कार्यक्रमों के अनुसार प्रणालियों को प्रभावित करने वाले अद्यतन।

श्रवण कुमार, सचिव

[विज्ञापन-III/4/असा./253/2026-27]

CENTRAL ELECTRICITY AUTHORITY

NOTIFICATION

New Delhi, the 31th July, 2026

F. No. CEA-HY-91-19/8/2024-Cyber Security Division.—Whereas public notices advertising the draft of the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2025 were published in six newspaper dailies, as required by sub-section (3) of section 177 of the Electricity Act, 2003 (36 of 2003) read with sub-rule (2) of rule 3 of the Electricity (Procedure for Previous Publication) Rules, 2005 for inviting objections and suggestions from all persons likely to be affected thereby, before the expiry of the period of thirty days, from the date on which the copies of the said draft regulations were made available to the public;

And whereas copies of the said newspapers containing the public notices and the said draft regulations on the website of the Central Electricity Authority were made available to the public on 07th October 2025;

And whereas the objections and suggestions received from the public on the said draft regulations were considered by the Central Electricity Authority;

And whereas Ministry of Electronics and Information Technology has accorded its concurrence to make these regulations in respect of the Cyber Security for power sector.

Now, therefore, in exercise of the powers conferred by sub-section (1) of section 177 read with clause (c) of section 73 of the Electricity Act, 2003(36 of 2003), the Central Electricity Authority hereby makes the following regulations relating to Cyber Security in power sector for ensuring safe and secure operation and maintenance of electrical plants and electrical lines, namely**: –**

Chapter I

Preliminary

1. **Short title and commencement -** (1) These regulations may be called the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026.

(2) These regulations shall come into force with effect from 1st April 2027:

Provided that the Regulations 5(9), 5(24), 5(33), 5(39), 6(2) and 6(7) shall come into force on such dates, as may be specified by the Authority through separate orders with prior approval of the Central Government.

2. **Scope and extent of applicability -** (1) These Regulations shall apply to -

(a) all the entities which own, operate, or manage Operational Technology infrastructure associated with the interconnected power system and their Information Technology infrastructure that is physically or logically connected to such Operational Technology infrastructure, for their existing as well as upcoming infrastructure:

Provided that in respect of generating companies, captive generating plants, and organisations having Energy Storage System, these regulations shall be applicable only where such entities have an installed capacity of 50 MW or more:

Provided further that the entities having an installed capacity of less than 50 MW are encouraged to implement the minimum baseline cyber security controls outlined in the "15 Elemental Cyber Defense Controls for Micro, Small and Medium Enterprises" issued by Indian Computer Emergency Response Team;

(b) power exchanges and over the counter platforms, except regulations 6, 11, and 12.

(2) The vendor shall comply with the regulations 11 and 12 of these regulations as applicable.

3. **Definitions** - (1) In these regulations, unless the context otherwise requires -

(a) **"Act"** means the Electricity Act, 2003 (36 of 2003);

(b) **"Bill of materials"** means a comprehensive list and structured inventories of components, sub-components, material, libraries, and modules used in product or system to facilitate a comprehensive visibility and transparency into composition of such product or system;

(c) **"Business continuity plan"** means documented procedures that guide an organisation to maintain a defined level of continued business operations;

(d) **"Chief Information Security Officer"** means the designated employee of senior management level of an entity, having knowledge of cyber security and matters related thereto and who is responsible for cyber security efforts and initiatives;

(e) "**Chief Information Security Officer – Ministry of Power**" means Chief Information Security Officer of Ministry of Power;

(f) **"communication system"** means a collection of individual communication networks, communication media, relaying stations, tributary stations, terminal equipment usually capable of inter-connection and inter-operation to form an integrated communication for power sector;

(g) **"Computer Security Incident Response Team – Power"** means an organisation established by the Ministry of Power as an extended arm of Indian Computer Emergency Response Team (CERT-In) for coordinating, reporting, and responding to cyber security incidents in power sector;

(h) **"critical Information Technology system"** means Information Technology system of an organisation whose unavailability or degradation would adversely impact its business operations;

(i) **"critical Operational Technology system"** means Operational Technology system of an organisation whose unavailability or degradation would adversely impact its business operations;

(j) **"critical system"** means critical Operational Technology system or critical Information Technology system or both, including Critical Information Infrastructure, as applicable, of an entity;

(k) **"Critical Information Infrastructure"** means Critical Information Infrastructure as defined in explanation of sub-section (1) of section 70 of the Information Technology Act, 2000 (21 of 2000);

(l) **"cyber asset"** means the programmable electronic device, with or without computing capabilities including its hardware, software, sub-components and data thereof that are connected over a network;

(m) **"cyber asset register"** means a record that contains list of all cyber assets and description thereof;

(n) **"cyber crisis management plan"** means cyber crisis management plan as defined in clause (d) of sub-rule (1) of rule 2 of the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018;

(o) **"cyber resilience"** means the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on cyber asset;

(p) **"cyber security audit"** means an audit to assess the cyber security posture by a CERT-In empanelled auditor or any other auditor, as may be designated by the Ministry of Power, Government of India through a separate order;

(q) **"Cyber security breach"** means cyber security breach as defined in clause (i) of sub-rule (1) of rule 2 of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013;

(r) **"Cyber security incident"** means cyber security incident as defined in clause(h) of sub-rule (1) of rule 2 of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013;

(s) **"Cyber security policy"** means procedure and processes for protecting information, computer resources, networks, devices, industrial control systems and Operational Technology resources and to improve the cyber security posture thereof;

(t) **"Cyber sabotage"** means deliberate action to disrupt, damage or destroy the information systems, networks or data processed therein for malicious purpose;

(u) **"Distributed Generation Resource"** means a generating station feeding electricity into the electricity system at voltage level of below 33 kV and includes grid-connected rooftop solar systems and Energy Storage System;

(v) **"Electronic Security Perimeter"** means the logical border surrounding Information Technology system or Operational Technology system or both that are electronically connected within which the access is monitored and controlled for protection of such system;

