware, software, and services. This reliance, inadequate national security standards, and weak accreditation

has made computer systems in Pakistan vulnerable to outsider cyberattacks and data breaches through embedded malwares, backdoors, and chipsets.

1.3 CHALLENGES AND RISKS

Since data treated as an economic asset, it faces threats and risks like any other asset. To mitigate IT security vulnerabilities, a comprehensive Cyber Security policy is a baseline mechanism to address the following risks and challenges globally. The most important of these are as follows.

1.3.1 Ownership at the Top

Information is one of the fundamental pillars of knowledge-based economies. Hence, information being a National asset, its management, governance, and regulation must be synchronized at the National level using all available resources, to secure this time-sensitive valuable asset. Cyber Security requires administrative support due to its sensitive nature, challenging domain, and cross-sectoral application.

1.3.2 Governance and Implementation challenges of Cyber Security Policy and Strategy

In the absence of a centralized policy and strategy for Cyber Security, attempts at securing the digital assets of the country are liable to be random and uncoordinated.

i. WEAK ENFORCEMENT OF STATUTES

The existing legislation related to Cyber Security does not provide effective legal protection of Pakistan's digital assets. The existing legislation related to Cyber Security is not sufficient to provide an adequate mechanism and there is a dire need to transform it in such a manner that it should keep the interest of the nation in letter and spirit without fail. For that matter, an appropriate ***legislative*** structure could help to ***comply against a centralized and robust compliance framework***.

ii. ASSESSMENT AND CONTINUAL IMPROVEMENT

The legal framework, structures, and processes related to Cyber Security require monitoring, assessment, and improvement on a continuous basis or they will lose their viability and become a threat themselves. The

implementation with regards to the compliance framework of Cyber Security policy needs to be constantly monitored, assessed, and improved.

For that matter, a holistic approach and appropriate legal and technical structures could help to identify the potential threats and consequences attached thereto, and properly it could investigate and no weak area be left to be exploited by the wrongdoers.

1.3.3 Enforcement of Required Structures and Processes

The assurance of Cyber Security requires proper structures and processes for governance, regulation, implementation, and enforcement. Any absence or weakness of the regulation structures poses a threat to Cyber Security.

i. Inadequate and Poor Quality of Resources

Cyber Security is a rapidly growing field that requires a continually updated set of relevant skills and resources as the inadequacy of the required skills shall lead to weaknesses in Cyber Security. Moreover, bridging the demand and supply gap in the digital workforce is an emerging challenge. The absence of a mechanism for ensuring the quantity and quality of these skills and resources is a threat to the Cyber Security of the country.

ii. Lack of Data Governance

Countries face the threat of data colonization whereby data is managed, controlled, and processed out of the legal jurisdiction of the country and there is limited or no bilateral agreement among the stakeholders in this regard. Threat actors are liable to pollute the information domain and citizen data may be sold to third parties without due consent or validation. Such proliferation and abuse of data lead to the exploitation of selected segments of society.

Weak governance of data, poor data quality, and absence of data stewardship generate unreliable information resources and poses a threat to Cyber Security.

iii. Reliance on External Resources

With the increasing use of information technology in all domains including operations technology, critical information assets are likely to be exposed to cyber-attacks. In absence of adequate local resources, reliance on external

resources including skills, hardware, and software, is a direct threat to Cyber Security.

iv. Challenges of Coordinated Response to Threats and Attacks

An effective response to risks, threats, and attacks requires a coordinated effort through a series of response teams (CERTs). The absence of such teams and lack of coordination between them is a major threat. This is majorly due to the weak Cyber Security posture and functions within the affiliate organizations. Empowering support organizations is vital to a successful Cyber Security ecosystem.

