Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

NATIONAL CYBER SECURITY POLICY 2021

Consultation Draft v1.0

JANUARY 25, 2021

MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION

Government of Pakistan

Table of Contents

1 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 the Cyberspace.

This unprecedented growth has ushered 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 a center in today's modern world. The world is now increasingly interconnected and people have un-precedented access to information and knowledge.

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

With the organic growth and proliferation of the internet, unfortunately, 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 the cyberspace.

These increasing incidents related to malicious use of ICTs in cyberspace is posing security and financial risks to 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 CYBER SECURITY LANDSCAPE

Pakistan existing policies do not provide effective cyber security mechanism. Electronic Transaction Ordinance, 2002 (covering only electronic financial transactions and records), Investigation for Fair Trial Act (IFTA) – 20013, Pakistan Telecommunication (Re-Organisation) Act - 1996 and Prevention of Electronic Crime Act (PECA) 2016 are the available legislations which cover

some but not all aspects of information and cyber security. State Bank of Pakistan (SBP) issues guidelines on cyber security for financial sector only, whereas PTA is in process of establishing Telecom CERT.

With regards to setups responsible for cyber security in the county, only selective Cyber Security Incident Response Teams (CSIRTs) are operational at organizations level in public and defence sectors. However, there is a void which needs to be bridged in terms of requisite legislation, implementation framework and lead organization, mandated for national cyber security.

Although, to undertake academic research, National Center for Cyber Security was established in 2018, but gap between supply and demand of talented cyber security experts still exists. With absence of indigenous national ICT and cyber security industry, Pakistan relies heavily on imported hardware and software. This reliance along with absence of national security standards and weak accreditation have made Pakistan vulnerable to foreign exploitation through imbedded malwares, backdoors and chipsets.

1.3 COURSE OF ACTION

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 development of essential and well-coordinated mechanisms, implementation of security standards and regulations under a policy and legislative framework.

In this regard, Prime Minister of Pakistan constituted Cyber Governance Policy Committee (CGPC), comprising of all relevant ministries and organisations in 2016. To create a cyber-governance framework, Government of Pakistan has formulated first National Cyber Security Policy - 2021 in line with our national cyber vision.

2 Vision, Scope & Objectives

2.1 VISION

"To develop secure and resilient cyber systems and networks for national cyber security and response."

2.2 SCOPE

This policy framework envisaged to secure entire cyberspace of Pakistan including all information and communication systems used in both public and private sectors.

2.3 OBJECTIVES

- To establish a **governance and institutional framework** for secure cyber ecosystem.
- To create **protection and information sharing mechanism** (CERTs/ SOCs) 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 enhance security of **government information systems** and infrastructure.
- To create an **information assurance framework** of **audits and compliance** for all entities in both public and private sectors.
- To ensure **integrity of ICT products**, systems and services by establishing a mechanism of **testing, screening, forensics and accreditation**.
- To develop **public private partnerships** and collaborative mechanism through technical and operational cooperation.
- To create a country wide culture of **cyber security awareness** through mass communication and education programs.
- To develop and create **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 framework on **national-global cooperation and collaborations** on cyber security.
- To Identify and process **legislative and regulatory actions** pursuant to the mandates of relevant stakeholders assigned in the policy.

2.4 PRINCIPLES

Guiding principles to achieve policy objectives are: -

- All actions will be driven by the need to protect our people and enhance national and public prosperity.
- Respective public and private organisations will be responsible to ensure cyber security of their online data, services, ICT products and systems.
- In case of any incident, government will lead the national response with support from both public and private sector.
- 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 in accordance with national and international laws and expect reciprocal respect of our national digital sovereignty.

3 Policy Framework

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 with an aim 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:**
  - Guide and expedite formulation and approval of **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 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.
  - Provide guidance 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 at the Central

Entity at the federal level for coordination and implementing all Cyber Security related matters.

- **National Level**: The Central Entity along with its National Computer Emergency Response Team (nCERT) and National Security Operation Center (nSOC).
- **Sectoral Level**: Sectoral Regulator(s)/ CERTs (Defense, Telecom, Banking and finance, Power, Federal and Provincial public sector)
- **Organisational Level**: Enterprises, entities and individual users.

3.2 ACTIVE DEFENCE

The Central Entity will also undertake specific actions which including but not limited to the following:

- Working with **Internet Service Providers (ISP) and Telecom operators to block malware attacks**, by restricting access to specific domains or web sites that are known sources of malware (known as Domain Name System (DNS) blocking / filtering).
- Preventing **email phishing and spoofing activity** on public networks.
- Promoting **security best practice** through internet governance organisations; such as **Internet Corporation for Assigned Names and Numbers** (ICANN), 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 for response against state-sponsored and criminal cyber activities targeting Pakistan networks and systems.

3.3 PROTECTING INTERNET BASED SERVICES

The Central Entity 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 are running correctly and not being maliciously interfered.
- Look to **expand beyond the gov.pk domain** into other digital services measures that notify users who are running out-of-date browsers.

