National Electric Power Regulatory Authority (Security of Information Technology and Operational Technology) Regulations, 2022

Notification

Islamabad ____, 2022

SRO._____.- In exercise of the powers conferred under section 47 of the Regulation of Generation, Transmission and Distribution of Electric Power Act, 1997 (Act No.XL of 1997) read with all other enabling provisions thereof, the National Electric Power Regulation Authority is pleased to make the following regulations.-

1. Short title and commencement.- (1) These regulations may be called the National Electric Power Regulatory Authority (Security of Information Technology and Operational Technology) Regulations, 2022.

(2) These regulations shall come into force at once unless it is provided otherwise hereunder.

2. Scope.- (1) These regulations set minimum standards for compliance by the licensees, registered persons and generation companies in the interest of ensuring safe and reliable electric power services are provided to the consumers and necessary trust is maintained among the stakeholders of the power sector.

(2) It shall be responsibility of every licensee, registration holder, generation company and consumer to ensure that its information systems are properly maintained and safeguarded against unauthorized access.

(3) Any licensee, registration holder, generation company or consumer connected to the national grid, shall ensure that sufficient safeguards are built in its system to prevent any damage to the critical infrastructure information system or data of national grid or system of another user of the national grid.

3. Definitions.- (1) The terms used in these regulations shall have the following meanings unless it appears repugnant to the context.-

(a) “Act” means the Regulation of Generation, Transmission and Distribution of Electric Power Act, 1997 (Act No.XL of 1997) as amended from time to time;

(b) “access device” means any device that may enable access to the system or any part thereof;

(c) “computer emergency response team of power sector” (Power CERT) means a computer emergency response team designated under section 49 of the Prevention of Electronic Crimes Act, 2016 (Act No.XL of 2016) by the Federal

Government for responding to any threats or attacks on information systems of the power sector;

(d) "critical infrastructure in power sector" includes any infrastructure of a licensee connected with the national grid, the loss or compromise of which could result in major detrimental impact on the availability, integrity, reliability or delivery of electric power services including those services, whose integrity, if compromised, could result in significant loss of life or property;

(e) "critical infrastructure information system or data" means an information system, programme or data that supports or performs a function with respect to a critical infrastructure;

(f) “identity theft prevention” means any arrangement developed and implemented in order to identify, prevent and mitigate identity thefts in compliance with these regulations.

(g) “Intrusion Detection System” (IDS) means network security applications and appliances which monitor events occurring in a computer system or network in order to identify violations, malicious activity and suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system;

(h) “Intrusion Prevention System” (IPS) means an extension of IDS, which in addition to performing intrusion detection also attempts to stop possible incidents.

(i) “information technology and other technology assets” (IT and OT assets) include any data, information system or device of a generation company connected to the grid, a licensee or registration holder’s that controls or enables control of its own or another licensee’s network or machines;

(j) “least privilege principle” means that security architecture shall be designed in a way that each entity is granted the minimum system resources and authorizations needed by the entity to perform its functions.

(k) “Security Operation Control” (SOC) means a team of technical experts designated by the relevant licensee to respond to a threat or attack on its information systems;

(l) “security breach” means any incident that results in unauthorized access of systems, applications, data, services, networks and/or devices.

(m)“security controls” are formal arrangements made to avoid, counteract and minimize security risks identified by a licensee in its Security Risk Assessment exercise including preventive, detective and corrective arrangements to mitigate security risks to protect licensee’s systems.

(n) “security objectives” means series of statements that describe licensee’s intent to safeguard itself from internal or external threats.

(2) The terms used in these regulations but not defined shall have the same meanings, unless it appears repugnant to the context, as assigned to them under the Act.

4. IT and OT assets security policy.- (1) Every licensee, registration holder and a generation company connected to national grid shall develop or adopt, implement and regularly review and update IT and OT assets security policy and manuals.

(2) The IT and OT assets security policy and manuals of a licensee, registration holder and generation company shall:

(a) define and put in place appropriate management structure with required skills and qualifications for developing, maintaining, reviewing and updating the information security framework. In particular hire qualified Cyber Security individuals and appoint Chief Information Security Officer (CISO);
(b) maintain inventory and categorize IT and OT assets
(c) enhance security of IT and OT assets particularly critical infrastructure;
(d) provide mechanisms to protect its systems from unauthorized access, to ensure integrity, confidentiality and authenticity of data and systems;
(e) ensure reliability and availability of information systems and data and maintaining operational effectiveness;
(f) ensure accountability by designing standard operating procedures, policies and controls to enable traceability of all operations and identification of the system user at the relevant time;
(g) promote a culture of cyber-security awareness within the organization; and
(h) requirement for regular monitoring security controls, responding to the Security Incidents, mitigating the risks and vulnerabilities in IT and OT assets;
(i) patch and Change Management;
(j) channels for training and awareness of the employees and contractors;
(k) adequately cover any gaps identified through a gap analysis conducted by it and adopt appropriate controls;
(l) cuidelines for acquisition of information technology IT and OT assets;
(m)formulation, roles and responsibilities of the SOC;
(n) mechanism for seamlessly implementing the guidelines from PowerCert and/or the Authority;
(o) conducting of regular audits, security risk assessment and management thereof;
(p) requirements and processes for evaluating employees, contractors and other relevant stakeholders for potential risks;
(q) establish channels of communications for sharing of any critical information relating to a threat to the power sector; and
(r) reporting of any significant threat or attack in real time to the Authority’s designated officer and PowerCERT.

(s) implement any other guidelines or directives issued by the Authority or PowerCERT in the interest of ensuring protection of power sector in general and any part thereof in particular.

7. Security controls implementation and improvement.- (1) The licensee shall ensure that appropriate security arrangements and security controls to protect IT and OT assets (such as systems, applications, networks, data, and information and communication systems) are in place. Licensee shall develop a set of controls based on relevant international standards, the Security Risk Assessment document, commensurate with the risk levels to meet the control objectives and as per instructions issued by the Authority or the PowerCERT.

(2) The minimum requirements with regard to the security controls shall be as follows:

(a) Access Rights Management: Users' access rights shall be appropriate and commensurate with their job functions and shall be periodically reviewed keeping in view the risk ranking of the systems, data and applications as outlined in Security Risk Assessment document. Changes in Access Rights shall be based on personal or systems change and shall only be applied after due authorization while ensuring proper implementation of "least privilege principle".

(b) Operating Systems Controls: Necessary Operating Systems' controls shall be implemented to ensure that access is physically and logically secured by ensuring that privileged access is restricted, regularly monitored and periodically audited.

(c) Remote Access: Remote access to high risk IT and OT assets shall only be granted after management's approval in writing and shall be subject to regular audits. Remote access shall also be based on strong authentication and encryption to secure communications.

(d) Physical Access: Licensees shall ensure that physical access to different systems, segments and data sites is restricted, regularly monitored and duly logged.

(e) IT and OT Network Security: IT networks shall be secured through the use of multiple layers of controls.

(f) Firewalls: Firewalls shall be deployed between different security domains to control network traffic**.** Firewalls selection and deployment policy shall be devised according to the characteristics of network (i.e. traffic volume, and risk classification of IT and OT assets).

(g) IDS/IPS: Network Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) shall be deployed between different security domains as per their risk classification.

(h) Identity Theft Prevention: Licensee shall develop and implement a proactive Identity Theft Prevention Program which includes procedures for identification of information to be protected, and threats due to thefts and frauds as well as methods for responding appropriately to identified threats.

(i) Encryption: Access, storage and data communication shall be encrypted using reliable encryption methods to strengthen the security of communications and sensitive payment data.

(j) Traceability: Licensee shall maintain the traceability of operations performed on IT and OT assets.

(k) Training: Relevant employees of the licensee shall have appropriate knowledge and background to perform their tasks. Regular trainings shall be arranged to keep employees aware of the security risks, security controls and security control monitoring mechanisms. Employees shall be regularly updated about the changes in internal policies and procedures to ensure operational effectiveness.

6. Conducting regular security risk assessment / vulnerability assessment.- (1) The licensee shall conduct and document a formal Security Risk / Vulnerability Assessment for Information Security Assets (IT and OT) with a view of identifying, estimating and prioritizing risks to which its operations are exposed due to Information Security vulnerabilities. The control testing shall be based on the controls mentioned in the relevant international standards. The Board of Directors shall review the risk / vulnerability assessment document and take steps to mitigate any risks and vulnerabilities identified.

(2) The risk / vulnerability assessment shall cover the following aspects as a minimum requirement:

(a) A current and detailed description of licensee's business and technology environment and existing security measures in place including identification of location, systems and methods for maintaining information;
(b) An identification of information and the information systems to be protected specifically;
(c) Classification and ranking (high, medium, low) of the sensitive systems and applications in order of their importance and based on the assessment of threats and vulnerabilities or risk assessment;
(d) Assessment of potential threats and vulnerabilities to security and integrity of data, information systems and applications;
(e) An evaluation of existing Security Controls' effectiveness against each threat and vulnerability;

(f) The security and contractual responsibilities of Service Providers (SPs), including customers who have access to the licensee's systems and data;

(g) Risks like Compliance, Concentration, Operational, Country and Legal shall be assessed by the licensees before entering into contract and while managing Information Security outsourcing arrangements with the SPs;

(h) The Security Risk / Vulnerability Assessment shall be carried out at least once a year; however, in case of a major security breach, significant changes to the infrastructure and introduction of a new product or service, an immediate review of risk assessment shall be carried out. Further, in case of a major security breach, risk assessment review shall include a detailed analysis of the factors that cause such security breaches.