1.4 COURSE OF ACTION

This Policy will serve as the foundation for the construction of a holistic digital ecosystem with supporting frameworks and components for the delivery of secure, reliable, and standardized digital services, applications, and digital infrastructure. This Policy will drive the fundamental demand in the local IT industry to ensure quality delivery of its products and services. This will provide an opportunity for local & international entrepreneurs and firms to offer core competencies, services, and solutions and offer an opportunity to local industry to become better positioned to compete and prosper on the international stage. The focus will also be on promoting online businesses enabling the smooth running of digital payments within and outside Pakistan.

Moreover, to mitigate cyber threats, the country faces today and to improve the national Cyber Security outlook, it is imperative to undertake the strengthening of national Cyber Security capabilities through the development of essential and well-coordinated mechanisms, implementation of security standards and regulations under a policy and legislative framework.

In this regard, the Government of Pakistan constituted Cyber Governance Policy Committee (CGPC). Noting the strategic importance of Cyber Security, the present Government has prioritized the formulation of the first National Cyber Security Policy – 2025. This initiative is in conformity with the national cyber vision.

2 Vision, Scope & Objectives

2.1 VISION

The vision is for Pakistan to have a secure, robust, and continually improving nationwide digital ecosystem ensuring accountable confidentiality, integrity, and availability of digital assets leading to socio-economic development and national security.

2.2 SCOPE

This policy framework is envisaged to secure the entire cyberspace of Pakistan including all digital assets of Pakistan, data processed, managed, stored, transmitted or any other activity carried out in public and private sectors, and the information and communication systems used by the citizens of Pakistan.

2.3 OBJECTIVES

- To establish **governance and institutional framework** for a secure cyber ecosystem.
- To enhance the security of **national information systems** and infrastructure.
- To create a **protection and information sharing mechanism** at all tiers capable to monitor, detect, protect and respond against threats to national ICT/ CII infrastructures.
- To protect National Critical Information Infrastructure by mandating **national security standards and processes** related to the design, acquisition, development, use, and operation of information systems.
- To create an **information assurance framework** of **audits and compliance** for all entities in both public and private sectors.
- To ensure the **integrity of ICT products**, systems, and services by establishing a mechanism of **testing, screening, forensics, and accreditation**.
- To protect the **online privacy of the citizens** by provisioning the required support and system to all the concerned institutions and organizations

that are dealing with citizens' data-related matters be more equipped and able to render their services, accordingly.

- To develop **public-private partnerships** and collaborative mechanisms through technical and operational cooperation.
- To create a country-wide culture of **Cyber Security awareness** through mass communication and education programs.
- To train **skilled Cyber Security professionals** through capacity building, skill development, and training programs.
- To encourage and support **indigenization and development** of Cyber Security solutions through **R&D Programs** involving both public and private sectors.
- To provide a framework on **national-global cooperation and collaborations** on Cyber Security.
- To Identify and process **legislative and regulatory actions** under the mandates of relevant stakeholders assigned in the policy.
- Risks related to Cyber Security need to be managed continuously. Encourage adoption of a **risk-based approach** to Cyber Security through frameworks including those for regulation, assurance, threat management, and incident management.

2.4 PRINCIPLES

Guiding principles to achieve policy objectives are: -

- All actions will be driven to protect online data privacy and security of citizens and enhance national and public prosperity in the digital domain.
- Respective public and private organizations responsible to ensure the Cyber Security of their data, services, ICT products, and systems will be supported to deliver the same.
- In case of any incident, the government will lead the national response with support from both the public and private sectors.

- Will regard a cyber-attack on Pakistan CI/ CII as an act of aggression against national sovereignty and will defend itself with appropriate response measures.
- Will act per national and international Cyber Security frameworks, standards and best practices and expect reciprocal respect of our national digital sovereignty.

Policy Deliverables

3.1 CYBER SECURITY GOVERNANCE

3.1.1 POLICY FORMULATION AND OVERSIGHT: CYBER GOVERNANCE POLICY COMMITTEE (CGPC)

A Cyber Governance Policy Committee (CGPC) has been constituted to assert national level ownership to policy initiatives related to cyber-governance and security. Cyber Governance Policy Committee is responsible for strategic oversight over national Cyber Security issues.

