REGISTERED No. M - 302
L.-7646

The Gazette of Pakistan

EXTRAORDINARY
PUBLISHED BY AUTHORITY

ISLAMABAD, WEDNESDAY, NOVEMBER 18, 2020

PART II

Statutory Notifications (S. R. O.)

GOVERNMENT OF PAKISTAN

PAKISTAN TELECOMMUNICATION AUTHORITY

NOTIFICATION

Islamabad, the 8th September, 2020

S. R. O. 1226(I)/2020.—In exercise of the powers conferred by Clause (o) of sub-section (2) of Section 5 of the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996), the Pakistan Telecommunication Authority is pleased to make the following regulations:—

PART-I

PRELIMINARY

1. **Short title and commencement.—**(1) these regulations may be called the "Critical Telecom Data and Infrastructure Security Regulations, 2020".

(2) They shall come into force from the date of gazette notification.

2. **Definitions.—**(1) In these regulations, unless there is anything repugnant in the subject or context:

Price : Rs. 20.00

[6081(2020)/Ex. Gaz.]

(a) **"Act"** means the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996);

(b) **"Authority"** means the Pakistan Telecommunication Authority established under section 3 of the Act.

(c) **"Authorized officer"** means an officer to whom the Authority has entrusted to ensure compliance of these regulations.

(d) **"Computer Emergency Response Team (CERT)"** means a team composed primarily of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents related to telecom.

(e) **"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.

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

(g) **"Cybersecurity"** means proactive and reactive measures for the protection of critical data and infrastructure from attack, damage and unauthorized access.

(h) **"Cybersecurity Event"** means any act or attempt, either successful or unsuccessful, made to gain unauthorized access to, disrupt, or misuse a licensee's telecom electronic systems or data stored on such telecom systems.

(i) **"Cybersecurity Incident"** means a cybersecurity event which may adversely impact the availability, integrity and confidentiality of critical data related to telecom or provision of licensed telecom services.

(j) **"Data Breach"** means the intentional or unintentional release of information stored / managed by the telecom licensee, to an entity which is not authorized to access the same.

(k) **"Malware"** means malicious code which can be exploited to breach telecom computer systems / Networks.

(l) **"Personal Data"** means Information associated with an individual or an organization, relating to its private, public and professional identification.

For Example:

1. Name, father / mother name, address, photo / Logo, CNIC Number / Passport Number / Registration number

2. Call Data Record (CDR), IP address details, Social media accounts, Phone numbers, Website

3. NTN Number, PIN Code

(m) **"Secure Area"** means physical space / area used for housing critical telecom infrastructure.

(n) **"Threat"** means a potential cause of an unwanted incident which may cause harm to telecom critical data or infrastructure.

(o) **"Vulnerability"** means weakness which can be potentially exploited by one or more threats.

3. **Scope and Applicability.—**These Regulations shall apply to all PTA licensees for the security of critical telecom data and critical telecom infrastructure related to Telecom Sector, in accordance with the procedures specified in these Regulations.

PART-II

LICENSEE OBLIGATIONS

4. **Cybersecurity Framework.—**(1) Licensee shall constitute a steering committee comprising of high level representation from key operational areas, to govern and ensure implementation of Cybersecurity initiatives.

(2) Keeping in view the requirements of these regulations, necessary policies shall be defined, approved and communicated by the licensee to its employees and other stakeholders such as partners, contractors and any other entity having interface with its telecom data / infrastructure to ensure compliance of these regulations.

(3) The policies mentioned in point 4(2) shall be regularly reviewed by the licensee at planned intervals or upon any significant change / event.

(4) Roles and responsibilities for cybersecurity shall be clearly defined and allocated by the licensee.

(5) Critical data and Infrastructure shall be identified and designated by the licensee for ensuring cybersecurity.

(6) Licensee shall maintain appropriate contact with relevant stakeholders to ensure cybersecurity.

(7) Employees and contractors shall be contractually bound by the licensee to relevant cybersecurity requirements with a formal and communicated disciplinary process in place for compliance.

(8) To ensure proper implementation of security measures, employees including relevant contractors / partners shall be made aware by the licensee of the security policies and requirements through awareness sessions, education and trainings.

(9) Where applicable the licensee shall also provide Cybersecurity awareness to its customers / subscribers for safeguarding against security threats and incidents.