7. Integrity, confidentiality and authenticity of data.- (1) It shall be the responsibility of the licensee providing data to another licensee or stakeholder of power sector to ensure that the data is free from any errors, access to data is provided to only duly authorized persons and there is a mechanism in place to ensure data is authentic.

(2) The national grid company and the licensees or generation companies connected with it shall put in place mechanism for any critical data validation.

8. Authority mandated audit and risk assessment.- The Authority may, for reasons to be recorded in writing, order a special audit and/or risk assessment with such objectives as may be deemed appropriate in respect of any licensee, registration holder and generation company including any interconnection between the stakeholders of the power sector.

8. Monitoring and computer incident response.- (1) A generation company connected to the national grid, a licensee or a registration holder shall ensure that approved mechanisms for monitoring of security controls and any computer incident in line with the relevant best practices are in place.

(2) Any computer incident shall be immediately tackled at the organizational level by the organizational CERT to ensure that an organizational incident is properly addresses and does not spread to or impact other licensees or stakeholders of the power sectors.

(3) Licensee shall develop and implement a formally approved mechanism for the monitoring of Security Controls. An analysis of the effectiveness of existing or proposed Security Controls Monitoring methods shall be part of this monitoring mechanism. Licensee shall ensure that at the minimum the following aspects are covered in the Security Controls Monitoring and Response mechanism:

(a) Monitoring of licensee's network activity by collecting and analyzing the host and network data related to security events. Examples of security events include privileged

access to sensitive operating systems, configuration changes, and access to critical applications etc;

(b) Methods for proactive monitoring of IDS/IPS and for responding to security breaches shall be listed in detail in the monitoring mechanism. A rapid response team shall be nominated and made responsible to respond immediately in case of a security breach;

(c) Monitoring and reporting mechanism of Authentication Controls shall be formally documented and approved by the senior management and implemented accordingly;

(d) Procedures and time required for restoration of licensee's systems shall be part of Security Controls Monitoring and Response process;

(e) Use of self-assessments, penetration testing, and independent security audits shall commensurate with the systems' complexity and risk exposures;

(f) Identification and listing of licensee's policy violations, unauthorized configuration changes and other conditions which can potentially increase the risk of security breaches;

(g) Procedures to ensure the monitoring of logs and audit trails on regular and pre-defined periodic basis shall be developed. The security logs and audit trials for IT and OT assets controls shall be retained for a period of five years.

9. Awareness and training.- (1) A formal awareness and training program regarding Information Security threats and safeguards to minimize frauds and Identity Theft risks shall be developed and implemented by the licensees.

(2) This program shall cover the following aspects at the minimum:

(a) An explanation of liabilities, roles and responsibilities of licensee as well as its customers and users for using IT and OT products and services offered by the licensee;

(b) Compliance to the disclosure requirements under the applicable laws;

(c) Contact details of help desk that might be needed in case of any information security issues;

(d) Procedure for re-authentication user profile updation;

(e) Complaint handling process including dispute resolution mechanism related to IT and OT Assets;

(f) Regular issuance of guidelines to customers and users on regular basis as required for mitigating the latest risks associated with IT and OT assets;

(g) Regular review and evaluation of the awareness and training programs by the management.

10. Regulatory reporting requirements.- (1) These regulations are subject to all relevant laws, rules and regulations issued by NEPRA from time-to-time. All the licensees shall ensure that

(a) All established security breaches shall be reported to National Electric Power Regulatory Authority. The incident and analysis reports of security breaches shall be furnished on quarterly basis as per the Schedule.

(b) Impact of security breach on licensee's business, systems, applications, users, and customers as well as dependent IT and OT assets shall also be submitted.

(c) A common mechanism for transfer of information, ranking of incidents level to be reported, the frequency of reporting and the use of relevant tools shall be adopted in consultation with the PowerCert.

11. PowerCert.- The Authority may notify a set of relevant experts from amongst the licnesees, generation companies and registration holders to act as PowerCert under these regulations.

Schedule

Details of Established Security Breaches in IT and OT

Name of the licensee: _____ For the Quarter Ending: _____

Sr.	Incident Analysis				Impact Analysis		Remarks (further details, if any)
	Source of security breach discovery	Nature of security breach	Reasons for the occurrence of security breach	Action(s) taken to rectify the Security Breaches	Asset Affected	Impact of security breach	