- **Core Functions:**
  - Formulate, guide, and recommend for the approval of the **National Cyber Security Policy** and **Cyber Security Act**.
  - Assist in addressing requirements of organizational structures, technical, procedural, and legal measures to support the policy mandate and implementation mechanisms.
  - Harmonize the working and operational reporting mechanism of all departments dealing with the subject.
  - Carry out consultations on aspects related to cyber governance on a regular and permanent basis.
  - Assign roles to national institutions for international representation and collaboration with global and regional bodies and organizations.
  - Guide to align policy with emerging cyberspace requirements through updates and periodic reviews.

- The policy recommendations of CGPC will be approved/endorsed by the Federal Cabinet.

3.1.2 INSTITUTIONAL STRUCTURE FOR IMPLEMENTATION

To achieve the objectives, an implementation framework shall be developed by a designated organization of the Federal Government, dealing with the subject of Cyber Security. This organization shall also act as the Central Entity at the federal level for coordination and implementing all Cyber Security related matters ***on the below levels:***

i. **National Level**: The Central Entity along with its National Computer Emergency Response Team (nCERT) and National Security Operation Center (nSOC).
ii. **Sectoral Level**: Sectoral Regulator(s)/ CERTs (including but not limited to Defense, Telecom, Banking and finance, Power, Federal, and Provincial public sector).
iii. **Organizational Level**: Enterprises, entities, and individual users.

3.2 ACTIVE DEFENCE

The relevant stakeholders will also undertake specific actions which including but not limited to the following:

- Working with **Internet Service Providers (ISPs) and Telecom operators to block malware attacks**, by restricting access to specific domains or websites that are known sources of malware (known as Domain Name System (DNS) blocking / filtering, etc.). Active defense strategies will be formulated with the engagement of respective stakeholders.
- Preventing **email phishing and spoofing activity** on public networks.
- Promoting **security best practice** through Internet governance organizations; such as **Internet Corporation for Assigned Names and Numbers** (ICANN), Asia Pacific Network Information Center (APNIC), the Internet Engineering Task Force (IETF), European Regional Internet Registry (RIPE), and UN Internet Governance Forum (IGF), etc.
- Work with **international law enforcement channels** to protect Pakistan citizens from cyber-attacks from unprotected infrastructure overseas.

- Work towards **implementation of controls** to secure the **routing of Internet traffic for government departments** to avoid illegitimately re-routed by malicious actors.
- Investing in capabilities enhancement programs of Law Enforcement Agencies (LEAs) and concerned Ministries/Divisions to enable them to respond against state-sponsored and criminal cyber activities targeting Pakistan networks and systems.

3.3 PROTECTING INTERNET-BASED SERVICES

The relevant stakeholders will initiate actions, including but not limited to:

- Develop an **Internet Protocol (IP) reputation service** to protect government digital services (this would allow online services to get information about an IP address connecting to them, helping the service get more informed on risk management decisions in real-time).
- Seek to install **products on government networks** to ensure that software is running correctly and not being maliciously interfered with.
- Look to **expand beyond the gov. pk domain** into other digital services measures that notify users who are running outdated technologies.
- Sharing of confidential information between public and private organizations, **safeguarding online data privacy of citizens, and ensuring complete data protection**.
- Strive for **protecting digital systems and services** attached thereto.

3.4 PROTECTION AND RESILIENCE OF NATIONAL CRITICAL INFORMATION INFRASTRUCTURE

To achieve this critical objective, the stakeholders will;

- **Operate requisite technical platforms** to protect National Critical Information Infrastructure, information and communication technologies (ICT), Next Generation(s) Mobile Service and Networks, and IoT security and work as a modal organization in the country. Encourage a culture of "accountability" and "self-governance" such

that respective public and private organizations will be responsible to safeguard their digital assets, data, products, and services to improve their confidentiality, integrity, and availability.

