CYBER SECURITY STRATEGY

FOR TELECOM SECTOR

2023-2028

www.pta.gov.pk

Table of Contents

Glossary

Cyber Security: It means proactive and reactive measures for the protection of critical data and infrastructure from attack, damage and unauthorized access.

Cyber Security Incident: It means a cyber-security event which may adversely impact the availability, integrity and confidentiality of critical data.

Cyber Threat: Any act that seeks to exploit vulnerabilities in a computer system or network for malicious purposes. Cyber threats can be initiated by individuals, groups, or nation-states.

CTDISR: Critical Telecom Data and Infrastructure Security Regulations 2020 issued by PTA.

NCSP: National Cyber Security Policy 2021 issued by Ministry of Information Technology and Telecommunication (MoITT).

PECA: Prevention of Electronic Crimes Act 2016.

NCCS: National Centre for Cyber Security, commenced by Government of Pakistan in June 2018. The NCCS project is a joint initiative of Higher Education Commission (HEC) and Planning Commission.

CII: Critical Information Infrastructure includes systems, networks, or assets, whether physical or virtual, that are essential to the functioning of a society and the economy. The disruption or destruction of CII could have a significant impact on the availability of essential services, the well-being of the population, or national security. Examples of CII include power grids, transportation systems, healthcare facilities, financial systems, and communication networks.

eSIM/iSIM: Embedded SIM cards that are built directly into devices, such as smartphones and tablets. They are designed to be more secure and offer more flexibility than traditional SIM cards.

ICT: Information and Communication Technology

IoT: Internet of Things, i.e. a network of devices, vehicles, and other items embedded with electronics, software, sensors, and connectivity, which enables them to connect and exchange data.

IXP: Internet Exchange Point is a physical location where internet service providers (ISPs) connect their networks to exchange traffic.

Smart Devices: Devices that are embedded with sensors, software, and connectivity, which allow them to connect and exchange data with other devices, networks, and the internet.

VPN: Virtual Private Network, a secure encrypted channel between a computer or network to another computer or network over the internet.

Whitelisting: A security practice that allows only pre-approved programs or applications to run on a computer or network while blocking all other programs or applications.

CERT: Computer Emergency Response Team means a team composed primarily of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

CTD: Critical Telecom Data means personal data related to PTA licensee, licensee users / customers which is retained by the telecom licensee and such information which is critical for the operations, confidentiality and security of the licensee telecom systems including voice / data communication of its users/ customers being handled by the telecom licensee.

CTI: Critical Telecom Infrastructure means equipment / assets whether physical or virtual, which are vital for the provision of telecom licensed services and for storing, processing and transferring data.

SBP: State Bank of Pakistan is the central bank of Pakistan responsible for regulating and supervising the country's banking and financial system.

NEPRA: National Electric Power Regulatory Authority is a regulatory body responsible for the regulation of electric power generation, transmission, and distribution in Pakistan.

SECP: Securities and Exchange Commission of Pakistan is a regulatory body responsible for regulating and supervising the securities market in Pakistan.

Acknowledgment

This document has been prepared as an obligation under clause 1.3.2 of National Cyber Security Policy, 2021. This report has been supervised by Dr. Muhammad Mukaram Khan, Director General CVD, of the Pakistan Telecommunication Authority (PTA).

The first draft was shared with Chief Information Security Officers (CISOs) of all major Telecom Operators as part of our regular consultative process. PTA values collective wisdom as key to successful implementation of every concept, as it induces synergy in our efforts with joint onus. We are grateful to valuable input by all, which has been incorporated in the final version.

This report has been finalized and completed with the joint efforts of team comprising Mr. Ahmed Bakhat, Director Cybersecurity; Mr. Rafay Baloch, Senior Consultant Cybersecurity; Mr. Sikandar Abbas, Deputy Director Cybersecurity; Mr. Kamran Khan, IT Officer Cybersecurity; and Mr. Arslan Shahid, Management Trainee Officer Cybersecurity at PTA. Proofreading was carried out by Ms. Tayyaba Iftikhar, Assistant Director PR.

In addition, the successful completion of this project owes much to the support of Mr. Mudassar Naveed, Director General Strategy & Development (S&D) and Mr. Muhammad Khurram Siddiqui, Director General Law & Regulations (L&R) at PTA.

Above all, we would like to express our gratitude to Honorable Members of the Authority for their valuable guidance, supervision and directions, which have been the primary inspiration behind the concept and contents of this report.

Maj General (R) Hafeez Ur Rehman, HI (M)
Chairman PTA

Mr. Muhammad Naveed
Member (Finance)

Dr. Khawer Siddique Khokhar
Member (Compliance & Enforcement)

FOREWORD FROM THE AUTHORITY

As the digital world evolves and expands, so must our commitment to cybersecurity. It is no longer enough to simply protect physical borders; now we must secure digital frontiers as well to protect our national cyber space. The National Telecom Cyber Security Strategy outlays Pakistan Telecom Sector's next five years' implementation framework to achieve the objectives laid out in the National Cyber Security Policy – 2021 for protecting the national digital infrastructure and sensitive data. It will help ensuring that the Telecom Sector is prepared against any inevitable cyber threat and attacks that may endanger national cyber security.

The National Telecom Cyber Security Strategy outlines a comprehensive set of initiatives to ensure that cybersecurity remains the focus of our efforts in the next five years, being one of the highest priorities of Pakistan Telecom Authority. It outlines specific measures to bolster the security of our networks, systems, and data; and to ensure that the infrastructure is resilient against potential cyber-attacks.

It also outlines effective measures to protect users from cyber threats and to respond swiftly and effectively to any cyber incident(s). This strategy is a result of extensive consultation with experts from the public and private sectors. It reflects the importance of cyber security in today's digital world and shows our commitment to ensure that the telecom sector is prepared to address any cyber threat. We commend the Ministry of Information Technology & Telecommunication (MoITT) for taking lead on this important issue by publishing National Cyber Security Policy 2021, and we are confident that this strategy will help protect Telecom Sector's digital infrastructure and telecom users in line with the said policy.

Executive Summary

The Cyber Security Strategy for Pakistan's Telecom Sector provides a strategic framework and road map for the implementation of National Cyber Security Policy - 2021 during the next five (05) years (2023-2028).

This strategy comprises six (06) pillars, each of which addresses a distinct area of cyber security. PTA's efforts will be added to each pillar throughout this tenure following a year-on-year incremental approach to improve overall cyber security posture of Pakistan's Telecom Sector. The strategy's foundation is a multi-stakeholder approach, involving the public/ private sectors, peer regulators, telecom operators, private security firms, academia, and civil society in active collaboration.