(w) **"entity"** includes generating companies, Captive generating plants, organisations having Energy Storage System; transmission licensees; distribution licensees; National Load Dispatch Centre; Regional Load Dispatch Centres; State Load Dispatch Centres; Power Exchanges and Over the Counter Platforms;

(x) **"Factory Acceptance Test"** means structured and documented testing process carried out by the vendor in the presence of the representative of the entity to verify functional, performance, contractual and safety requirements of system or equipment or major component thereof before dispatch;

(y) **"Information Technology system"** means the Information Technology system consisting of user endpoints, network resources, applications, servers, and communication components deployed therein;

(z) **"obsolete asset"** means an asset declared by original equipment manufacturer or original equipment supplier whose production and services have discontinued, and its support is no longer available, and that asset is not suitable for its intended purpose due to technological advancement, operational changes and may pose security or operational risk;

(aa) **"Operational Technology"** means programmable hardware or system that detects or causes changes through the direct monitoring or control of physical devices, processes, and events;

(bb) **"prosumer"** means a person who consumes electricity from the grid and can also inject electricity into the grid for distribution licensee, using same point of supply;

(cc) **"protected system"** means protected system as defined in clause (k) of sub-rule (1) of rules 2 of the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018;

(dd) **"remote access"** means an access to any cyber asset of an organisation through an external network;

(ee) **"remote operation"** means day-to-day operation and control of Information Technology or Operational Technology system of an entity performed from a distant location from such system;

(ff) **"self-audit"** means an audit by an entity in a financial year to assess its compliance with all applicable regulations specified in these regulations;

(gg) **"sensitive information"** means data or information that, if disclosed, modified, or destroyed, could negatively impact the privacy, integrity, security or operations of an organisation or an individual;

(hh) **"Site Acceptance Test"** means structured and documented testing conducted to verify functional, performance, contractual and safety requirements, at the site of installation and ensure that a system or equipment and its major components operate as intended in its final operational environment, before its commissioning;

(ii) **"Sub-Sectoral Computer Security Incident Response Team"** means an entity designated by the Authority to assist Computer Security Incident Response Team - Power in cyber security related matters;

(jj) **"Technical Criteria Certificate"** means a certificate issued to an organisation by a designated certification body accredited for ensuring conformance to cyber security standards specified by the Central Government;

(kk) **"threat"** means any circumstance or event having the potential to exploit a deficiency and negatively impact the confidentiality, integrity or availability of a cyber asset or Information Technology system or Operational Technology system;

(ll) **"trusted source**" means a mechanism designed to mitigate specific security requirements particularly cyber security supply chain risks by ensuring that equipment, services, manufacturer and service providers, associated with power sector meet an established criteria;

(mm) **"Vulnerability"** means vulnerability as defined in clause (p) of sub-rule (1) of rule 2 of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013;

(nn) **"vendor"** means original equipment manufacturer, original equipment supplier, system integrator, supplier of hardware or software associated with original equipment, contractor or service provider including cloud service provider; and manufacturer and supplier of hardware, firmware, or software

associated with the original equipment or control systems, including but not limited to inverters, communication modules, monitoring systems, and related control or energy management software, of a Distributed Generation Resource owned by a prosumer.

(2) Words and expressions used but not defined in these regulations shall have their respective meanings assigned to them in the Act, Rules and other regulations made thereunder.

CHAPTER II

COMPUTER SECURITY INCIDENT RESPONSE TEAM - POWER

4. (1) **The Computer Security Incident Response Team – Power shall** -

(a) be the coordinating agency for reporting and responding to cyber security incidents associated with power sector;

(b) be the nodal agency of power sector for analysis, prediction and prevention of cyber security incidents and dissemination of information thereof;

(c) collect data and information pertaining to any cyber security incident from an entity including network architecture, details of assets, logs, cyber forensic records, forensic image, policies and procedures or any other relevant information, in the form, manner and mode as specified by it:

Provided that sensitive data as well as sensitive information collected shall be protected against breaches and shall only be used for cyber security purpose by designated government agencies but not be disclosed to any third party without explicit communication to the concerned entity.

(2) **The roles and responsibilities of Computer Security Incident Response Team - Power in** Power **Sector include the following, namely** -

(a) collect and analyze cyber incidents, vulnerabilities and threats related to power sector;

(b) predict cyber security incidents, threats and vulnerabilities related to power sector;

(c) coordinate and collaborate with Indian Computer Emergency Response Team, National Critical Information Infrastructure Protection Centre and other agencies designated by the Central Government in the area of cyber security, to resolve the cyber security incidents related to power sector;

(d) issue alerts, advisories, and guidelines as well as threat intelligence in coordination with Indian Computer Emergency Response Team, National Critical Information Infrastructure Protection Centre and any other agencies designated by the Central Government in the area of cyber security;

(e) create or develop Standard Operating Procedures, security policies, sub-sector specific benchmarks, security controls, and best practices for incident response activities in consultation with Indian Computer Emergency Response Team, National Critical Information Infrastructure Protection Centre, sub-sectoral Computer Security Incident Response Teams, Electricity Regulatory Commissions, entities, and other agencies designated by the Central Government in the area of cyber security;

(f) undertake proactive measures to increase the cyber security awareness through capacity building initiatives and interventions;

(g) ensure the improvement of cyber security posture of the power sector through cyber security assessments, cyber security audits, certification audits, self-audits, third party audits and exercises including mock-drills and simulations;

(h) coordinate for laying down the sub-sector specific cyber security framework, protocols, and rules;

(i) advise the entities in preparation of their Cyber Crisis Management Plan;

(j) coordinate with entity for ensuring the implementation of their Cyber Crisis Management Plan during actual cyber crisis;

(k) facilitate and promote Research and Development in the domain of cyber security through collaboration with Industry, Research Institutes and Academia;

(l) formulate and implement of measures to ensure cyber security of supply chain of cyber assets specified by the Central Government or the Authority;

(m) establish central cyber security coordination forum and regional cyber security coordination forums of power sector to support Computer Security Incident Response Team - Power, in accordance with a separate order issued by the Authority, for periodic review of cyber security posture, deliberate upon cyber security challenges, information sharing, coordinated response planning and improve the overall posture of sector;

(n) Any other functions associated with cyber security related matters in the power sector, as directed by the Central Government or the Authority.