- **Institute processes** for identification, prioritization, assessment, and protection of Critical Information Infrastructure.
- Ensure a secure **ICT environment including mobile systems and cloud-based solutions** through state-of-the-art security measures.
- Mandate implementation of **national security standards** by all critical sector entities, to reduce the risk of disruption.
- **Develop a mechanism for the protection of Critical Information Infrastructure** and its integration at the entity level through relevant sectoral CERTs.
- Establish and **enforce Cyber Security risk management methodologies** according to any of the prevalent international standards inter alia ISO/IEC 27005:2008 and ISACA RISK IT etc.
- Mandate all **operators of national, provincial, and organizational** Critical Information Infrastructure to **hire qualified Cyber Security individuals** and add an appointment of **Chief Information Security Officer (CISO)**.
- **Enforce the use of digital certifications and its accreditation including accreditation of national security standards** in developed, developing, and deployed information and communications networks or systems in public and private sectors.

3.5 PROTECTION OF GOVERNMENT'S INFORMATION SYSTEMS AND INFRASTRUCTURE

To cater to a specific need of public sector information infrastructure, the stakeholders will:

- Access to all government systems with the mandated and desired access control technology
- Encourage the establishment of national Data Centers to co-locate servers and telecom Quality infrastructure for all government entities - federal & provincial.

- Define and enforce a **robust Government Authentication** and **Data Protection Framework** including data classification and to ensure that appropriate controls exist to protect data.
- Create **vulnerability management and patch management program** for all government technical systems.
- Work with relevant government entities to ensure **mandatory allocation of a certain percentage of the ICT project budget** for Cyber Security Assurance.
- Formulate a mechanism for the creation and enforcement of **staff vetting and clearance schemes** across the government.
- Improve **security in government and critical infrastructure outsourcing and procurement** through vetting and assurance of suppliers and enforcement of security clauses in contracts. Enforce **periodic security & risk assessments** of critical suppliers.

3.6 INFORMATION SECURITY ASSURANCE FRAMEWORK

For the attainment of this objective the stakeholders will:

- Implement the concept of "**Cyber Security by Design**" in ICT products and services through screening and accreditation of national security standards.
- Upgrade and establish next-generation **national Cyber Security forensic and screening setups** to safeguard against advanced cyber threats in Artificial Intelligence (AI) driven environment.
- To create an information assurance framework for **Cyber Security audit and compliance** requirements for all entities in both public and private sectors.
- Create infrastructure and/or leverage existing facilities/ platforms/ resources for conformity assessment and certification of compliance to Cyber Security best practices, standards, and guidelines (e.g., ISO 27001 ISMS certification, PCI/PA DSS for FIs, or other industry standards and benchmarks, internal security system audits, Penetration testing /

vulnerability assessment, application security testing, web security testing, business continuity planning test, etc.).

- Develop and mandate organizations for the **establishment of testing, screening, forensics, and accreditation facilities** in line with laid national and international best standards in order to gain from evolving best practices and standards.

3.7 PUBLIC-PRIVATE PARTNERSHIP

The stakeholders will develop a framework to: -

- Nurture an environment for entrepreneurship based on cooperation among government, industry, academia, and research institutions in different areas e.g. supply chain risk management, etc.
- Provide governmental support to start-ups and facilitate them to grow into competitive companies.
- Enable privately-owned Cyber Security groups/ organizations to collaborate with government bodies and regulate their actions.
- Facilitate the exchange of information on the development of new legislation and regulation between stakeholders.
- Any other framework as deemed appropriate by the Federal Government.

3.8 CYBER SECURITY RESEARCH AND DEVELOPMENT

Considering the importance of indigenous security product design, development, and manufacture; the stakeholders will develop and implement a framework involving all segments in public and private sectors to:

- Undertake Research & Development programs aimed at short-term, medium-term, and long-term goals.
- Research & Development programs shall address all aspects including the development of Cyber Security systems, testing, deployment, and maintenance throughout the life cycle.
- Encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of Cyber Security challenges.