Following are the **PILLARS** of this Strategy**:**

a. **Legal framework.** To provide legal and regulatory cover to all our efforts, which includes but not limited to:
   (1) PTA's Critical Telecom Data and Security Regulations - 2020 (CTDISR).
   (2) Pakistan's Cyber Security Policy - 2021
   (3) PTA's Cyber Security Framework - 2022

b. **Cyber Resilience.** To defend Critical Telecom Infrastructure (CTI) and Critical Telecom Data (CTD) by employing defense in depth and zero trust model.

c. **Proactive Monitoring & Incident Response.** To defend collectively and generate a synergized aggregated response of the Telecom Sector as a whole to ward off any cyber-attack.

d. **Capacity Building.** With the help of:
   (1) International subject experts.
   (2) Local technical resources.
   (3) Academia.

e. **Cooperation & Collaboration with**:
   (1) International Organizations.
   (2) National CERT.
   (3) Other Sector Regulators.
   (4) Local Intellect.
   (5) Academia.

f. **Awareness Trainings.** At the level of:
   (1) Organizational.
   (2) End User.

CHAPTER 1

National Telecom Cyber Security Strategy

1.1. Introduction

Cyberattacks, with various motives, have increased in complexity due to exponential digitization, technological innovations and ever-expanding cyberattack surface. Cyberattacks have evolved from commodity malware, insider threats, crimeware, exploits, hacktivism and terrorism – to increasingly complex coordinated multipronged state-sponsored attacks aimed at disrupting the national critical infrastructure of victim states. Therefore, proactive cyber security measures to improve the resilience of Critical Information Infrastructures (CII) have become common security need of all nations' industrial sectors, and their operators since disconnected silos of prevention/ monitoring or investigation technologies fall short in generating required results.

The recent years have witnessed a wave of major security breaches that have revealed vulnerabilities in both sophisticated international and national networks. The likes of SolarWind, Microsoft Exchange and Moveit exploits serve as stark reminders, breaching even the most advanced layers of security and propagating on a broad scale. A recent addition to these is the access of hackers to sophisticated AI tools such as ChatGPT or its malicious variants such as WormGPT or FraudGPT, the use of which can enable even script kiddies to create sophisticated payloads to successfully breach multilayered cyber defense. Over the past decade, Pakistan has found itself on the receiving end of comparable state-sponsored cyberattacks.

This is of significant concern, especially considering Pakistan's low standing in global cyber security rankings, which renders the nation susceptible to its adversaries aiming to disrupt national stability. These cybersecurity threats are not simply a challenge to our digital networks; they pose a profound risk to our national security, economy, and social fabric.

The Cyber Security Strategy for the Telecom Sector seeks to ensure the security and resilience of the telecom sector in the face of ever-evolving cyber threats. It outlines various challenges and opportunities associated with the protection of critical telecom infrastructure and provides a framework for collaborative action to address these challenges. The strategy emphasizes the need for a risk-based, integrated approach to cyber security, and identifies key action areas including risk management and governance, cyber defense and incident response, research and development, and public-private partnerships. Through this approach, the strategy seeks to ensure the security of the telecom sector and ensures continued operation of its vital services.

1.2. Vision

This strategy is envisioned to create a secure, resilient, and trusted digital ecosystem for Pakistan's Telecom Sector. This will not only empower our users and businesses to harness the opportunities of the digital age without any interruption but will also protect the telecom sector from the risks associated with cyber threats. PTA strives to build a secure and reliable digital infrastructure with robust and effective measures to protect our

citizens' data and privacy and to prevent disruptive cyberattacks. This effort ensures the confidentiality, integrity, and availability of information.

This vision emphasizes the importance of maintaining the availability of Critical Information Infrastructure (CII) in the face of cyber threats in order to ensure that businesses and telecom users in Pakistan can continue to rely on secure and uninterrupted access to digital services. Additionally, this vision promotes trust, innovation, and economic growth in the digital world, which are essential for the continuous development and prosperity of our nation.

1.3. Aim

This strategy aims to strengthen the ability of the Pakistan Telecom Sector to protect itself from cyber threats and reduce the potential impact of cyberattacks on Pakistan's national security, economy and public services. It sets out several measures to protect Pakistan from cyber threats, including improving cyber security awareness and education, investing in cyber security research and development, and collaborating with a range of partners, both in the public and private sectors.

This strategy further aims at ensuring that critical telecom infrastructure is resilient to cyberattacks even during adverse circumstances, i.e. telecom services are functional/ available and integrity of telecom data is made certain. The National Telecom Cyber Security Strategy (NTCSS) also aims to support the creation and implementation of a comprehensive cyber security framework that will ensure the resilience and protection of telecom infrastructure and services. This will include measures to strengthen the security of networks and systems, improve access control, enhance the security of data and transactions, and ensure compliance with applicable regulations and standards.

1.4. Scope

a. This strategy applies to all PTA licensees (Cellular Mobile Operators, Fixed Local Loop, Long Distance & International, Wireless Local Loop etc), Class Licensing and Registration holders, Telecom Infrastructure Providers, Telecom Towers licenses, Manufacturing license holders, Internet Services Providers etc.

b. PTA, while defending its internal ICT infrastructure, will function as cyber security enforcement and coordinating center for implementing this strategy.

c. PTA will also serve as a bridge between government-level bodies (such as the National Cyber Security Authority and National Computer Emergency Response Team) and its licensees to enhance the national cyber security posture.

d. Many steps planned in this strategy will only be effective if these are harmonized at a national level, so similar initiatives are expected at the national and other sectoral levels to synergize the cyber security efforts at the national level. PTA will collaborate with all other stakeholders to strengthen the cyber security at national level.

e. The strategy also covers steps planned at various areas of focus, such as security of critical assets and ICT systems of licensees; maintaining confidentiality, integrity and availability of customer and

internal data in transmission, storage, and processing; and establishing organizational framework/guidelines for strategy implementation and governance mechanisms.

1.5. Broad Contours of the Strategy

a. Every Licensee to devise and maintain an independent, fool-proof and multi-layer defense considering whole environment around it as hostile and compromised.

b. The strength of a chain is measured by the weakest link. Therefore, as every organization strengthens its defense, it should keep an eye on the threats emanating from other members' infrastructure due to weak or compromised controls in order to keep their environment safe. A vulnerability at one end may weaken the sector as a whole. Critical review, innovation and coordination are necessary in building a holistic sum secure, which would be stronger than its units.

c. A well-synergized response to any incidence coordinated at the PTA level is necessary to effectively block any attempt to compromise the cyber security of the telecom sector.

d. While no defense is invincible and there is always room for refinement, a culture of continuous improvement is indispensable. This involves a steady process of risk analysis, patching vulnerabilities with effective controls, identifying residual gaps through a robust audit system, and conducting periodic, non-intrusive vulnerability assessments and penetration testing.

e. Cultivating a culture of healthy competition where companies feel proud of their efforts and strive to take the lead over others.