(3) The directions and guidelines of Computer Security Incident Response Team - Power, in the matters related to cyber security of power sector, shall be complied with by entities and vendors, as applicable.

(4) The Authority through a separate order may designate sub-sectoral Computer Security Incident Response Teams in power sector for generation, transmission, distribution, grid operation, and any other sub-sector, along with their roles and responsibilities to assist Computer Security Incident Response Team - Power.

CHAPTER III

General Cyber Security requirements

5. **The entity shall** -

(1) designate regular employees of senior management level as Chief Information Security Officer and alternate Chief Information Security Officer;

(2) ensure that the positions of Chief Information Security Officer and alternate Chief Information Security Officer shall not remain vacant at the same time;

(3) define roles and responsibilities of Chief Information Security Officer and alternate Chief Information Security Officer in accordance with the Central Government's regulatory framework and relevant guidelines;

(4) ensure that the Chief Information Security Officer reports to the head of the entity:

Provided that in case any entity such as the State Load Dispatch Centre is not an independent entity but part of a holding company or parent company, such entity shall have a separate Chief Information Security Officer, who shall report to head of such holding company or parent company, as applicable and shall also have Alternate Chief Information Security Officer;

(5) ensure an employee is designated as Chief Information Security Officer, for a minimum period of three years;

(6) ensure that role of the Chief Information Security Officer is ring fenced to the tasks of cyber security related matters only;

(7) provide contact details of the Chief Information Security Officer and alternate Chief Information Security Officer and updation thereof in public domain and communicate such details to Computer Security Incident Response Team - Power as well as all internal and external stakeholders;

(8) ensure that Chief Information Security Officer attends cyber security training courses for at least five man-days in each financial year;

(9) establish a dedicated Information Security Division headed by Chief Information Security Officer, within India, for dealing with all cyber security related matters and the same shall remain operational round the clock. Further-

(a) the Information Security Division shall be deployed with sufficient staffing;

(b) the staff deployed in Information Security Division shall have valid certificate of successful completion of domain specific cyber security course;

(c) the staff deployed in Information Security Division shall attend cyber security training courses associated with power sector for at least five man-days in each financial year;

(d) the staff shall be deployed in Information Security Division for a minimum tenure of three years;

(10) have a defined and documented Cyber Security Policy, which is approved and reviewed annually by the head or board of the entity, as the case may be;

(11) prepare a Cyber Crisis Management Plan in consultation with Computer Security Incident Response Team - Power, to manage and recover from all possible cyber crisis situations in shortest possible time with minimum impact on business operations:

Provided that the Cyber Crisis Management Plan shall be vetted by Indian Computer Emergency Response Team, approved and reviewed annually by the head or board of the entity, as the case may be;

(12) ensure separation of Information Technology networks containing Critical Information Infrastructure from Internet as well as rest of the Information Technology networks:

Provided that in case internet is required for Information Technology networks containing Critical Information Infrastructure, the same shall be sourced securely with suitable hardening measures as specified by designated agencies of the Central Government;

(13) ensure deployment of all required security devices including firewalls at Electronic Security Perimeter, such that the deployed security system meets the requirements of, inter-alia, packet filtering; deep packet inspection; content, user and application based filtering; detection and inspection of encrypted traffic; intrusion detection and prevention; geo-fencing; facility for automatic signature and behaviour updates; user controlled updates; detection, inspection and filtering based on signature and behavioural anomalies;

(14) ensure that any web service or web-based application including website, web portal, and Application Programming Interfaces, having public access, shall be deployed only after cyber security audit clearance:

Provided that any software update, including patch, in web applications and web services shall be deployed only after successful testing and confirmation, such that the subject update is free from any cyber security vulnerability, and after ensuring that such update is free from any cyber risk:

Provided further that any software update qualified for prior requirement of cyber security audit, as specified in Cyber Security Policy, shall be deployed only after its cyber security audit clearance:

Provided also that all software updates, those not necessitated for prior cyber security audit, shall be assessed during next cyber security audit;

(15) ensure deployment of all required security devices for all critical web applications, identified as per the procedure detailed under Cyber Security Policy, such that the deployed security system meets the requirements of, inter alia, application layer filtering including detection and filtering of web based encrypted traffic; ensuring bidirectional protection; facility for automatic signature and behavioural updates; intrusion detection and prevention, user controlled update mechanism; content, user and application based filtering; geo-fencing; detection, inspection and filtering of encrypted traffic based on signature and behavioural anomalies;

(16) identify and segregate systems as critical and non – critical systems, as per the procedure detailed in Cyber Security Policy;

(17) ensure that remote access to cyber assets, if necessary, may be permitted only for troubleshooting and emergency requirements, as per the procedure specified under Cyber Security Policy:

Provided that such access for the cyber assets associated with non – critical system may be permitted with approval of Chief Information Security Officer for troubleshooting and emergency requirements only along with suitable security control measures:

Provided further that approval for such access to critical systems or cyber assets thereof may be granted after a comprehensive risk assessment is conducted along with identification of effective measures thereof and such access shall be continuously monitored to detect any anomaly or attempts of unauthorised use:

Provided also that record of risk assessment, physical document of approval and logs with respect to each such access to critical system shall be maintained for a period as specified in data retention policy;

(18) conduct cyber security awareness program and cyber security exercises including mock-drills and tabletop exercises, at least once in every six months;

(19) ensure that sensitive information and sensitive data including such data and information hosted on cloud as well as such historical data and information, is stored in an encrypted, secured, and protected environment and resides within India only;