- Facilitate commercialization of the outputs of Research & Development into commercial products and services for use in public and private sectors.
- Set up Centers of Excellence in areas of strategic importance for the security of cyberspace.
- Mandate all local entities at the appropriate time (depending on the growth of indigenous capabilities) to gradually shift on indigenous products.

3.9 CAPACITY BUILDING

With the ever-growing need for enhanced Cyber Security measures, there is an equal demand for producing well-trained human resources. Therefore, the stakeholders will:

- Establish **Centers of Excellence** to educate and train human resources in Cyber Security domains to strengthen and uplift the human support base.
- Formulate and implement customized **human resource development programs** to fulfill the Cyber Security needs of both public and private sectors.
- Increase Cyber Security **research and development (R&D) budget** for the development of indigenous Cyber Security solutions to minimize dependency on foreign technologies.
- Establish a **special court** to adjudicate the matters related to Cyber Security and related proceedings.
- Include **cybercrime-related curriculum in the graduate and post-graduate Engineering and Law related degrees**, training of prosecutors, lawyers and judges, etc.

3.10 AWARENESS FOR NATIONAL CULTURE OF CYBER SECURITY

Mass awareness effort is of paramount importance to create knowledge on relevant risks, preventive measures, and effective responses to cyber threats in all public and private entities. Both top-down and bottom-up approach is essential to create a cyber-aware culture. The stakeholders will:

- Plan and implement **education programs on cyber-ethics and security** programs customized for specific sectors of society, such as students, government officials, law enforcement agencies, and private organizations employees.
- Encourage the **corporate sector to protect cyberspace** by maintaining the desired level of Cyber Security in their products and services.
- Preparation and execution of **national awareness program** to educate end-users at home or workplace.
- Implementation of a **Cyber Security awareness program for government** systems.
- Add Cyber Security awareness to the **national education curriculum** at the middle and secondary levels.

3.11 GLOBAL COOPERATION AND COLLABORATIONS

The Ministry of IT & Telecom and the Central Entity will play a key role in recommending the country's viewpoint for the international forum and will make recommendations for joining international collaborations. Representation at the national and international events on information and Cyber Security shall include the Ministry of IT & Telecom, Ministry of Foreign Affairs, Ministry of Law & Justice, Ministry of Interior, and other stakeholders including the Central Entity as per requirement. The Ministry of IT & Telecom, in consultation with the Central Entity, will:

- Work with all international partners such as ITU-IMPACT etc.
- Maintain continuous presence and provide professional input from Pakistan to all major global and regional organizations and professional bodies related to the subject including ICANN, GAC, ITU, APT, and other such UN and non-UN agencies.
- Affiliation of all national, regional, and international bodies to establish desired coordination and cooperation to establish cyber situational awareness.

- Develop a mechanism for trusted information exchange about cyber-attacks, threats, and vulnerabilities with the public, inter-governmental and non-governmental bodies locally and globally.

3.12 CYBERCRIME RESPONSE MECHANISM

The stakeholders will:

- Assist and enhance government capacity by augmenting law enforcement agencies' technical capability to respond to cybercrimes.
- Establish liaison and coordination with other national and international cybercrime agencies for sharing of information and cooperation.
- Strengthen the processes and procedures and embed Cyber Security in the public and private service networks vulnerable to cybercrimes.

3.13 REGULATIONS

In order to achieve defined objectives and effectively implement National Cyber Security Policy, it is imperative to introduce appropriate objective-based legal frameworks for cyber governance. These will be formulated after consultation with stakeholders and will include, but not limited to the following:

- Formulation of National Cyber Security Plan and Cyber Security related Law(s).
- Rules and regulations for national Cyber Security framework.
- National Cyber Security /Governance Operations and information sharing mechanism, for incident handling, management capability, and cyber situational awareness.
- Compliance, screening, accreditation, and risk management regulations: for Critical Information Infrastructure, public-private partnerships, capacity building, Cyber Security awareness, R&D programs, and global cooperation.
- Standardization of Digital and Network Forensics processes and Infrastructure for Cyber Governance in harmonization with this policy and PECA 2016/ any other relevant law.