1.6. Objectives

a. Building a strong team of cyber security professionals with continued skill-set development to steer this vision to reality.

b. Fostering a sector-wide cyber security culture in the telecom industry, where everyone is thinking and performing its duties with cyber security in mind. It will require continuous awareness, training, cyber drills, audits, healthy competitions and an effective award-reward mechanism. Continuous risk analysis and management to cater for the dynamic nature of technological developments, threats and techniques which are introducing novel vulnerabilities each day.

c. Devising a resilient defense against all kinds of cyber threats identified through risk analysis to protect their critical infrastructure and data by employing a layered defense-in-depth model.

d. Proactive monitoring of critical telecom infrastructure against all kinds of cyber threats and taking steps to prevent them from escalating into incidents. Minimizing surprise while having a holistic view of the complete telecom sector's infrastructure to maintain a balance and generate an effective response.

e. Timely detection of all cyber security incidences and not leaving the adversaries with any chance to compromise critical telecom infrastructure.

f. A well-coordinated and synergized response to all kinds of cyber incidences to minimize their effect. The whole telecom sector needs to react as one single 'unit' to generate a full-blown effective response to every such incidence with a view to making cyberattacks economically and politically

unfeasible. The aim is to maintain business continuity at all costs with a minimum impact on the services being delivered to the citizens of Pakistan.

g. Create a nationwide culture of cyber security through mass communication awareness and education programs.

CHAPTER 2

Legal framework for Cyber Security

2.1. Existing Legal Frameworks

Various steps to address the cyber security legislative framework have been initiated by federal and provincial bodies and sectoral regulators under the enactments. Key legal instruments related to cyber security in Pakistan are as under:

a. **Computer Emergency Response Team Rules - 2023 (CERT)**. Promulgated by Federal Government in pursuant to section 51 read with section 49 of PECA and National Cyber Security Policy - 2021.
b. **Critical Telecom Data and Infrastructure Security Regulations - 2020 (CTDISR).** The CTDISR-2020 is a set of regulations issued by PTA that requires licensees to implement measures for the detection, prevention, and response to cyber threats.
c. **Electronic Transaction Ordinance - 2020 (ETO).** Covering only electronic financial transactions and records.
d. **Investigation for Fair Trail Act - 2013 (IFTA**). Investigation for collection of evidence by means of modern techniques and devices to prevent and effectively deal with scheduled offences and to regulate the powers of the law enforcement and intelligence agencies and for matters connected therewith or ancillary thereto.
e. **National Cyber Security Policy - 2021.** The NCSP-2021 is a policy document that provides a comprehensive framework for ensuring cybersecurity in Pakistan. It delineates the roles and responsibilities of various government and private sector stakeholders, including PTA, in ensuring cybersecurity in the country.
f. **National Cyber Security Framework for Telecom Sector – 2022.** The NCSF-2022 for Telecom Sector is a framework document that provides guidelines for implementing cybersecurity measures in the telecom sector. The framework is expected to facilitate the development of a secure and resilient digital ecosystem in Pakistan.
g. **Prevention of Electronic Crimes Act - 2016.** Preventing unauthorized acts with respect to information systems and provide for related offences as well as mechanisms for their investigation, prosecution, trial and international cooperation with respect thereof and for the matter connected therewith or ancillary thereto.

Compliance with these legal instruments play pivotal role to ensure effective control on cyber security related issues in the telecom sector. PTA's licensees are required to comply with the relevant provisions of these legal instruments to maintain a robust and effective cyber security posture.

2.2. Formulating a High-Powered Steering Committee/Task Force to Oversee the Implementation of the Strategy

To ensure that cyber security objectives and expected outcomes are achieved, an industry-wide high-powered Telecom Cybersecurity Task Force (TCSTF), comprising CISOs of all major telecom operators, would be formed with the approval of the Authority to oversee the progress on implementation of this strategy. The task force would hold monthly meetings to track the progress of the initiatives and identify/mitigate any hurdles along the way. Each domain under this strategy will be transformed into the Key Performance Indicator (KPI) to be

assigned to the telecom operators and this task force will evaluate their progress. Similarly, all members will be made responsible/ accountable for the implementation of the initiatives under this strategy and will be expected to coordinate their efforts with relevant stakeholders as a part of the implementation process. This will not only provide a platform to collaborate at industry level, but will make the industry a shareholder in responsibilities.

2.3. Formulating New Regulations and Uplifting Existing Cyber Security Regulations

PTA has already published the Critical Telecom Data and Infrastructure Security Regulations - 2020 (CTDISR), which are in effect since November 2020. To ensure that telecom operators can plan well and allocate requisite budget/resources, a grace period of one year was granted to implement the controls as defined in CTDISR. To ensure compliance with transparency, the telecom licensees have been mandated to conduct third-party audits from PTA's approved audit firms.

Subsequently, PTA formulated Cyber Security Audit Criteria, after consultation with the industry, to standardize the audit process. PTA plans to further improve this criterion and introduce certain provisions to ensure maximum participation.

Foremost among the new regulations that need to be implemented is the Data Protection Regulations/Directives for telecom sector after the enactment of National Data Protection Bill. PTA recognizes the importance of this bill and may develop necessary regulations and frameworks to implement it. The goal is to ensure that the regulations sufficiently protect users' data and critical telecom infrastructure while also facilitating innovation and technological adoption.

Furthermore, CERT rules have also been promulgated by MoITT for the purpose to facilitate hierarchical monitoring and response mechanisms at the national level. These efforts are aimed at strengthening the cybersecurity landscape of the country and ensuring the safe and secure use of digital technologies by all stakeholders. PTA is also intending to look into other multi-dimensional approaches to take more effective steps related to cyber security such as eSIM/iSIM. In addition, the IP/VPN whitelisting, IXP, NTP etc. are also under consideration.

2.4. Improvising Existing Cyber Security Framework and Introducing New Frameworks to meet Challenges in Ever-growing Evolving Cyber Space

To ensure that PTA's Cyber Security Regulations (CTDISR) are uniformly implemented across the board, PTA released the "National Cyber Security Framework for Telecom Sector" in June 2022. The framework is based on CTDISR and defines the obligation of auditors and licensees. This includes interpretation and supporting documents *(technical aspects*) against each clause along with necessary compensating controls. Additionally, all controls have been classified based on Control Levels (CL1 to CL3), CL1 being the basic and CL3 as advanced security control, with continuous improvements following their degree of criticality.

PTA, as part of this strategy, plans to improve the framework with continuous feedback from the industry and academia. It is also considering the latest technological advancements to ensure that the framework is in line with the best security practices and future developments. Similarly, PTA also plans to map the control levels

defined in the framework corresponding to the categories of telecom operators. The telecom operators have been classified (Cat1 to Cat5) through various factors such as the number of subscribers, number of licenses, types of licenses, size of the network, and revenue etc. Similarly, PTA plans to formulate a baseline cyber security framework for manufacturers and importers of Smart Devices (IoT) in the light of regulations to be introduced for such devices. The requirements would ensure a balance between security and usability and would include security controls such as patch management, authentication strength, data transparency/security, and cyber-attack resilience, etc.