5. **Physical And Environmental Security.—**(1) Physical security for secure areas should be designed and implemented by the licensee.

(2) Security perimeters shall be defined by the licensee for secure areas.

(3) Physical access to assets at secure areas shall be managed and protected by the licensee.

(4) Only authorized personnel shall be provided access to secure areas.

(5) Licensee shall ensure that access points where unauthorized persons can enter secure area are be controlled and if possible isolated from CTI.

(6) Physical log book or electronic audit trail shall be maintained and monitored by the licensee for personnel accessing secure areas.

(7) The physical environment of secure areas shall have monitoring/ surveillance by the licensee to prevent and respond against a cybersecurity incident.

(8) Procedures for working in secure areas shall be designed and implemented to safeguard against cybersecurity incidents.

(9) Physical protection against natural disasters, hazards, malicious attack or accidents shall be designed and applied by the licensee for secure areas.

(10) Secure areas should be protected from power failures and other disruptions caused by failures in supporting utilities.

(11) Power and telecommunication cabling for CTI should be protected from interception, interference or damage.

(12) Maintenance for Equipment at secure areas shall be correctly carried out by the licensee for its availability and integrity.

(13) Appropriate protection shall be applied by the licensee at secure areas for unattended equipment to safeguard against unauthorized access.

(14) Assets pertaining to CTI should not be taken off-site without proper authorization

(15) Appropriate security shall be applied by the licensee to off-site CTI assets taking account risks outside the licensee's premises.

(16) Clear desk policy for papers and removable storage media and clear screen policy for critical data processing facilities shall be adopted by the licensee.

6. **Monitoring.—**(1)Automated network monitoring systems shall be put in place by the licensee to detect unauthorized / malicious users, connections, devices, and software with preventive action.

(2) Authority may issue guidelines/specifications for deployment, operations, management and access to information/logs of said Monitoring Systems.

(3) CTI shall be monitored to identify and prevent eavesdropping, unauthorized access and cyber threats.

(4) Licensee shall ensure that event logs for user activities, exceptions, faults and cybersecurity incidents are produced, stored and regularly reviewed to identify and mitigate security threats and incidents.

(5) Event logs should include the following when relevant:

i. User IDs

ii. Successful and rejected system access attempts

iii. System activities

iv. Use of system utilities and applications

v. Records of any transactions executed by users

vi. Data files accessed and kind of access

vii. Timestamp and details of key events

viii. Identity of device

ix. Location

x. Records of successful and rejected data and other resource access attempts

xi. System configuration changes

xii. Network addresses and protocols

xiii. Alarms raised by access control system

xiv. Activation and de-activation of protection systems such as Anti-Virus and Intrusion detection systems

(6) Logging facilities and log information shall be protected by the licensee against tampering and unauthorized access.

(7) Logs from multiple sensors and sources shall be aggregated and correlated by the licensee to understand attack targets and methods

(8) System administrators should not have permission to erase or de-activate logs of their own activities and controls should be in place to audit their activities.

(9) Clock synchronization shall be performed to ensure that clocks within an organization are synchronized to a single reference time.

(10) Vulnerability scans shall be carried out by the licensee to perform counter measures against vulnerabilities.

7. **Malware Protection.—**(1) Critical telecom infrastructure shall be protected against malware by the licensee.

(2) Automated malware protection shall be applied by the licensee to identify and eliminate malicious software activity.

(3) A policy shall be formulated and enforced by the licensee to prohibit the use of unlicensed and unauthorized software.

(4) A vulnerability management plan shall be developed and implemented by the licensee.

(5) For systems and software being used by the licensee, exploitation of related technical vulnerabilities shall be avoided by obtaining their information in a timely fashion and taking appropriate measures to address associated risks.

(6) A formal policy shall be formulated and enforced by the licensee to protect against risks associated with data and software obtained from external networks or any other medium.

(7) Employees shall be made aware through training and awareness sessions by the licensee to safeguard against malware distributed using the internet.

(8) Procedures and responsibilities shall be defined by the licensee to deal with malware protection on CTI as well as carrying out required trainings.

(9) Appropriate business continuity plan should be prepared by the licensee for recovering from malware attacks including necessary data / software backup and recovery arrangements.

