Ministry of Information Technology
& Telecommunication

**DIGITAL PAKISTAN**

# NATIONAL CYBER SECURITY POLICY 2025

**2025 - 2026**

**MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION**

Government of Pakistan

National Cyber Security Policy 2025

## 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 us here d in a new era, marked with easy and low-cost access to highly interconnected networks around the globe.

## 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 areal ready in place by different federal & provincial bodies and sect oral 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.

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

# 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.

## 2.4 PRINCIPLES

Guiding principles to achieve policy objectives are:-

- AI 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.

# 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 over sight 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.

## 3.2 ACTIVE DEFENCE

The relevant stakeholders will also undertake specifications 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.

## 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).
- Look to **expand beyond the gov. pk domain** in to other digital services measures that notify users who are running outdated technologies.

## 3.4 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.

## 3.5 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.

## 3.6 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.

## 3.7 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.

- Increase Cyber Security **research and development (R&D) budget** for the development of indigenous Cyber Security solutions to minimize dependency on foreign technologies.

## 3.8 GLOBAL COOPERATION AND COLLABORATIONS

The Ministry of IT & Telecom and the Central Entity will play a key role in recommending the country's view point for the international forum and will make recommendations for joining international collaborations. 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.

## 3.9 CYBER CRIME RESPONSE MECHANISM

The stakeholders will:

- Assist and enhance government capacity by augmenting law enforcement agencies 'technical capability to respond to cybercrimes.
- Strengthen the processes and procedures and embed Cyber Security in the public and private service networks vulnerable to cybercrimes.

## 3.10 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. 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.

## 3.11 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.).

## 3.12 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

## 3.13 APPENDIX – GLOSSARY OF TERMS

- **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.

## 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.

## 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.