(20) include all cyber security requirements as well as applicable cyber security rules, regulations issued by the Central Government and Non - Disclosure Agreement in Service Level Agreement with the vendors, as specified under Cyber Security Policy, to ensure the confidentiality, integrity and availability of sensitive information during their contract period as well as after completion of such contract period:

Provided that vendor having cyber or physical access or both to the critical systems including staff of vendor engaged for operation or maintenance or both of such systems, may be permitted after carrying out personnel risk assessment and mitigative measures taken thereof along with an undertaking complying with Service Level Agreement:

Provided further that in case of any cyber security breach, the entity shall enquire into the matter and initiate action against such vendors including cloud service provider committing cyber security breach;

(21) ensure online and offline backups of all critical systems in a separate, safe and secure environment as specified in cyber security policy;

(22) facilitate a comprehensive cyber security audit encompassing all critical systems, as specified under regulation 13, at least once in every financial year but with a minimum and maximum gap of nine months and fifteen months, respectively, between two consecutive cyber security audits:

Provided that the cyber security auditing agency engaged by entity shall deploy its qualified personnel but exclusive of any staff deployed for such entity, if any:

Provided further that no three consecutive audits shall be carried out by the same auditing agency or personnel;

(23) ensure that all Information Technology products procured comply with and tested in adherence with the orders issued by the Central Government;

(24) ensure compliance with and acquire ISO / IEC 27001 certificate or Technical Criteria Certificate encompassing all critical systems:

Provided that no four consecutive audits for the certification of ISO 27001 or Technical Criteria Certificate shall be carried out by the same auditing agency or personnel;

(25) maintain asset register-

(a) for all cyber assets along with the requisite details including ownership, hardware, firmware, software, and patch as per the procedure defined in Cyber Security Policy;

(b) recording the details of all critical systems along with the requisite details including its configuration, hardware, software, network architecture depicting data flows and communication protocols used therein:

Provided that such register shall be reviewed and updated at least once in every financial year or upon commissioning of any new cyber asset or critical system including replacements thereof, whichever is earlier;

(26) maintain Cyber Risk Assessment and Mitigation Plan for all assets detailed in cyber asset register, as per the procedure defined in Cyber Security Policy:

Provided that Cyber Risk Assessment and Mitigation Plan shall be updated at least once in every six months and reviewed at least once in every financial year and such Cyber Risk Assessment and Mitigation Plan shall be implemented to manage the vulnerabilities, threats and risks associated thereof;

(27) ensure that the cyber security audit including vulnerability assessment and penetration testing is carried out prior to the commissioning of any new critical system including replacement of such system and manage vulnerabilities and risks for critical system as per the mechanism defined in Cyber Security Policy;

(28) furnish relevant information including system details and functionality, of all new critical systems commissioned including those replaced, as per asset register associated with critical systems to the Computer Security Incident Response Team - Power within thirty days of such commissioning or replacement;

(29) provide the relevant information to National Critical Information Infrastructure Protection Centre for identification of Critical Information Infrastructure. Further, within sixty days of an asset being identified as a Critical Information Infrastructure by National Critical Information Infrastructure Protection Centre, entity shall approach the Appropriate Government for notifying such asset as a Protected System;

(30) ensure that Critical Information Infrastructure and Protected System are not discoverable on public platforms unless approved by the head or board of the entity, as applicable, on the basis of business requirements, criticality, and risk assessment of such system;

(31) ensure that the procurement process mandates inclusion of Factory Acceptance Test and Site Acceptance Test including testing of cyber security requirements;

(32) ensure that the clocks of all relevant information processing systems within Information Technology and Operational Technology systems, as applicable, are synchronised to a reference time source as provided in the Cyber Security Policy:

Provided that prior to selection of such reference time source detailed cyber risk assessment shall be carried out;

(33) ensure that all personnel including personnel engaged by vendors in day-to-day operation and

maintenance of all critical systems, have mandatorily undergone designated cyber security courses pertaining to power sector;

(34) ensure that the systems, networks, and applications associated with physical security of critical systems are physically separated from the network of such critical systems:

Provided that in case of such physical separation is not feasible, with approval of head of the entity, subject systems, networks, and applications shall be logically separated from the networks of such critical systems;

(35) maintain Incident Response and Recovery Plan, as specified in Cyber Security Policy, to recover from cyber incidents and resume normal operations at the earliest:

Provided that such plan shall be reviewed and updated at least once in every six months;

(36) have surveillance and continuous monitoring of Information Technology systems and Operational Technology systems, as applicable, for identification of threats as well as vulnerabilities and provide incident response and remediation support thereof;

(37) ensure that logs of all security devices deployed at Electronic Security Perimeter are enabled to record exchange of data and information flowing through such devices;

(38) ensure regular, at least once in every year, review and updation of rules and policies of perimeter security devices;

(39) ensure that the Information Technology equipment and services are procured from trusted sources, in accordance with orders, directions or guidelines issued by the Central Government from time to time;

(40) comply with the directions and requirements issued under the Information Technology Act, 2000 (21 of 2000) and with all rules and regulations made thereunder, in addition to these regulations;

(41) have structured vulnerability disclosure and management programs with vendors and Computer Security Incident Response Team – Power;

(42) maintain a register to record all cyber security incidents along with relevant details, as per the format prescribed by Computer Security Incident Response Team - Power.

CHAPTER IV

Additional Cyber Security requirements of Entities related to Operational Technology Systems.

