Subject: **Cyber Security Advisory – Strengthening "Know Your Client (KYC) Processes for Cybersecurity Compliance and Threat Mitigation" (Advisory No. 20)**

Context. It has recently been observed that Critical Information Infrastructure (CII) sectors provide their Application Program Interface (API) services to other sectors as per client services requirements. However, in some cases the provided APIs remain vulnerable to potential Cyber-attacks and exploitation. Ensuring Cyber hygiene and strengthening client end process is a joint responsibility of API service provider and client. Best practices to regulate and ensure KYC have been highlighted in ensuing paras for compliance.

2. **KYC**. KYC is a regulatory process used to verify the identity, background and risk level of potential clients before entering into a business relationship. KYC is critical in ensuring the security and compliance of internet and telecommunication services. By enhancing KYC processes, ISPs and regulatory bodies can mitigate cyber threats, safeguard client information and maintain compliance with national regulations, thereby fostering a more secure and trustworthy digital ecosystem in Pakistan.

3. **Guidelines - KYC Implementation**. Following are few guidelines (but not limited to) for enhancing the KYC process in the telecommunication, internet and banking sectors:

a. **Ensure Robust Identity Verification Mechanisms**

(1) **Mandatory Client Verification**. Strong KYC protocols must be implemented, requiring verified identity documents (CNIC, passport etc) for all clients subscribing to telecommunication and internet services.

(2) **Digital Verification Systems**. Secure, automated identity verification technologies (e.g. biometric verification, real-time facial recognition) should be adopted to improve accuracy and reduce the risk of forged identities.

(3) **Re-verification for High-Risk Users**. User information must be reviewed and updated regularly, especially for high-risk accounts (e.g. users engaging in frequent international traffic, anonymous users or high-volume data users).

b. **Implement Enhanced Data Security and Privacy Measures**

(1) **Encryption of Client Data.** All KYC related data must be encrypted both at rest and in transit to prevent unauthorized access and data breaches.

(2) **Access Control**. Access to sensitive client information must be restricted to authorized personnel only, with Multi-Factor Authentication (MFA) implemented for administrative access to KYC databases.

c. **Continuous Monitoring and Cyber Threat Intelligence Integration**

(1) **Use Behaviour Monitoring**. Sophisticated and effective tools must be utilized to monitor user activity and flag anomalies that deviate from established usage patterns (e.g. unusual login locations, data spikes or suspicious communication patterns).

(2) **Risk Based Client Profiling**. Users must be classified into low, medium and high-risk categories, with high-risk clients undergoing enhanced due diligence (EDD), including in depth background checks and monitoring.

(3) **Collaboration with Cyber Threat Intelligence**. Threat intelligence sources should be integrated to proactively detect emerging cyber threats that may target clients or infrastructure (e.g. phishing, malware attacks).

d. **Protect Against KYC-Related Cyber Threats**

(1) **Phishing and Social Engineering Defences.** Awareness programs must be created for employees and clients to recognize and report phishing attempts and social engineering attacks aimed at stealing KYC information.

(2) **Incident Response Planning**. A comprehensive incident response plan focusing on KYC data breaches must be developed, including containment, root cause analysis, client notification and mitigation steps.

(3) **Regular Security Audits**. Third-party security audits must be conducted regularly on systems managing KYC data to identify vulnerabilities and compliance gaps.

e. **Support Customer Privacy and Trust**

(1) **Transparency in data collection**. The purpose and the scope of KYC data collection must be clearly communicated to clients, ensuring they understand how their data will be used, stored and protected.

(2) **Consent Based Data Collection**. Explicit consent from clients must be obtained before collecting or processing personal information, adhering to data privacy regulations.

(3) **Data Minimization**. Only essential KYC data required for identity verification and service provision should be collected, with excessive data collection avoided to minimize exposure to privacy risks.

f. **Address National Security and Cyber Threats, Proactively**

(1) **Prevent Anonymous Access**. Strict enforcement of KYC policies must be ensured to prevent anonymous access to internet services which can be exploited for cyberattacks, terrorism and disinformation campaigns.

(2) **Internet Shutdown Procedures**. During national security threats or unrest, collaboration with PTA must be ensured to lawfully implement internet shutdowns or monitoring measures, while maintaining transparent records of affected clients.

(3) **Content Monitoring and Regulation**. KYC data must be used to monitor and control access to illegal or harmful content as per PTA's guidelines, ensuring user activity aligns with Pakistan's cybersecurity objectives.