PTA has taken various initiatives, including security hardening of the telecom infrastructure of its operators, and taking steps for blocking the websites and social media platforms/groups involved in the infringement of personal information etc. These actions aim to protect the telecom users' data. Additionally, PTA is collaborating with the MoITT in pursuing enactment of the Data Protection law, which is currently in the consultation phase. Moreover, PTA is also working with the Ministry of Interior to devise a secure mechanism for acquisition and handling of users' data by law enforcement agencies used during investigations.

2.5. Formulating a Unified Cyber Security Framework with Multi-stakeholder Collaboration

Several sectors such as Energy, Financial, Manufacturing Industry, Transport, Postal, National Digital Database/Identity, and Health etc. are operating in silos and have formulated regulations and frameworks specific to their licensees and constituencies. For instance, the State Bank of Pakistan issued a detailed policy on "Information Technology Governance & Risk Management in Financial Institutions" that covers various aspects such as reviewing the effectiveness of information security programs on annual basis, formulation of cyber security action plans to anticipate/ withstand/ detect/ respond to attacks, and establishing cyber security awareness program etc. SBP also conducts audits of their licensees on annual basis. Other regulators are also in process of devising their cyber security regulations. There is, however, a need to standardize these regulations/ frameworks to avoid duplications/ contradictions. It is important to achieve a unified and standardized cyber security framework across all the sectors, thereby improving the national security. PTA is not only taking a lead in devising all necessary cyber security related frameworks for the telecom sector, but is also engaged with peer regulators such as **State Bank of Pakistan (SBP)**, **National Electric Power Regulatory Authority (NEPRA)**, **National Database Registration Authority (NADRA)**, **Security & Exchange Commission of Pakistan (SECP)**, **Competition Commission of Pakistan (CCP)** etc., for standardization of these regulations/ frameworks. PTA has signed Memorandum of Understanding (**MoUs**) with most of these regulators to work jointly in the area of cyber security and mutually share information. Similarly, several telecom operators are licensees of other regulators as well for variety of services and are following multiple security guidelines as per their license agreements. Hence a unified framework is important to avoid duplication of efforts causing compliance fatigue.

2.6. Introducing Regulations to Improve Privacy of Users

In this digital age, PTA considers users' privacy of paramount importance. For this reason, licensees are required to explicitly communicate privacy policy at the time of onboarding customers such as during the issuance of SIM cards, establishment of Internet connections, and enrollment of corporate customers etc. Licensees are being

made responsible to disseminate the privacy policy to all customers through SMS, email, and recorded phone call etc. The privacy policy should state the type of data to be collected, reason for collection, retention policy, usage policy and right to be forgotten. Similarly, any changes in privacy policy should be communicated to all customers. PTA, in consultation with its operators, plans to keep improving these regulations owing to ever evolving nature of digital world. This would include, but not limited to, the regulations related to the confidentiality during human-to-machine and machine-to-machine communication e.g. IoT devices and users connecting to publicly accessible Wi-Fi networks.

Similarly, PTA will also explore avenues to formulate privacy regulations to shield various metadata from threat actors. Several initiatives, such as the EU ePrivacy Directive etc, are there to achieve the same effect. Metadata can be used to co-relate user activities and can directly affect the privacy of users. Hence, such data must be anonymized or removed, in case permission was not explicitly granted by the user. PTA has taken several initiatives to prevent users from being spammed. Moreover, the regulator will also explore avenues to further tighten the grip to disallow sending of unsolicited electronic communications such as emails, messages, auto-dialed phone calls etc.

2.7. Conducting Cyber Security Audits/Inspections for Licensees and Publishing Cyber Security Metrics

To ensure compliance against CTDISR, upon completion of third-party assessment from PTA's approved audit firms, PTA conducts a validation audit of the licensees to ensure quality of the audit. PTA in 2022, conducted validation audits of the top 15 operators based on their customer-base, size of the network, license types etc. Due to the large number of licensees, it is not possible to conduct validation audits of every licensee every year. Hence, PTA plans to build a risk scoring mechanism based on various factors such as threat intelligence, results from external vulnerability assessments, participation in National Telecom CERT (nTCERT) and conducting surprise audits and inspections etc. Telecom operators are required to share PTA's audit report with their board of directors and provide timeline for compliance against the observations highlighted. A confirmatory visit of PTA team may be performed to validate the compliance.

PTA has started publishing Annual Cyber Security Report which includes detailed compliance level, strong/ weak areas observed during audits, and overall cyber security ranking as per CTDISR compliance matrix. The annual report is published on PTA's website after the completion of each audit cycle. This not only introduces healthy competition among the telecom operators, but also ensures transparency to their customers regarding the importance their service provider places on the security of their privacy/data. This will allow customers to make their choice based on the priority that a Telecom Operator is giving to the cyber security of its critical infrastructure and the protection of personal data of its customers.

2.8. Risk Management through National Telecom Risk Register

PTA is taking steps to further safeguard the telecom industry in Pakistan. As a part of these efforts, PTA will develop a National Telecom Sector Risk Register, which will give a comprehensive oversight into the cyber security challenges being faced by the telecom sector. This register will not only detail the risks but also suggest

strategies for prioritizing and mitigating them. Instead of relying on a conventional scoring mechanism, PTA will establish an automated system to classify risks based on their actual business impact. Furthermore, PTA will introduce risk-based auditing approach, encouraging all 3rd party audit firms to adopt this method.

CHAPTER 3

Cyber Resilience

3.1. Resilient Cyber Security Architecture for Critical Telecom Infrastructure

PTA will take necessary measures to ensure that the Critical Telecom Infrastructure (CTI) is resilient against cyberattacks. In other words, in case of adverse circumstances, the systems will continue to operate and function smoothly. In response to sophisticated security threats, PTA will work jointly with the industry to spot and implement advance technologies/techniques that can be applied to protect and defend Critical Telecom Infrastructure.

Special consideration is to be given to eliminating the use of legacy devices and software in CTI and implementing necessary compensating controls in case legacy devices/software are required for some time. PTA will encourage the diversification of technologies and components that power the infrastructure, etc., with a mix and match of platforms and vendors to achieve defense in depth while ensuring interoperability.

To transfer the advantages of the cyber security policies and operations, PTA will work with the telecom industry to ensure the continuity of vital business processes.