6. **In addition to requirements mandated for entities under the regulation 5, the entity shall** – (1) ensure physical isolation of Operational Technology system from internet as well as Information Technology system:

Provided that in case such isolation from Information Technology system is not possible due to business requirements, such Information Technology and Operational Technology interconnection may be permitted, as per the procedure defined in Cyber Security Policy, with suitable hardened logical separation between Operational Technology system and Information Technology system, on the basis of risk assessment of such interconnection and approval of head or board of the entity, as applicable:

Provided further that such inter-connection is continuously monitored for detection of malicious activities and corrective measures thereof:

Provided also that such approval and logs associated with such inter-connection shall be retained for a period as specified in data retention policy;

(2) ensure deployment of suitable perimeter level cyber security devices including firewall at point of inter-connection of Operational Technology system with communication system of power system such that the deployed security system meets the requirements of, amongst other requirements, the detection and filtering of Operational Technology related protocols as well as traffic; content, user and application based filtering; deep packet inspection, intrusion detection; geo-fencing; user controlled updates; detection based on signature and behavioural anomalies and filtering thereof:

Provided that the updates including signatures for devices forming part of such security system shall be carried out in offline mode, as specified in Cyber Security Policy;

(3) ensure that control and operation of power system elements and exchange of information thereof including real time data shall be over a dedicated communication channel isolated from the internet through perimeter level cyber security devices and shall be confined to national boundaries only:

Provided that for entities having business requirements or cross border power system elements, the exchange of information and real time data, as identified under Cyber Security Policy, may be permitted beyond the national boundaries only through dedicated separate communication system and unidirectional gateway, isolated from internet and along with cyber security devices, to transmit and receive subject to the condition that such information and data are monitored continuously to detect any anomaly or unauthorised attempt:

Provided further that in case of exchange of real time information and data associated with end consumers, the same may be permitted through secured connection, isolated from public access, subject to the condition that exchange of sensitive information and data thereof over such connection shall be encrypted to ensure its confidentiality, integrity, and privacy;

(4) ensure that if remote operation is necessary for business requirements, the same shall be, within India, with the prior approval of head or board of the entity, as applicable, as per the procedure specified in the Cyber Security Policy, through a dedicated communication channel, isolated from internet, having cyber security system mandated under the regulation 6(3);

(5) ensure that all Operational Technology equipment, components, and parts thereof deployed for control and operation of power system shall comply with orders issued by the Central Government;

(6) ensure that the communication system of Operational Technology system is isolated from that of Information Technology system;

(7) ensure that the Operational Technology equipment and services are procured from trusted sources, in accordance with orders, directions, or guidelines issued by the Central Government from time to time;

(8) ensure that the Operational Technology environment is segmented into different trust levels on the basis of criticality, security requirements, and risk assessment;

(9) ensure that the communication system particularly channel, catering the Operational Technology data and information between the two entities is protected by owner of such system against cyber security threats.

CHAPTER V

Functions of Chief Information Security Officer and Information Security Division

7. (1) The Chief Information Security Officer and Alternate Chief Information Security Officer shall be citizens as well as residents of India and shall possess a degree in engineering or equivalent from a recognised institute, with at least fifteen years of experience in domain of power sector or Information Technology:

Notwithstanding anything contained in these regulations, the Authority may specify additional qualifications for Chief Information Security Officer of entity, through separate orders:

Provided that in absence of Chief Information Security Officer the roles and responsibilities of the Chief Information Security Officer shall be performed and executed by Alternate Chief Information Security Officer.

(2) The Chief Information Security Officer shall -

(a) be the nodal officer for all cyber security related matters;

(b) coordinate with all concerned stakeholders associated with the cyber security related matters.

(3) The functions of the Chief Information Security Officer, with the assistance of the Information Security Division shall include the following, namely -

(a) reporting of cyber security incidents within six hours to Computer Security Incident Response Team - Power and Indian Computer Emergency Response Team:

Provided that in case any incident is concluded as a cyber sabotage in critical systems, the same shall be reported within twenty-four hours;

(b) quarterly review of compliances as mandated in Cyber Security Policy;

(c) implementation of cyber security control measures for critical systems, as specified in Cyber Security Policy, to firm up their cyber resilience;

(d) in case of Critical Information Infrastructure or Protected System, implementation of validated cyber security control measure as per guidelines of National Critical Information Infrastructure Protection Centre;

(e) acting upon the cyber security related directives, guidelines and advisories issued by the Central

Government, the Authority, Indian Computer Emergency Response Team as well as Computer Security Incident Response Team - Power;

(f) gathering of cyber threat intelligence, its analysis, identification of threat vectors, assessment of cyber security risks and mitigation measures thereof;

(g) sharing of the detailed report of detected cyber security incidents, Action Taken Reports, Root Cause Analysis, and other relevant information with Computer Security Incident Response Team - Power and Indian Computer Emergency Response Team;

(h) retention of all cyber security related data, information and documents in the manner, form and period as specified in data retention policy;

(i) custody of all documents specified in First Schedule of these regulations;

(j) ensuring the updation of firmware and software of all critical systems, with patches as provided in Cyber Security Policy;

(k) ensuring the storage of logs of all Information and Communication Technology systems and logs as well as forensic records pertaining to cyber security incidents for the period, as specified in Cyber Security Policy;

(l) providing required information including allocated, used and unused public IPs to Computer Security Incident Response Team - Power;

(m) ensuring random testing of day-to-day operations of critical systems for being in conformance with its Cyber Security Policy and corrective measures thereof;

(n) prepare a procedure to facilitate remote access to cyber assets associated with non-critical system, for troubleshooting and emergency requirements including suitable security controls required and process to grant approval for such access;

(o) prepare a procedure, as specified in Cyber Security Policy, to facilitate safe and secure remote operation of Operational Technology system and updation thereof;

(p) ensure the development, implementation, review and updation of Cyber Security Policy, Cyber Crisis Management Plan, data retention policy, and backup policy;

(q) ensure the preparation, updation and review of asset register for cyber assets and critical systems as well as Cyber Risk Assessment and Mitigation Plan;

(r) ensure synchronisation of all Information Technology systems and Operational Technology systems to the reference time source, as specified under Cyber Security Policy.