- Compliance for auditing and ensuring the national Cyber Security standards across Pakistan.
- Prioritizing initiatives to address growing dimensions of the cybercrimes by empowering the legal entities and rectifying the shortcomings under PECA 2016.

3.14 ESTABLISHING TRUST IN DIGITAL TRANSACTIONS

In order to build and maintain the trust of users in the security and integrity of digital services. This will cover the below-mentioned areas:

- Enforce Digital Certifications for the authenticity of individuals and businesses including enhancing technology for enabling digital signature / electronic transactions.
- Encourage work on scalable Public Key Infrastructure (PKI) as per future business requirements (e-passport, e-voting, e-filing, e-procurement, e-governance, etc.).
- Encourage multiple Certification Service Providers and enabling the security and trust of digital services such as E-commerce, Fin-tech, and other government to citizen services.

3.15 IMPROVE PAKISTAN'S ICT RANKING

The objective of improving Pakistan's ICT ranking based on international indices and benchmarks will be achieved by focusing on the below areas:

- Map the existing position of Pakistan in the international market with regards to ICT keeping in view the business and innovation environment, infrastructure, affordability, skills readiness, and socioeconomic impact.
- Support the measures to improve the provision of data to the international rating agencies.

3.16 RISK MANAGEMENT AND RISK-BASED APPROACH

The management of incidents and problems will require risk management because of resource limitations. The objective of risk management and adoption of a risk-based approach will be achieved by requiring and encouraging organizations to define the risk criteria, risk

appetites, and risk tolerances for themselves as part of their enterprise risk management activity. In addition to that, risk mitigation plans will be required to be maintained by all bodies and organizations themselves.

The notable Cyber Security risks/challenges could be the Internet of Things, Ransomware, AI (Artificial Intelligence), Server less Apps, Critical National Infrastructure, Sophisticated Phishing Campaigns, Strategic Use of Information Operations, Cloud Computing, Cyber Security awareness, Hacker-for-hire services, and Skills shortages, etc.

3.17 APPENDIX – GLOSSARY OF TERMS

- **Critical Sector** - Government systems, utility infrastructure (electricity, gas, and water), education, health, transport system (air, road, rail, and sea), emergency services, manufacturing facilities, banking and financial sector, telecommunication/ ICT sector, dams, etc.
- **Critical Information Infrastructure (CII)** - This generally includes the energy, telecom, finance, water & healthcare sectors.
- **Accountability** - State of being answerable for decisions and activities.
- **Cyber Security** - Preservation of confidentiality, integrity, and availability of information in Cyberspace.
- **Digital Asset** – Systems, applications, services in cyberspace or any other sandbox environment.

Interim Measures

The implementation mechanism provided for this policy may require considerable time to be completely functional. Therefore, during this interim period, the capacities and capabilities which state organizations and institutions currently have and are supportive of the implementation of this policy will be utilized and their continued use will be integrated with an all-encompassing implementation mechanism.

Pakistan Telecommunication Authority as per Telecom Act 1996, Telecommunications Policy 2015, and PECA 2016 will implement Telecom Sector technical platform (sectoral CERT as provided herein) in collaboration with the telecom industry.

To achieve the short term, medium, and long-term objectives sectoral bodies such as banking, telecom, education, and provincial institutions will be empowered to strengthen the national Cyber Security posture. In short term, capacity building of relevant stakeholders around stated policies, standards, and procedures will be prioritized and planned to achieve within the first year of the policy.

Policy Review and Implementation

The National Cyber Security Policy 2025 is subject to inclusive review after every three years and as when required, depending on the emerging global cyber trends and technological advancements by the relevant organization in consultation with all stakeholders.