3.2. Establishing Internet Resilience

Currently, a significant number of Pakistani domains under the .pk Top Level Domain (TLD) are resolved and hosted outside of Pakistan. This is especially concerning for government domains; although most are registered under the .pk TLD, the majority of their servers are located abroad. In adverse situations, access to these servers could be compromised, potentially disrupting the availability of essential services. To address this vulnerability, PTA intends to assess the dependencies of the Critical Information Infrastructure on external elements, including domain resolution, routing, and more. PTA is dedicated to strengthening the resilience and redundancy of internet-driven resources, ensuring that national critical services remain accessible even under adverse circumstances.

3.3. Implementation of Zero-Trust Model for the Telecom Sector

The threat landscape is evolving, and traditional perimeter-based security architectures are unable to cater for complex attacks. The zero-trust model works on the presumption that all users are untrusted, and the attacker is already inside the network. In other words, there is no well-defined external or internal network boundary, and all users accessing systems are subject to access control divisions built around identity and context-aware access management. This may involve attributes such as device versions, network locations, IP reputation etc. Similarly, access to information is provided on a “Need to Know” basis and the least privilege principle.

Hence, PTA, with the help of Telecom Cyber Security Task Force, will explore ways for implementing Zero-Trust Model across the industry in the light of NIST SP 800-207 and other reference implementations. During initial

phases, the model would be replicated on large-size Telecom Operators and gradually would be enforced across other licensees as well.

3.4. Encouraging Emerging Technologies to Safeguard Cyber Risk Landscape, Evolving Threats and Proactively Implement Countermeasures

PTA is strategizing to expedite the evolution of next-generation telecommunication infrastructure. In collaboration with the MoITT and its network operators, PTA is working towards the swift deployment of 5G services in Pakistan. Along with this roll out, PTA is working proactively to ensure the security of 5G network infrastructure, mitigating threats to the allied services enabling Internet of Things (IoT), the machine-to-machine economy, autonomous driving, and Industry 4.0/5.0, etc.

Understanding the potential risks to the telecom sector due to the reliance on emerging technologies and digital transformation is a primary focus at PTA. To this end, a comprehensive assessment of critical telecom infrastructure, their interdependencies, and the supply chain is underway to minimize inherent risks.

In addition, PTA aims to grasp the intricacies of nascent digital technologies like IoT, artificial intelligence, and blockchain etc. Armed with this knowledge, it will partner with relevant stakeholders to formulate/review necessary guidelines and procedures to expedite their adoption. These will address cyber threats by integrating security principles, such as secure design by default, supply chain security, and incident management during the deployment of these technologies.

Recognizing the inherent vulnerabilities of mass IoT adoption, PTA will engage with researchers, manufacturers, and other relevant stakeholders to reduce these risks. Necessary safeguards will be included in the cybersecurity frameworks to tackle associated challenges.

5G is foreseen to be instrumental in enabling emerging technologies, including blockchain-based applications. PTA will explore the use of blockchain-based solutions and smart contracts to ensure the foolproof integrity of information. Prospects such as the deployment of blockchain across Pakistan Mobile Data (PMD) to streamline processes, smart contracts for Mobile Number Portability (MNP) and Service Level Agreement (SLA) monitoring, and smart contracts for roaming management and automatic dispute settlement will be considered.

The PTA will also support the adoption of eSIM/iSIM, given their crucial role in facilitating IoT and machine-to-machine connectivity. Moreover, it will support the introduction of upcoming protocols like LTE-M and NB-IoT while emphasizing the importance of their security features and safeguards. The potential of AI in detecting suspicious activities and preventing fraud will be investigated, with special attention given to the use of AI/ML for the detection of grey traffic.

3.5. Ensuring Localization of Critical Telecom Users' Data

PTA believes in the free flow of data; however, Critical Telecom Data (CTD), as defined in the PTA's Cyber Security Framework - 2022, needs to reside within the geographical boundaries of Pakistan as per the obligations under CTDISR and operators' licenses. The term CTD refers to confidential and personal data related to PTA licensees, users/customers, sensitive data belonging to government institutions, and such information which is critical for the operations/ confidentiality/ security of the Telecom Operators' systems including voice/data

communication of their users/customers etc. Furthermore, any data that can result in a financial loss and impede organizations from performing their duties, cause a major loss of competitive ability or a combination thereof, can also be classified as CTD.

The localization would only be limited to Personal Identifiable Information (PII) and CTD, whereas free flow of the rest of the data will be allowed. Similarly, the data localization policy will be aligned with the "**Data Protection Bill/ACT**" and "**Cloud Policy**".

CHAPTER 4

Capacity Building

4.1. Building Skilled Cyber Security Workforce

A technically skilled workforce, supported by innovative research and development, is fundamental to Pakistan's ability to develop innovative self-reliant solutions to emerging cybersecurity challenges. This priority covers initiatives to build and retain this expertise and to harness the resources for collaborating with academia and relevant stakeholders. PTA, in collaboration with all stakeholders, is already contributing and will expedite progress in the following initiatives:

a. Encouraging and formulating necessary benchmarks to ensure that skillset (international certification, international/ national level contribution/ achievement, international/ national cyber security event e.g. Hackathon etc., on-job achievements, and freelance profile etc.) is given due weightage along with the mandatory academic qualifications and degrees.

b. Creating opportunities for imparting relevant skills by playing an active role in cyber security activities, such as Hackathons, Capture the Flag Challenges, hands-on workshops through public-private partnerships, and collaboration with academia and the international community in organizing on-demand trainings/ workshops. PTA has been very active in organizing such events in past.

c. Devising recruitment and retention strategies aimed at ensuring a sufficient level of cyber security expertise internally for the telecom sector.

d. Working with academia, HEC and PEC in bridging the gap between curriculum and the industry need. PTA will facilitate the grooming of young graduates by arranging internships/ workshops/ visits/ awareness sessions in partnership with the telecom industry. These initiatives will provide students with meaningful practical experience while preparing them with the necessary knowledge and skills to meet the needs of the fast-evolving cyber landscape.

4.2. Managing Brain Drain by Building Talent Pool

Given the increasing global demand for cybersecurity professionals, Pakistan is experiencing a brain drain. It's imperative to foster talent pools and create an environment conducive to retaining skilled professionals within the country. This ensures that we have ample talent to meet the industry's needs. To tackle this challenge, PTA will collaborate with key stakeholders such as industry experts, academia, and government organizations. Their joint efforts will focus on building domestic talent pipelines through professional training. Additionally, to enhance retention, it's crucial for the industry to offer competitive packages and job security that are at par with international standards. PTA has recently reorganized its Cyber Security Directorate with positions at a competitive or higher package than the industry to encourage talented resources. PTA has also directed all its licensees to setup a dedicated CISO office with necessary manpower and appointment of a C-level security officer (CISO) to ensure due importance to the cyber security in their organization and to improve recruitment/retention of talented cyber security resources.