CHAPTER VI

Cyber Security Policy

8. The Cyber Security Policy shall be aligned with the Business Continuity Plan of entity covering Operational Technology as well as Information Technology environment, as applicable, and the same may include -

(1) defined purpose and scope along with all applicable cyber security requirements and compliances thereof;

(2) for Protected Systems, provisions ensuring alignment with National Critical Information Infrastructure Protection Centre guidelines and control requirements;

(3) defined roles and responsibilities of relevant internal and external stakeholders;

(4) defined procedure to prepare cyber asset register, consisting of all cyber assets and classification thereof on the basis of their criticality and risk identified in Cyber Risk Assessment and Mitigation Plan; and update such procedure for detailed visibility and management of all cyber assets;

(5) defined procedure to identify all systems and classify such systems as critical systems, on the basis of a defined criteria considering their impact on the Business Continuity Plan, as well as record details of such systems in a register:

Provided that such procedure shall be reviewed and updated at least once in every financial year;

(6) defined procedure for Cyber Risk Assessment and Mitigation Plan to identify vulnerabilities and threats against each cyber asset and risk associated thereof, control and mitigation measures in commensuration with criticality of such risks and implementation thereof:

Provided that such procedure shall be reviewed and updated at least once in every financial year;

(7) defined mechanism to manage the vulnerabilities and risks in critical systems by timely identifying deficiencies and threats in such systems, including receipt of associated information from internal and external sources, analysis of such information, risk assessment, and management thereof:

Provided that such mechanism shall be reviewed and updated at least once in every financial year or upon commissioning of any new critical system, including replacement thereof, whichever is earlier;

(8) procedure to identify and report cyber sabotages in critical systems including receipt of such information from internal as well as external stakeholders;

(9) defined Incident Response and Recovery Plan detailing list of all type of incidents, risk analysis, and risk-based incident specific response plan for effective and timely restoration of affected system:

Provided that an incident which necessitates entity level strategic recovery plan shall be classified as a crisis;

(10) mechanism for random testing of day-to-day operations of critical system, for being in conformance with applicable policies, rules and regulations issued by Computer Security Incident Response Team - Power and other agencies designated by the Central Government in the area of cyber security:

Provided that such testing shall not interrupt the operations and functionality of such systems and safety thereof;

(11) access control mechanism to critical systems and cyber assets associated thereof, applications having public access, sensitive information and sensitive data, shall be governed by Access Management based on the principles of Authentication, Authorisation and Accounting criteria and criticality thereof:

Provided that a detailed procedure may be laid down to restrict the physical and logical access to documents and records specified under data retention policy;

(12) personnel risk assessment process to identify risks associated with personnel deployed by vendor, having authorised cyber or physical access to critical system and assets associated thereof or engaged for Operation or Maintenance or both of such system, on the basis of their roles and responsibilities including change in such roles and responsibilities and mitigating measures thereof:

Provided that for the employees engaged in day-to-day Operation and Maintenance or having authorised cyber or physical access to critical system and assets associated thereof, personnel risk assessment shall be carried out, on the basis of their roles executed and duration of deployment in such entrusted tasks, after their termination, resignation, and superannuation from their employment;

(13) mechanism to ensure that all access points to critical systems are secured physically and monitored continuously and also such access is restricted for physical protection of these systems and cyber assets associated thereof:

Provided that in case of a perceptible threat of physical damage to any of these systems or assets thereof, the physical access granted to any individual for such system or asset may be revoked;

(14) cyber supply chain risk management process to identify and assess cyber security risks associated with supply chain of critical systems and services thereof along with mitigative measures;

(15) defined procedure for remote access to cyber assets along with the details of authorisation to grant approval for such access on the basis of their criticality, such that such access is safe and secured through suitable control measures including minimum duration with least privileges, multi-factor authentication, and geo-fencing;

(16) defined procedure for remote operation of Operational Technology systems to meet the business requirement, on the basis of assessment of cyber risks associated with such operation and mitigation measures thereof:

Provided that such procedure shall be reviewed and updated once in every year or upon any change necessitated to meet business requirements, whichever is earlier;

(17) digital data protection and privacy policy in line with applicable rules and regulations issued by the Central Government;

(18) defined backup policy to ensure that online or offline backup data or both, as applicable, of all critical systems is up to date, but not older than a month, and retained in a separate and safe environment for the period as specified in the data retention policy:

Provided that the backup policy shall be reviewed and updated at least once in every financial year and ensure that the integrity of backup data and its restoration is tested such that the same meets the requirements of Business Continuity Plan;

(19) defined mechanism to ensure storage of sensitive data and its backup, as well as its transmission over dedicated communication channel or internet, is encrypted to ensure its confidentiality, integrity, and availability:

Provided that in case encryption of certain sensitive data is not feasible due to business requirements, the same, in unencrypted form, may be permitted over a dedicated communication channel;

(20) annual cyber security training program for capacity development of all personnel having authorised cyber or physical access or both to critical system and assets associated thereof;

(21) Internet access policy to monitor and restrict the internet traffic to ensure defined and authorised use only;

(22) phase out plan for obsolete cyber assets as well as those assets nearing end of useful life and management thereof along with their safe and secure disposal;

(23) plan for collaboration with industry, research institutes, stakeholders and academia to promote Research and Development activities in the domain of cyber security:

Provided that scope and assets for such collaboration may be identified after carrying out detailed risk assessment and such collaboration shall be effected after signing of Non-Disclosure Agreement;

(24) define criteria to classify the software updates including patches in critical systems into two categories-

(a) a software update that qualifies for requirement of prior cyber security audit before its deployment, and

(b) a software update that does not require prior cyber security audit before its deployment but necessitates such assessment in next cyber security audit.