8. **Data Protection.—**(1) Privacy shall be ensured for critical telecom data stored by the licensee and it shall only be used for the purpose for which it was obtained from customers / users.

(2) Data shall be protected from unauthorized disclosure, modification, loss and destruction.

(3) Licensed data retention timeframes shall be observed and where required clarity shall be sought from the Authority for retention timeframe of any data for which a retention timeframe is not mentioned in the license.

(4) Data shall be appropriately classified by the licensee to ensure that personal and critical telecom data receives appropriate level of protection.

(5) Consideration should be given to the possibility of deterioration of storage media, and data handling procedures shall be made accordingly to avoid data loss.

(6) Storage media shall be stored in a safe and secure environment in line with relevant manufacturer requirements.

(7) Storage media shall be disposed securely to avoid any unauthorized release of data.

(8) Data breach should be avoided during physical transfer of storage media.

(9) A policy shall be made and enforced to protect critical data access, process or store at teleworking sites.

(10) Privacy and protection of personal and critical telecom data, either at rest or in transit shall be ensured and licensee may use encryption to avoid any data breach.

(11) An organization wide data policy shall be prepared and implemented by the licensee to ensure protection and privacy of personal and critical data and prevent its unauthorized release / access.

(12) No Data shall be stored beyond country's geographical boundaries without the approval of the Authority.

9. **Critical Telecom Infrastructure Management.—**(1) Assets shall be classified by the licensee to ensure that Critical Telecom Infrastructure receive appropriate level of protection.

(2) Licensee shall ensure that Assets associated with Critical Telecom Infrastructure are inventoried with responsibility assigned to either an individual or a designated entity to ensure that associated cyber threats such as technical vulnerabilities are effectively managed.

(3) Rules shall be documented and implemented by the licensee for acceptable use, transfer, removal and disposition of assets.

(4) Employees or external users having access to assets related to critical infrastructure, shall be made aware by the licensee of their Cybersecurity requirements.

(5) An access control policy shall be established, documented and enforced by the licensee to prevent unauthorized access to CTI.

(6) A policy shall be formulated and enforced by the licensee to enable only authorized access to Network and Network services.

(7) A user access mechanism shall be implemented by the licensee to enable assignment of user rights and access privileges for systems and services.

(8) A password management mechanism should be put in place by the licensee to ensure quality passwords.

(9) Employees shall be made accountable for protecting their secret authenticated information.

(10) It shall be ensured by the licensee that Critical Telecom Infrastructure shall not be compromised to prevent unauthorized access to critical telecom data including real time data /voice connections.

11) Licensee shall ensure that patches for Critical vulnerabilities are applied and verified within 72 hours.

(12) Licensee should only use Vendor-supported software versions for systems and applications that store Critical Data.

(13) Licensee should validate and audit all the privileged accounts on an annual or more frequent basis

(14) Multi-factor authentication shall be implemented for all users accessing any part of Critical Telecom Infrastructure.

10. **Backup.**—(1) Backup copies of data, relevant software and system images related to critical data and CTI, shall be taken and tested regularly and upon any significant change by the licensee.

(2) The backup shall be stored by the licensee at a remote site located at a suitable distance from the primary site.

(3) A copy of backups must be disconnected from computers and networks, and should be placed in a non-rewritable and non-erasable manner.

(4) Backup arrangements should cover all system information, applications and data necessary for recovery to ensure business and service continuity.

(5) Appropriate retention timeframe for critical data shall be defined keeping in view the relevant regulatory requirements.

(6) Encryption shall be applied to safeguard backup data from unauthorized access.

(7) A back up policy shall be formulated and enforced to ensure compliance.

(8) Full recovery of backups must be tested at-least once annually and upon a fundamental infrastructure change.

11. **Cybersecurity Incident Management.—**(1) A Computer Emergency Response Team (CERT) shall be established by the licensee to ensure a quick, effective and orderly response to Cybersecurity incidents.

(2) CERT should be capable of Planning, detection, initiation, response, Recovery and Post-incident analysis having well-defined functions and communicated processes in place which should be tested periodically.

(3) CERT shall have established and designated communication and reporting channels to enable internal and external users including subscribers and other sources to report Cybersecurity events as quickly as possible.