4.3. Women's Inclusion in Cyber Security Initiatives

PTA has always championed diversity in job roles and promotions with an aim of increasing female participation in all walks of life. Cyber security is no exception to this commitment. To materialize this vision, PTA has been encouraging selection of talented female cybersecurity specialists and will continue this policy in the future. The same is expected from the telecom industry as the nature of the job and the location of their offices provide a conducive environment for women to work side-by-side with male experts. The objective is to elevate cybersecurity awareness among women and motivate them to embrace roles as cyber security professionals.

4.4. Trainings with International Organizations

PTA has been collaborating with various international organizations (APNIC, ISOC, ICANN, ITU, NCSC, and ISACA etc.) for the training of technical resources of telecom sector in Pakistan. These include trainings on IXP, DNS Security, Routing Security, and IPv6 etc. These trainings are free for telecom operators and maximum participation is **encouraged** to include at least one member from all major operators. PTA is in touch with these organizations and international vendors (MasterCard, Huawei, Fortinet, GroupIB, CISCO, Meta and Microsoft etc.) to arrange more trainings in the future as well, which include but not limited to the following areas:

a. Routing and Switching training.
b. SOC fundamentals, installation and operations.
c. SOC analyst training.
d. Threat Intelligence: concept, installation, integration and operations.
e. Incident response.
f. Vulnerability assessment and penetration testing.
g. IPv6.
h. DNS Security.
i. Routing security.
j. Non-intrusive scan of public facing interfaces and their hardening.
k. Cyber security frameworks and audit techniques.
l. Risk assessment and control implementation.
m. Financial frauds and social engineering.

4.5. Paid Professional Trainings

CVD, in collaboration with HR Directorate, is arranging professional trainings for its cyber security and IT resources for their technical grooming and preparing them to attain maximum level in relevant international certifications. Some of the trainings include:

a. CISA.
b. CISM.
c. CISSP.
d. SOC analyst.
e. Incident responder.
f. Ethical hacking/ Ethical forensics.
g. Web application vulnerability assessment.

All telecom operators are also expected to arrange professional trainings for their technical resources and encourage them to acquire maximum relevant international certifications in their areas. Besides

these, PTA will also organize professional trainings utilizing the forum of nTCERT through its vendors and international collaborators, such as National CERT, APCERT, FEMA, Malaysia CERT, FIRST etc.

CHAPTER 5

Cooperation, Collaborations and Partnerships

5.1. Fostering Collaboration

PTA believes in collaboration at every level and fosters collective wisdom to devise its regulations/frameworks/guidelines/SOPs. As a normal modus operandi, all the regulations are normally shared with the industry as part of joint consultation process during their inception. Similarly, ministries and other government organizations are consulted on various matters as and when required. At a peer level, PTA remains in constant interaction with the other sectoral authorities/regulators for collaboration in the areas of mutual interest. PTA has recently signed a number of Memorandums of Understanding (MoU) with other sectoral regulators, such as CCP, NADRA, NEPRA, SBP, SECP, etc. to collaborate in various areas of interest. All government policies received from the ministries are also shared with the telecom operators for their feedback. Besides these, PTA is pursuing collaboration in the following areas:

a. Collaborate with international partners like ITU-IMPACT and others to build a more secure and resilient global digital landscape.

b. Maintain a continuous presence and provide professional input to all major global and regional organizations and professional bodies related to cyber security, including ICANN, GAC, ITU, APT, and other UN and non-UN organizations.

c. Affiliation with all national, regional, and international bodies to establish desired coordination and cooperation to establish cyber situational awareness.

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

5.2. Collaboration with Telecom Operators

PTA has established National Telecom Security Operation Center (nTSOC) to connect and work collaboratively with all telecom operators and private sector security companies by sharing cyber incidents, securing critical data and infrastructures and exchanging intelligence on potential threats. PTA, in collaboration with TCSTF, is working on devising SOPs for the joint operation of nTSOC with all the connected SOCs of its operators to synergize efforts at telecom sector level. This includes SOPs for 24/7 manning of SOCs, incident sharing and escalation mechanisms, Threat Intelligence Sharing Mechanism, incident handling and coordination, Post-incident Forensic Analysis and Reporting, and cyber drills. PTA is also working with TCSTF to identify and arrange trainings for cyber security resources at the telecom sector level.

5.3. Collaboration with other Regulators & Sectoral CERTS

There is a need to improve inter-sectoral collaboration between PTA and SBP, NEPRA, NADRA, PEMRA, SECP etc. so as to lessen the hurdle in proactively detecting and responding to security threats and incidents.

5.4. Collaboration with Global CERTS for Threat Intelligence Sharing

PTA will engage with Global CERTS through National CERT and actively participate and collaborate with fora such as FIRST, APCERT, and European Union Agency for Cyber Security (ENISA) etc. Similarly, PTA also actively seeks to collaborate with the relevant agencies in the areas of policy formulation and governance to regularly update its regulations in order to keep them in line with the world best practices.

5.5. Engage in Regional Cyber Security Fora with a Focus on Capacity Building

PTA is continuously involved in the cyber security confidence-building measures at international and regional level, where it actively puts forward its position regarding the applicability of upcoming cyber policies. Besides this, PTA has been engaged with various international cyber security fora to acquire free trainings for the cyber security resources of telecom sector. There have been numerous engagements in the past, which will continue in the future in order to build a strong cyber security team at national and telecom sector level.

5.6. Bilateral/ Multilateral Cooperation

PTA will be pursuing an active approach to international engagement on cyber security through networking/ agreements with key allies and other eminent nations to strengthen cooperation on cyber security. PTA's cyber security team would engage with the international community through active participation in global security conferences and will partner with the private sector to organize international cyber security conferences.

To enhance bilateral and regional cooperation on capacity building, involving international partners, the private sector and civil society is expected to unlock the true potential and ensure the secure transition to the digitization age.

Bilateral and multilateral cooperation will result in a sustained improvement in cyber security in partner states. It will be possible to enshrine democratic and normative values and ideals worldwide. Consequently, cyber capacity building will increase overall global cyber security.

5.7. Collaboration with National Centre for Cyber Security (NCCS)

PTA recognizes the need for collaboration with academia and R&D centers to add innovation to its current and future initiatives. National Centre for Cyber Security (NCCS), a joint initiative of the Higher Education Commission (HEC) and Planning Commission, is an important player in the development and implementation of innovative ideas in Pakistan related to cyber security. PTA aims to collaborate with NCCS in various ways to strengthen cyber security capabilities. The Cyber Vigilance Division of PTA has been working closely with the NCCS Secretariat at Air University to identify areas where joint research and development efforts can be undertaken to improve cyber security of the telecom sector.

The collaboration between PTA and NCCS is an important step towards building a strong and resilient cyber security ecosystem in Pakistan.

