Compliance under NEPRA Security of Information Technology and Operational Technology Regulations, 2022

Clause No	Clause Description	IT Complaince Status Complaint/ Partially Complaint/ Non-Complaint	OT Complaince Status Complaint/ Partially Complaint/ Non-Complaint	Remarks for IT Status	Remarks for OT Status
4.	**IT and OT Assets Security Policy**				
4(1)	Every licensee, registration holder and a generation company connected to national grid shall develop or adopt, implement and regularly review (at least once in every three years) and update IT and OT assets security policy and manuals				
4(2)	The IT and OT assets security policy and manuals of a licensee, registration holder and generation company shall:				
4(2)(a)	define and put in place appropriate management structure with required skills and qualification for developing,maintaining,reviewing, and updating the information security framework,and particularly hire qualified Cyber Security individuals and appoint Chief Information Security Officer (CISO)				
4(2) (b)	provide for maintenance of inventory and categorization of IT and OT assets;				
4(2) (c)	provide for enhancement of security of IT and OT assets, particularly critical infrastructure;				
4(2) (d)	provide mechanisms to protect its systems from unauthorized access, to ensure integrity, confidentiality and authenticity of data and systems;				
4(2) (e)	provide guidelines for acquisition of information technology IT and OT assests;				
4(2) (f)	ensure reliability and availability of information systems and data and maintaining operational effectiveness;				
4(2) (g)	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;				
4(2) (h)	provide for formulation,roles and responsibilites of the SOC;				
4(2) (i)	provide the requirments for regular monitoring of security controls,responding to the Security Incidents,mitigating the risks and vulnerabilities in IT and OT assets;				
4(2) (j)	provide for patch and change management;				
4(2) (k)	provide for conducting regular audits,security risk assessment and management thereof;				
4(2) (l)	adequately cover any gaps identified by it through a gap analysis and enable appropriate controls;				
4(2) (m)	provide requirments and processes for evaluating employees,contractors and other relevant stakeholders for potential risks;				
4(2) (n)	define a business continuity plan to ensure service continuity in case of any incident;				
4(2) (o)	provide for data diposal procedure and requirments that avaoid any unauthorized access or use of such data;				
4(2) (p)	promote a culture of cyber-security awareness within the organization; and channels for training and awareness of the employees and contractors;				
4(2)(q)	establish channels of communications for sharing of any critical information relating to a threat to the power sector; Provided that it shall be ensured that any information shared in this regard is kept confidential;				
4(2)(r)	mechanism for seamlessly implementing the guidelines from PowerCert and/or the Authority;				

4(2) (s)	reporting of any significant threat or attack in real time to the Authority's designated officer and PowerCERT.				
4(2) (t)	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.				
5.	**Security Control Implementation and Improvement**				
5 (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.				
5(2)	The minimum requirements with regard to the security controls shall be as follows:				
5(2)(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".				
5(2)(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.				
5(2)(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. Provided that a licensee, registration holder or a generation company shall not allow remote access to any critical infrastructure in the power sector, from a country that is considered hostile towards Pakistan.				
5(2)(d)	Physical Access: Licensees shall ensure that physical access to different systems, segments and data sites is restricted, regularly monitored and duly logged				
5(2)(e)	IT and OT Network Security: IT networks shall be secured through the use of multiple layers of controls.				
5(2)(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).				
5(2)(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.				
5(2)(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.				
5(2)(i)	Encryption: Access, storage and data communication shall be encrypted using reliable encryption methods to strengthen the security of communications and sensitive payment data.				
5(2)(j)	Traceability: Licensee shall maintain the traceability of operations performed on IT and OT assets.				

5(2)(k)	Data Backup: Regular backup of important data, transactions and software shall be ensured.				
5(2)(l)	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**				
6(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.				
6(2)	The risk / vulnerability assessment shall cover the following aspects as a minimum requirement:				
6(2)(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;				
6(2)(b)	An identification of information and the information systems to be protected specifically;				
6(2)(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;				
6(2)(d)	Assessment of potential threats and vulnerabilities to security and integrity of data, information systems and applications;				
6(2)(e)	An evaluation of existing Security Controls' effectiveness against each threat and vulnerability;				
6(2)(f)	The security and contractual responsibilities of Service Providers (SPs), including customers who have access to the licensee's systems and data;				
6(2)(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;				
6(2)(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**				
7(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.				
7(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 mandate audit and risk assessment**				
8(1)	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.				
9.	**Monitoring and computer incident response**				

9(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.				
9(2)	A generation company connected to the national grid, a licensee or a registration holder shall develop and shall have in place incident management plan to tackle immediately any incident 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.				
9(3)	A generation company connected to the national grid,a licensee or a registration holder 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 Monitoing mthods 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:				
9(3)(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;				
9(3)(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;				
9(3)(c)	Monitoring and reporting mechanism of Authentication Controls shall be formally documented and approved by the senior management and implemented accordingly;				
9(3)(d)	Procedures and time required for restoration of licensee's systems shall be part of Security Controls Monitoring and Response process;				
9(3) (e)	Use of self-assessments, penetration testing, and independent security audits shall commensurate with the systems' complexity and risk exposures;				
9(3)(f)	Identification and listing of licensee's policy violations, unauthorized configuration changes and other conditions which can potentially increase the risk of security breaches;				
9(3)(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.				
10.	**Awareness and training**				
10(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				
10(2)	This program shall cover the following aspects at the minimum:				
10(2)(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;				
10(2)(b)	Compliance to the disclosure requirements under the applicable laws;				
10(2)(c)	Contact details of help desk that might be needed in case of any information security issues;				
10(2)(d)	Procedure for re-authentication user profile updation;				

10(2)(e)	compliant handling prcoess including dispute resolution mechanism relaed to IT and OT Assets;				
10(2)(f)	regular review and evaluation of the awareness and training programs by the management.				
10(2)(g)	Regular issuance of guidelines to customers and users on regular basis as required for mitigating the latest risks associated with IT and OT assets;				
11.	**Regulatory Reporting requirements**				
11(1)	These regulations are subject to all the relevant laws, rules and regulations issued by the Authority from time-to-time. All the licensees, registration holders and generation companies connected to the grid shall ensure that:				
11(1)(a)	all established security breaches shall be reported to the Authority. The incident and analysis reports of security breaches shall be furnished on quarterly basis as per the Schedule;				
11(1)(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; and				
11(1)(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(2)	Any incident involving a security breach or threat shall be reported to the Authority immediately but not later than seventy-two hours from the first knowledge of the incident.				