REGULATORY • CENTRAL ELECTRICITY AUTHORITY

Cyber Security in Power Sector

CEA (Cyber Security in Power Sector) Regulations, 2026

Gazette notification: 31 July 2026 | **In force from:** 1 April 2027

Gazette of India • Extraordinary • Part III—Section 4

Brought to you by powerppt.com

Quick Reference

What changed, what matters

EFFECTIVE DATE

Force from 1 Apr 2027; Regs 5(9), 5(24), 5(33), 5(39), 6(2), 6(7) commence on dates separately notified.

INCIDENT REPORTING

6 hours to CSIRT-Power & CERT-In; cyber sabotage in critical systems reported within 24 hours.

COVERAGE

Entities owning/operating OT + connected IT infrastructure for the interconnected power system. Gencos, captive plants and ESS covered at 50 MW+. Power exchanges/OTC platforms covered (except Regs 6, 11, 12).

AUDIT & CERTIFICATION

Audit report within 6 weeks of commencement; critical/high risks fixed in 1 month, medium/low in 3 months.

GOVERNANCE

CISO + Alternate CISO, dedicated 24x7 Information Security Division, annually reviewed Cyber Security Policy, Cyber Crisis Management Plan.

VENDOR CONTROLS

Recovery procedures, patches, EOL data, Bill of Materials, hardened configuration, structured vulnerability disclosure.

OT SEGREGATION

OT systems physically isolated from Internet and IT systems, with tightly controlled, risk-assessed exceptions and perimeter security.

RECORD RETENTION

First Schedule: 12 categories of documents including policies, plans, asset registers, incident registers.

Applicability & Scope

Regulation 2 — who these regulations cover

COVERED ENTITIES

- ✓ Generating companies, captive generating plants & Energy Storage Systems — installed capacity ≥ 50 MW
- ✓ Transmission & distribution licensees
- ✓ National / Regional / State Load Despatch Centres
- ✓ Power exchanges & Over-the-Counter platforms (except Regs 6, 11 & 12)
- ✓ All entities owning, operating or managing OT infrastructure tied to the interconnected power system, and connected IT infrastructure

BELOW 50 MW

Entities under 50 MW installed capacity are encouraged (not mandated) to adopt CERT-In's "15 Elemental Cyber Defense Controls for MSMEs" as a minimum baseline.

VENDOR SCOPE

Vendors must comply with Regulations 11 & 12 (vendor cyber security requirements and Distributed Generation Resource / prosumer obligations), as applicable.

Regulations come into force 1 April 2027

Governance Structure

Regulations 5(1)–(9) & Chapter V — CISO and Information Security Division

1

CISO & Alternate CISO

Senior-management employees; positions never vacant simultaneously; min. 3-year tenure; reports to head of entity (or holding/parent company, as applicable).

2

Eligibility

Citizen & resident of India; engineering or equivalent degree; ≥ 15 years' experience in power sector or IT; ≥ 5 training man-days per financial year.

3

Information Security Division

24x7 operational, sufficient staffing, domain-certified staff, min. 3-year staff tenure; headed by the CISO, based within India.

4

Cyber Security Policy

Documented, board/head-approved, reviewed annually; aligned with the entity's Business Continuity Plan.

5

Cyber Crisis Management Plan

Prepared with CSIRT-Power, vetted by CERT-In, approved by head/board, reviewed annually.

6

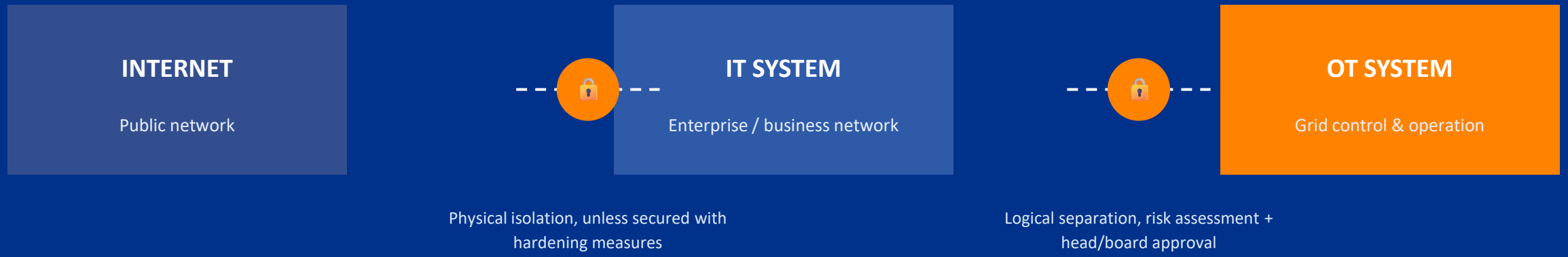
Public Disclosure

CISO/Alternate CISO contact details published and kept current; shared with CSIRT-Power and stakeholders.