CHAPTER 6
Security Monitoring & Incident Response

6.1. Continuous Monitoring – the Key to Cyber Resilience

One of the most important factors contributing to the success of a cyberattack is to achieve surprise over the victim, while maintaining balance remains the most crucial element of an effective defense. No defense is impregnable and a determined attacker will eventually breach it. While defense in depth provides necessary layering to give sufficient time to the defender to respond, effective monitoring and timely response are the two essentials that enable the defender to guard against and repulse any attack. SOC, a combination of SEIM, Threat Intelligence and SOAR, gives a defender 360-degree view of its critical infrastructure, mechanism to raise alerts to the relevant response team, and generate an effective auto/semi-auto response to ward off such threats. At second layer, a team of responders or Computer Incidence Response Team (CIRT) responds to a partially or fully successful compromise/breach in order to block further damage and restore the infrastructure into its original state while hardening the system once again more effectively based on the lessons learnt.

PTA has successfully established National Telecom SOC (nTSOC) to coordinate monitoring of critical telecom infrastructure in real-time and generating an effective synergized sector-wide response in the case of an identified cyberattack. As part of its activity 1, over 22 telecom operators' SOCs have successfully been integrated with the nTSOC. The SOC is still in a nascent phase, however, it is a continuous process of improvement which will go a long way to mature this concept.

6.2. Building and Promoting Home-Grown Indigenous Security Products & Solutions

With the collaboration of the private and public sectors' IT companies, PTA is pursuing the development of home-grown security tools with the ability to share threat data that can help security teams detect incidents across complex environments. This collaboration will not only strengthen our confidence by relying on the products with maximum low-level transparency, but will also give a chance to the local IT industry to produce products at par with the international key players, especially in the area of cyber security where we cannot totally rely on foreign products. Many banks and telecom operators are using indigenous cyber security products, encouraging local companies as a jump-up point to compete with international products worldwide.

PTA is already engaged with local partners in developing such products and with the continuous two-way engagement, will keep on improving these solutions to the point where these can be pitched against the best cyber security products of the world.

Similarly, when engaging foreign companies, preference will be given to the software developed as a joint venture with local companies deploying the solutions in a "Whitebox Model" i.e., the source code, configuration, design documents and non-disclosure agreement by both sides to safeguard the intellectual property of the industry on one side, and providing sufficient security assurance and transfer of technology to the country on the other side. PTA expects the same from telecom industry in order to encourage local IT industry and to start adopting home-grown trusted products with inside visibility.

6.3. Continuous Security Monitoring through National Telecom SOC

PTA has established National Telecom SOC (nTSOC) and National Telecom CERT (nTCERT), whereby all its operators' SOCs are being integrated to capture sector-wide cyber security picture, monitor the cyber health of telecom industry in real time and generate a synergized industry-wide response to any cyber-attack to mitigate its effect. PTA's vision and focus are to develop and operate nTSOC/ nTCERT using highly trusted indigenously built technology components which are resilient at the time of need, can be matured with future enhancements and can be tailored to specific security needs. PTA has established nTSOC in order to coordinate all efforts of securing critical telecom infrastructure (CTI) and making it resilient across nationwide telecom operators using trusted partnerships and cooperation amongst all public-private stakeholders. PTA plans to undertake the following steps as a part of this strategy:

a. Develop a unified platform for monitoring, analysis, orchestration and intelligence sharing of CTI through the integration of operators' SOC platforms.

b. Incorporate security monitoring solutions across prominent telecom operators to establish a consolidated security dashboard. This initiative will allow for real-time analysis of security alerts and foster efficient incident management.

c. Integrate the telecom sector's critical assets into a unified security monitoring platform. This platform will provide comprehensive oversight and facilitate proactive responses to potential threats.

d. Incorporate cyber Threat Intelligence (TI) platform/tools with selected global/local open source/ commercial TI feeds.

e. Develop Case Management Tools for industry regulatory compliance.

f. Build process/workflow automation tools where required.

g. Develop human capability, including skilled and certified workforce to manage SOC/CERT operations (L2/3 analysts, System/ NW experts for generating/coordinating response, Deep Analysis Team to conduct analysis of new threats with the help of threat hunting platforms and labs with academia and other relevant stakeholders for forensics and malware reverse engineering etc.).

h. Support small operators in deploying cost-effective security solutions to integrate their NWs with PTA's unified platforms and meet compliance

i. Ensure that nTSOC is interoperable, compatible, vendor agnostic and scalable to meet seamless integration, interoperability, manageability, and infrastructure/resource scalability requirements

6.4. Build Effective Response Using nTCERT

With access restricted to its licensees only, PTA inaugurated the Telecom CERT portal in March 2021 for point to point information sharing on emerging threats. The portal offers its licensees with latest cyber security alerts, advisories, and awareness infographics. Threat intelligence data and advisories specific to telecom sector are shared for compliance. The portal was followed by the launch of a public nTCERT website for raising awareness among telecom operators and the public on security alerts not restrictive in nature. The website contains the

latest security advisories and alerts for the public, awareness messages on the safe usage of Internet services, information on capacity-building initiatives and workshops etc. To enhance the capacity, capability and effectiveness of nTCERT, PTA will take the following steps:

a. Building an effective CERT with reactive and proactive parts (auto email/SMS sharing, real-time notifications, auto advisory attachments in incident forwarding, getting feedback on CTDISR Survey Form, statistics/graphs on available data, logging of user activities in portal etc.) and Integration with ticketing systems/service desk and CI/ CD pipeline for DevOps environment.

b. Build an emergency Incident Response Team (IRT) for Tier 3 expert responses for handling high level issues and to assist telecom operators in identifying, recovering and responding to high level security incidents affecting Critical Telecom Infrastructure (CTI).

c. Establishing effective collaboration with international CERTs through the National CERT for timely threats, advisories and experience sharing.

CHAPTER 7

Cyber Awareness for Developing National Culture

7.1. Increase Cybersecurity Awareness among General Public

To increase public awareness on responsible and safe usage of the Internet/social media, PTA regularly disseminates advisories, security alerts etc. through broadcast media, social media and short messages to all mobile users. More recently, PTA conducted a media campaign to raise awareness of Lost and Stolen Device System (LSDS), which has proven effective in reducing mobile snatching incidences. PTA has also leveraged social media in its campaigns to raise public awareness on fraud SMS and calls; reporting of unlawful online content; prohibition on import, sale, and use of GSM boosters, amplifiers, and repeaters; and the legality issues of providing internet services without a license. Similarly, in the case of cyber security, PTA is determined to take the following measures to increase the effect:

a. PTA will focus on imparting public awareness related to cyber incidents, their targets, processes and mitigations to mobile phone users. This will be achieved through digital fora, telecom operators sending alerts in direct messages, and other available sources.

b. PTA will expedite with the telecom operators to protect their respective cyberspace by maintaining the desired level of cyber security in their services to the customers.

c. Efforts will be directed towards incorporating cybersecurity awareness into the national educational curriculum for high schools and colleges, in collaboration with the Ministry of Information Technology and Telecommunication (MoITT), HEC, Federal and provincial education ministries.

d. PTA will collaborate with educational institutions to hold special awareness sessions on responsible use of the Internet/ social media, consequences of unlawful activities on the Internet/ social media platforms, especially concerning sensitive (sacrilegious/sectarian/indecent) content which can lead to real-world physical harm to the society.

e. Creating short videos (15 to 30 seconds) on safe, responsible, legitimate, and productive use of the Internet/ social media. The videos will be disseminated through electronic/ social media for public awareness.

f. Conducting seminars and training sessions in colleges/ universities to educate students regarding the challenges and opportunities provided by the Internet/ social media.