Further, the suggestive list of software updates, which requires prior cyber security audit, is specified at the Second Schedule:

Provided that Computer Security Incident Response Team - Power, with the approval of Authority, may revise this list from time to time;

(25) defined change management process to record changes implemented in all critical systems and to ensure that planned changes on such systems and cyber assets associated thereof are controlled:

Provided that such process shall ensure that software updates including patches qualified for prior requirement of cyber security audit shall be version controlled along with provision of roll-back:

Provided further that the updates including patches in Operational Technology system shall be digitally signed by original equipment manufacturer and such updates may be deployed in offline mode, after their risk assessment and successful testing in simulated environment. However, in case the digital signature of original equipment manufacturer is not available for any patch, the validity and authenticity of such patch shall be verified;

(26) a mechanism to facilitate storage of logs and forensic records as mandated in data retention policy in a safe and secured environment;

(27) a procedure to select reference time source, after assessing its associated cyber risks for synchronizing all processing systems of Information Technology and Operational Technology environment to such source:

Provided that the reference time source selected for Operational Technology system shall be, either terrestrial or India specific satellite based and independent of internet;

(28) defined procedure for logical separation of Operational Technology system from Information Technology system to ensure safe and secure operation of both Information Technology systems as well as Operational Technology systems:

Provided that the identified data and information from Information Technology to Operational Technology and that from Operational Technology to Information Technology shall flow through separate communication channel and unidirectional gateway;

(29) defined procedure by cross border entities to identify and classify the data as well as information including real time data permitted to be communicated beyond national boundaries, on the basis of risk assessment and business requirements:

Provided that Computer Security Incident Response Team - Power may review and assess such procedure, data and relevant information, as and when required;

(30) defined procedure to identify web applications along with a criterion to classify such applications as critical web applications, on the basis of their impact on business operations and continuity;

(31) defined procedure for safe and secure disposal of out of service or obsolete cyber asset and data stored therein;

(32) defined procedure for safe and secure disposal of sensitive data and sensitive information;

(33) data retention policy specifying the manner and form of retention of various documents and records as well as data and information including -

(a) backup of data of critical systems;

(b) record of logs, risk assessment, and approval thereof for each grant of remote access to critical systems;

(c) logs and grant of approval associated with interconnection of Operational Technology system with Information Technology system;

(d) cyber security documents including certificates of cyber security tests, Factory Acceptance Test and Site Acceptance Test results, cyber security audit reports and other documents as mandated by the Central Government;

(e) record of changes including software updates and patches implemented in critical systems:

Provided that the data retention policy shall be reviewed and updated at least once in every financial year and the data, information and documents shall be retained to ensure -

(a) at least last two working data backups are available;

(b) risk assessment, physical record of grant of approval and logs with respect to each remote access to critical system are available for at least one year;

(c) reports of Factory Acceptance Test and Site Acceptance Test including test of cyber security requirements are available throughout life of cyber asset;

(d) record of risk assessment for remote operation in Operational Technology environment along with approval received thereof are available for at least one year;

(e) cyber security audit reports of last three years are available;

(f) certification audit reports of last four years are available;

(g) self-audit reports of last three years are available;

(h) logs of all Information and Communication Technology systems, inter-connection of Operational Technology system with Information Technology system and forensic records are available for a period of one hundred and eighty days;

(i) the logs associated with an incident including logs pertaining to one hundred and eighty days prior and post to such incident are available for at least three hundred and sixty-five days from occurrence of such incident:

Provided further that the access to such information, data and documents may be restricted to authorised persons only, on the basis of procedure defined under access control mechanism:

Provided also that the Authority may, through separate orders include any other document and specify any other manner, mode, and period for retention of documents under data retention policy.

CHAPTER VII

Cyber Crisis Management Plan

9. **The cyber crisis management plan shall** – (1) include detailed Standard Operating Procedure to detect and identify all incidents, criteria to classify an incident as a crisis and list of all possible crisis scenarios;

(2) identify stakeholders along with their roles and responsibilities for all possible crises and communication of such roles as well as responsibilities thereof;

(3) include the manner and mode of communication with internal as well as external stakeholders for close coordination during the crisis;

(4) include mitigative measures to minimize the impact and recover from crisis at the earliest.

10. **Responsibilities of the entities** – The entity shall -

(1) ensure availability of all essential communications with relevant internal and external stakeholders during cyber crisis;

(2) test the efficacy of Cyber Crisis Management Plan at least once in every year through exercises and mock drills for scenarios selected for that year out of all identified crisis scenarios specified under it:

Provided that the selection of scenarios in any year shall not overlap with the scenarios tested and verified earlier unless the cycle of all listed scenarios has been completed for testing and verification;

(3) prepare a detailed report of each actual crisis handled and recovered along with experience gained, lessons learnt, feedback received, lapses observed and proposed measures thereof:

Provided that the relevant information including brief about actual crisis, its handling and takeaways shall be shared with Computer Security Incident Response Team - Power and other stakeholders for collective improvement of cyber security ecosystem of power sector:

Provided further that the Cyber Crisis Management Plan shall be updated by incorporating qualified observations of its own and that of other stakeholders to improve its cyber security posture.

CHAPTER VIII

Cyber Security requirements for Vendor

11. **Cyber Security requirements for vendor -** The vendor shall -

(1) provide documented and tested procedures as well as recovery plan to the entity for restoration of systems supplied by them from potential cyber crisis scenarios;

(2) ensure, either digitally signed or validated and authenticated, security patches and updates for all systems as well as components supplied by them are available to the entity throughout their contract period or useful life of such systems, whichever is later;

(3) provide detailed document to the entity consisting of all requirements and processes including security patches as well as updates required to be installed on the third-party components to integrate a component or sub-system supplied by them;

(4) provide details of end of support or end of life of software, hardware and system to the entity, as applicable, supplied by them including those sourced from third parties;

(5) provide Bill of material to the entity, as per Indian Computer Emergency Response Team guidelines issued from time to time, comprising detailed list of all components supplied by them for applications including firmware, deployed in critical systems;

(6) ensure that the hardware and software are hardened by enabling all inherent security capabilities, secured configuration, and controls, before supplying to the entity;

(7) establish a formal structured process for entities to report vulnerabilities in the products and services. Further, the vendor shall furnish such vulnerabilities to the Computer Security Incident Response Team - Power, through its vulnerability disclosure and management program.