POWERPPT.COM

OT / IT Segregation

Chapter IV, Regulation 6 — additional requirements for Operational Technology



KEY OT REQUIREMENTS

- Perimeter cyber security devices (firewall) at every OT interconnection point
- Control/operation & real-time data over a dedicated channel, isolated from internet, confined to national boundaries (cross-border data via unidirectional gateway only)
- Remote operation only within India, with prior head/board approval, via a dedicated isolated channel
- OT communication system kept separate from IT communication system; segmented into trust levels by criticality
- OT equipment, components & services procured only from Central-Government-notified trusted sources

Incident Reporting Timelines

Regulation 7(3)(a) — CISO reporting obligations

6 HRS

Cyber security incident reported to CSIRT-Power & CERT-In

24 HRS

Incidents concluded as cyber sabotage in critical systems

30 DAYS

New critical system details furnished to CSIRT-Power post go-live

CYBER SECURITY AUDIT TIMELINES (Regulation 13)

6 weeks

Auditor submits audit report from commencement

1 month

Critical & high-risk vulnerabilities addressed

3 months

Medium & low-risk vulnerabilities addressed

9–15 months

Gap allowed between two consecutive audits (annual, min–max)

POWERPPT.COM

Vendor Requirements

Chapter VIII, Regulations 11–12 — obligations flowing to suppliers & contractors

1

Recovery Procedures

Documented, tested recovery plans for systems supplied, to restore from cyber crisis scenarios.

2

Patches & Updates

Digitally signed / validated security patches available through contract period or useful life, whichever later.

3

End-of-Life Disclosure

Details of end-of-support / end-of-life for software, hardware & systems, including third-party sourced items.

4

Bill of Materials

Detailed component/firmware inventory for items deployed in critical systems, per CERT-In guidelines.

5

Hardened Configuration

Hardware & software hardened — inherent security capabilities and controls enabled before supply.

6

Vulnerability Disclosure

Formal structured process for entities to report flaws; vendor shares vulnerabilities with CSIRT-Power.

POWERPPT.COM

Record Retention

First Schedule — 12 categories of documents to be retained by the CISO

01 Cyber Security Policy	**02** Cyber Crisis Management Plan	**03** Data Retention Policy	**04** ISO/IEC 27001 or Technical Criteria Certificate
05 Asset Register (cyber assets & critical systems)	**06** Cyber Risk Assessment & Mitigation Plan	**07** Incident Response & Recovery Plan	**08** Cyber Security Incident Reporting Register
09 Bill of Materials	**10** Business Continuity Plan	**11** Remote Operation Procedure	**12** Remote Access Procedure

Selected retention periods: audit reports – 3 yrs | certification audit reports – 4 yrs | self-audit reports – 3 yrs | ICT & interconnection logs – 180 days | incident-linked logs – 365 days

POWERPPT.COM

Software Update Triggers

Second Schedule — situations requiring a successful cyber security audit before deployment

1. Critical system impact (generation, transmission, distribution, load management)
2. Access control modifications (authentication, authorisation, admin privileges)
3. Integration with third-party systems exchanging sensitive data
4. Security protocol changes (encryption, transmission protocols)
5. New features, user interfaces or APIs widening the attack surface
6. Resolution of previously identified critical/high impact vulnerabilities
7. Incident response & monitoring system changes
8. Reform or regulatory-mandated system updates

Regulation Structure

10 Chapters and 2 Schedules

I	Preliminary
II	Computer Security Incident Response Team – Power
III	General Cyber Security Requirements
IV	Additional Requirements for OT Systems
V	Functions of CISO & Information Security Division
VI	Cyber Security Policy
VII	Cyber Crisis Management Plan
VIII	Cyber Security Requirements for Vendor
IX	Cyber Security Audit
X	Miscellaneous

FIRST SCHEDULE

Documents & information to be retained — 12 categories (Reg. 7(3)(i))

SECOND SCHEDULE

Suggestive criteria for software updates requiring prior cyber security audit — 8 situations (Reg. 8(24))

POWERPPT.COM

Excite your officer/staff with the stunning presentations at Powerppt.COM

Thanks for using PowerPPT's Presentation!



Brought to you by powerppt.com