7.2. Provide Context-Aware Dynamic Risk Analysis & Incident Analysis

PTA will provide context-aware dynamic risk analysis to its operators for proactive implementation of necessary safeguards. Similarly, the PTA incident response team, based upon input from cyber incident investigation and R&D, will provide a “Post-Incident Analysis Report” to the Telecom Industry. This will allow the industry to proactively implement cyber defense to protect against similar cyberattacks.

7.3. Encourage Employee Awareness Programs & Collaboration of Learning Modules with the Telecom Industry & Academia

As the root cause for several compromises and incidents is related to Business Email Compromise (BEC), apart from implementing necessary security controls, employees' awareness at all levels is important. Hence, PTA will work with telecom operators and government organizations to introduce eLearning modules to train government/ private employees on cyber security knowledge. Employees' awareness programs will be made part of the Key Performance Indicators (KPI) at PTA and the same will be instructed to the telecom operators.

These training programs will be shared with the other sectors as well to raise awareness among their employees. Subsequently, PTA in collaboration with the relevant government organizations, industry and academia, will work on unifying various "eLearning Modules" as part of the employees' onboarding process and ensuring continuous participation by making them part of the KPI.

7.4. Extend Public Reskilling Efforts and Attracting Young Talent to Widen National Cyber Security Pool

PTA will focus on incorporating cyber security in the larger public reskilling efforts for widening the pool of the cyber security workforce. PTA will undertake the following steps in this regard:

a. Working with the MoITT, IGNITE, PSEB and academia to conduct specialized programs for capacity building of the telecom sector. The Government of Pakistan (GoP) is already concentrating on emerging technologies and their cyber security dimensions and leadership aspects.

b. Working with the GoP to formulate a structure to incentivize startups, academia, and Industry for developing home-grown cyber security products/solutions.

c. Working closely with IGNITE to facilitate creation of incubation centers to encourage investment/development in critical areas of cyber security.

d. Targeted campaigns and awareness programs to attract bright minds in cyber security and building structure for providing enticing career opportunities.

e. Work with academia and HEC to run programs and awareness campaigns for transitioning non-computer science graduates with an aptitude for cyber security.

CHAPTER 8

Summary and Conclusion

8.1. Summary

The National Telecom Cyber Security Strategy is an initiative to ensure the security and resilience of the telecom sector. It addresses the challenges posed by the increasing interconnectivity of telecom networks, the cyber threats they face, and the need to protect their data and customer information. The strategy focuses on areas, such as risk management and governance; cyber defense and incident response; research and development; and public-private partnerships.

It emphasizes the need for a comprehensive and integrated approach to cyber security across the telecom sector and lays out a framework for collaborative efforts to protect critical telecom infrastructure and services. The strategy also identifies key challenges and opportunities for the sector and provides a roadmap for action to ensure the security of the telecom sector.

The strategy also outlines several initiatives and activities that will be undertaken to help protect the national critical infrastructure. These include enhancing public-private partnerships, investing in research and development, and developing a unified national framework for cyber security. The strategy also calls for increased public awareness and education to help people recognize, prevent, and respond to cyber threats.

8.2. Expectations / Obligations from Telecom Sector

At a high level, following are the expectations from telecom companies to achieve the objectives of this strategy:

a. Telecom companies should ensure that all personnel are trained and educated on cyber security practices and procedures, especially on employees' responsibilities to ward off insider threats.

b. Telecom companies should ensure that their networks and systems are compliant with PTA's regulations and directives, especially to the CTDISR and Cyber Security Framework.

c. Telecom companies are obligated to ensure consistent monitoring and timely updates of their networks and systems to mitigate the risk of cyberattacks. This can be particularly achieved by establishing CERT/SOCs and facilitating round-the-clock monitoring. Employing skilled Level 1, 2, and 3 resources, alongside clearly defined processes, is paramount to this effort. Additionally, it is crucial for these companies to ensure the integration of their SOC with nTSOC, which will enable an effective, synergized response to any potential cyberattack. This proactive, unified approach is crucial for enhancing overall cyber resilience in the telecom sector.

d. Telecom companies must implement robust measures to protect customer data from unauthorized access. Prioritizing data privacy is essential to maintain trust among users.

e. Telecom companies should ensure that their systems are designed to detect and respond to cyber security incidents promptly.

f. Telecom companies should frequently assess their systems and networks to ensure that security flaws are identified and addressed. In this regard, they need to devise and practice a well-defined

three tier audit process, culminating in validation by the PTA cyber security team. The operators should approach this effort positively, cooperating with external teams to improve their security posture.

g. Telecom companies should collaborate with other organizations within the industry and PTA in sharing relevant information about cyber security threats and incidents. Instead of hiding cyber incidences, we should be working on a mutual-trust model to fight this menace jointly.

h. Telecom companies should provide customers with information about cyber security threats and how to protect themselves from such threats.

i. Last but not least, telecom companies need to devise their long term (strategic i.e. 3-5 years), medium term (2-3 years), and short term (yearly) plans to achieve the objectives defined in this strategy.

8.3. Conclusion

National Telecom Cyber Security Strategy stands as a robust and integrated blueprint aimed at fortifying the security and resilience of the telecom sector in Pakistan. This strategy not only charts the course of future actions but also discerns the challenges and opportunities that lie ahead. It underscores the importance of fostering collaborative efforts and public-private partnerships to safeguard our critical telecom infrastructure and services.

In an era marked by increasing cyber threats, this strategy is a pivotal initiative towards ensuring the security and stability of our telecom sector. It reaffirms the commitment to navigating the complex digital landscape, bolstering our defenses, and advancing our national interest in the digital realm.

This strategy embodies a commitment to maintaining the confidentiality, integrity and availability of our telecom services and sensitive data. It underscores the vision of a resilient and secure digital infrastructure, while fostering trust and confidence amongst citizens, businesses, and government entities alike. It paves the way for a future where our telecom sector continues to be an engine of growth, innovation and prosperity, maintaining security of its critical information infrastructure against the upcoming cyber threats of tomorrow.