12. **Responsibility of vendors** - In the case of Distributed Generation Resource of prosumers, it shall be the responsibility of vendor to -

(1) ensure that any application, associated monitoring and control servers, and the real-time data of such systems including any data or information hosted on cloud platforms as well as associated historical data or information, be stored in an encrypted, secure, and protected environment and shall reside exclusively within India;

(2) ensure that remote access and remote operation of the grid-connected devices as well as exchange of their real time data and information with remote applications, aggregators, and distribution licensees shall be established through secure channel after mutual authentication and such communication shall be encrypted;

(3) provide such information as may be required for the purpose of verification of a trusted source, in accordance with the orders, directions or guidelines issued by the Central Government from time to time:

Provided that this regulation for the existing Distributed Generation Resource of prosumers shall come into force on such date, as may be specified by the Authority through separate order.

Chapter IX

Cyber Security Audit

13. **Cyber Security Audit** - The entity shall ensure that -

(1) cyber security audit shall be conducted, as per scope detailed in cyber security audit guidelines and directions issued by Computer Security Incident Response Team - Power and other cyber security agencies designated by the Central Government;

(2) the scope of cyber security audit shall also include verification of closure of all audit findings identified in the previous cyber security audit;

(3) the auditor submits its cyber security audit report within six weeks of its commencement, and all critical and high-risk vulnerabilities shall be addressed within a period of one month and medium as well as low risks vulnerabilities within a period of three months from the date of submission of cyber security audit report by the auditor:

Provided that appropriate compensatory controls shall be deployed to contain critical and high-risk vulnerabilities, till audit clearance of such vulnerabilities.

14. **Responsibilities of Chief Information Security Officer** -

(1) Chief Information Security Officer shall review the audit compliances and ensure that the auditor shall submit its cyber security audit closure report within six months from commencement of cyber security audit.

(2) Chief Information Security Officer shall report major audit findings including critical and high-risk vulnerabilities observed in cyber security audit closure report along with any non - compliances with respect to critical systems to the head or board of the entity, as the case may be:

Provided that Chief Information Security Officer - Ministry of Power, may ask for audit closure report of any entity at any point of time for examination and, if need be, after seeking written clarification, with prior approval of the Authority and prior notice to such entity, may appoint a third-party auditor for verification of audit compliances, the cost of which shall be borne by entity:

Provided further that in case the findings of the third-party audit are in variance with the observations of cyber security audit closure report, Chief Information Security Officer - Ministry of Power may take further necessary action.

CHAPTER X

MISCELLANEOUS

15. **Self-audit** - The entity shall conduct self - audit to assess its compliance with these regulations every financial year:

Provided that, for cyber security and compliance with these regulations, the entity may designate any member of the board or of senior management, as the case may be, to be responsible for such compliance:

Provided further that the entity shall address the non-compliances in a time bound manner and ensure that all such non-compliances are addressed before self-audit scheduled in next financial year:

Provided also that Chief Information Security Officer - Ministry of Power, based on the facts available or reported by any individual, may examine compliance report of any entity and after seeking written clarification, with prior approval of the Authority and prior notice to such entity, may appoint a third-party auditor to verify claim made by the entity, the cost of which shall be borne by such entity.

16. In specific cases, after seeking written clarifications and examination thereof, Chief Information Security Officer - Ministry of Power may recommend to the Central Government for initiation of appropriate proceedings under relevant provisions of the Information Technology Act, 2000 (21 of 2000) or to file a petition before Appropriate Commission for proceedings under section 142 of the Act.

17. **Power to Relax** - The Authority through an order, for reasons to be recorded in writing, may relax any of the provisions of these regulations on its own motion or on an application made before it by an interested person to remove the hardship arising out of the operation of any of these regulations, applicable to a class of persons.

FIRST SCHEDULE

[see clause 3(i) of regulation 7]

The following documents and information shall be retained -

1. Cyber Security Policy along with documents and procedures listed therein.
2. Cyber Crisis Management Plan.
3. Data Retention Policy and all documents and information listed thereunder.
4. ISO/ IEC 27001 Certificate or Technical Criteria Certificate.
5. Asset register for cyber assets and critical systems.
6. Cyber Risk Assessment and Mitigation Plan.
7. Incident Response and Recovery Plan.
8. Cyber Security Incident Reporting register.
9. Bill of materials.
10. Business Continuity Plan.
11. Remote operation procedure.
12. Remote access procedure.

THE SECOND SCHEDULE

[see clause 24 of regulation 8]

The suggestive criteria for software updates requiring Prior Cyber Security Audit

Software updates including modifications and enhancements to applications, websites, web portals, and associated systems meeting any of the following criteria shall mandatorily require a successful cyber security audit prior to deployment, namely -

1. **Critical system impact**: Updates that affect core operational processes, such as energy generation, transmission, distribution or load management wherein vulnerabilities could compromise the functionality or reliability of critical infrastructure.
2. **Access control modifications**: Updates that alter user authentication, authorisation mechanisms, or administrative privileges including those involving identity management systems or access control policies.
3. **Integration with third-party systems**: Updates involving integration with external systems, applications or third-party services especially those that exchange sensitive data or enable cross-platform communication.
4. **Security protocol changes**: Updates introducing changes to encryption standards, data transmission protocols or other security-related configurations that could impact the protection of sensitive information.
5. **Introduction of new features or interfaces**: Updates adding significant new functionalities, user interfaces or Application Programming Interfaces that could present potential attack surfaces.
6. **Resolution of security vulnerabilities**: Updates addressing previously identified Critical and High impact vulnerabilities where an incomplete or improper implementation could exacerbate security risks.
7. **Incident response and monitoring systems**: Updates affecting systems or tools related to cyber security monitoring, incident response or log management wherein any disruption could hinder the ability to detect or respond to threats effectively.
8. **Reform or regulatory mandated systems**: Updates impacting systems subject to regulations or pursuant to reforms programs of Appropriate Government.

SHARVAN KUMAR, Secy.

[ADVT.-III/4/Exty./253/2026-27]

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.

VINOD KUMAR Digitally signed by VINOD KUMAR Date: 2026.08.05 16:30:06 +05'30'