3.4 PROTECTION AND RESILIENCE OF NATIONAL CRITICAL INFORMATION INFRASTRUCTURE

To achieve this critical objective, the Central Entity will;

- **Operate requisite technical platforms** to protect National Critical Information Infrastructure and work as nodal organization in the country.
- **Institute processes** for identification, prioritization, assessment and protection of Critical Information Infrastructure.
- Ensure 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 protection of Critical Information Infrastructure** and its integration at the entity level through relevant sectoral CERTs.
- Establish and **enforce risk management methodologies** according to international standards inter alia ISO/IEC 27005:2008 and ISACA RISK IT etc.
- Mandate all **operators of national, provincial and organisational** Critical Information Infrastructure to **hire qualified Information Security individuals** and add an appointment of **Chief Information Security Officer (CISO)**.

- **Enforce accreditation of national security standards** in developed, developing and deployed information and communications networks or systems at public and private sectors.

3.5 PROTECTION OF GOVERNMENT'S INFORMATION SYSTEMS AND INFRASTRUCTURE

To cater for specific need of public sector information infrastructure, the Central Entity will:

- Define and enforce a **robust Government Authentication** and **Data Protection Framework**.
- Create **vulnerability assessment and patch management process** for all government technical systems.
- Work with relevant government entities to ensure **mandatory allocation of a certain percentage of ICT project budget** for Information Security Assurance.
- Formulate a mechanism for creation and enforcement of **staff vetting and clearance scheme** across the government.
- Improve **security in government outsourcing and procurement** through vetting of suppliers and enforcement of security clauses in contracts.

3.6 INFORMATION SECURITY ASSURANCE FRAMEWORK

For attainment of this objective the Central Entity will:

- Implement the concept of "**Information 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 advance cyber threats in Artificial Intelligence (AI) driven environment.
- To create an information assurance framework for **cybersecurity 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, internal security system audits, Penetration testing / vulnerability assessment, application security testing, web security testing etc.).

- Develop and mandate other organisations for **establishment of testing, screening, forensics and accreditation facilities** in line with laid national and international standards.

3.7 PUBLIC PRIVATE PARTNERSHIP

The Central Entity will develop a framework to: -

- Nurture an environment for entrepreneurship based on cooperation among government, industry, academia and research institutions.
- 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 exchange of information on development of new legislation and regulation between stakeholders.
- Any other framework as deemed appropriate by the Federal Government.

3.8 CYBERSECURITY RESEARCH AND DEVELOPMENT

Considering importance of indigenous security product design, development and manufacture; the Central Entity 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 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 security of cyber space.
- Mandate all local entities at appropriate time (depending on the growth of indigenous capabilities) to gradually shift on indigenous products.

3.9 CAPACITY BUILDING

With ever-growing need for enhanced cybersecurity measures, there is an equal demand of producing well trained human resource. Therefore, the Central Entity will:

- Establish **Centers of Excellence** to educate and train human resource in cyber security domains to strengthen and uplift 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 development of indigenous cyber security solutions to minimize dependency on foreign technologies.
- Include **cybercrime related curriculum in the graduate and post graduate Law related degrees**, training of prosecutors, lawyers and judges etc.

3.10 AWARENESS FOR NATIONAL CULTURE OF CYBERSECURITY

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 Central Entity will:

- Plan and implement **education programs on cyber ethics and security** programs customized for specific sectors of society, such as students, government officials and private organisations employees.

- Encourage **corporate sector to protect cyberspace** by maintaining desired level of cyber security in their products and services.
- Preparation and execution of **national awareness program** to educate end users at home or at work place.
- Implementation of a **cybersecurity awareness program for government** systems.
- Add cyber security awareness to the **national education curriculum** at middle and secondary level.

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 view point for international fora and will make recommendations for joining international collaborations. Representation at the national and international events on information and cyber security shall include Ministry of IT & Telecom, Ministry of Foreign Affairs and 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 organisations and professional bodies related to the subject including ICANN, GAC, ITU, APT and other such UN and non-UN agencies.
- Develop 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 Central Entity will:
- Assist and enhance government capacity by augmenting law enforcement agencies technical capability to monitor, identify and 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 frameworks and regulations for cyber governance. These will be formulated by in consultation with stakeholders and will include, but not limited to the following:

- Formulation and processing of National Cyber Security Policy and Cyber Security Act.
- Rules and regulations for national cybersecurity framework.
- National Cyber Security /Governance Operations and information sharing mechanism: for incident handling, management capability and furnishing evidences.
- 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.
- Digital Certifications for authenticity of individuals and businesses.
- Sharing of confidential information between public and private organizations, safeguarding privacy of citizens and ensuring data protection.
- Standardization of Digital and Network Forensics processes and Infrastructure for Cyber Governance in concert with this policy and PECA 2016.
- Compliance for auditing and ensuring the national cyber security standards across Pakistan.

4 Interim Measures

The implementation mechanism provided for this policy may require considerable time in order to be completely functional. Therefore, during this interim time 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 continual use will be integrated with 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 telecom industry.

5 Policy Review and Implementation

The National Cyber Security Policy 2021 is subject to inclusive review after every three years, depending on the emerging global cyber trends and technological advancements by the relevant organization in consultation with all stakeholders.