(4) Reported and monitored Cybersecurity events shall be assessed and accordingly classified as Cybersecurity incidents.

(5) All Cybersecurity incidents shall be formally recorded and Post-incident review report of all the incidents must be maintained.

(6) Incidents shall be responded with a goal to achieve normal security level and initiating necessary recovery to resume business continuity.

(7) Procedures shall be defined and applied to identify, collect and preserve information related to a Cybersecurity incident which can serve as evidence.

(8) Cybersecurity incidents shall be analyzed to reduce likelihood of their future occurrence and resolve any identified security weaknesses.

(9) Licensee shall establish processes for collecting, analyzing and responding to cyber threat intelligence information collected from internal and external sources. The licensee shall share threat feeds with PTA.

(10) To safeguard the Telecom Sector as a whole, licensee CERT shall be in contact with Telecom sector CERT established by PTA as well as other licensees

CERTs to share security alerts/advisories/events/incidents information in a timely fashion.

12. **Service and Cybersecurity Continuity Management.—**(1) The licensee shall ensure that during all situations, Service and Cybersecurity continuity shall be ensured to ensure provision of licensed services and safeguard integrity, availability and confidentiality of CTI and critical data.

(2) Formal processes and procedures shall be formulated, documented and implemented by the licensee to ensure required level of continuity for Services and Cybersecurity during adverse situations.

(3) Redundancies shall be arranged by the licensee for CTI and Cybersecurity systems and said arrangements shall be verified at regular intervals to ensure their efficacy.

PART-III

CONTINUAL IMPROVEMENT

13. **Cybersecurity Reviews.—**(1) Licensee shall carry out quarterly periodic reviews of Cybersecurity measures for analysis and improvement of Cybersecurity measures.

(2) At least once a year or upon a significant change / event, the licensee shall carry out an independent review from a third party after getting due approval from PTA, of its Cybersecurity measures and implement required corrective actions.

(3) Technical compliance reviews for CTI such as vulnerability assessment and penetration testing shall be regularly carried out by the licensee at least once every six (6) months to identify and rectify vulnerabilities and security weaknesses.

(4) The licensee shall assist the Authority or its designated personnel for carrying out audit of its Cybersecurity capabilities with implementation of any identified short comings within the recommended timeframe.

PART-IV

MISCELLANEOUS

14. **Breach of Conditions of Regulations.—**(1) In case of non-compliance of any procedure specified in these Regulations and as directed by the Authority from time to time, or upon receipt of information from any source of non-compliance of these Regulations and directions of the Authority, the Authority or an authorized officer of the Authority not below the rank of Director, may initiate action against the offender.

15. **Directions of the Authority.—**(1) All directives, notifications, standard operating procedures and orders issued by the Authority from time to time on or before notification of these Regulations shall be binding and applicable on the Licensees.

16. **Consumer Education & Awareness.—**(1) All licensees shall take necessary steps for the awareness of consumers to safeguard against Cyber threats.

17. **Inspection.—**(1) In order to ensure compliance of these Regulations, the Authority through its authorized officer(s) may inspect the premises and records maintained by the Licensee(s) at any time.

(2) The concerned Licensee(s) shall provide all the information and shall extend all possible assistance to the authorized officer(s) or representative of the Authority to inspect the records.

18. **Reporting Requirements.—**(1) Reports mentioned in the regulations such as security policies, incident reports, and security reviews etc. shall be submitted to PTA upon conclusion of an activity / event or as and when required by the Authority.

(2) In case of a data breach or damage to CTI or critical data, the licensee shall duly inform the Authority within 72 hours from the discovery of the incident.

(3) Access to reports and logs of security monitoring systems shall be provided to the Authority as per its defined guidelines.

19. **Confidentiality of Information.—**(1) Without prejudice to the provisions of any law for the time being in force, every Licensee shall ensure the confidentiality of all information disclosed by the subscribers under the provisions of these Regulations.

[No. 97/Regs/PTA/2020/197.]

ERUM LATIF,
Director (Law & Regulations).

PRINTED BY THE MANAGER, PRINTING CORPORATION OF PAKISTAN PRESS, ISLAMABAD.
PUBLISHED BY THE DEPUTY CONTROLLER STATIONERY AND FORMS, UNIVERSITY ROAD, KARACHI.