CEA (Cyber Security in Power Sector) Regulations, 2026

Notified 31 July 2026 | In force from 1 April 2027 | *Gazette of India, Extraordinary, Part III—Section 4*

COVERAGE & APPLICABILITY

Entities owning/operating OT infrastructure tied to the interconnected power system, and connected IT infrastructure. Gencos, captive plants & Energy Storage Systems covered at ≥ 50 MW installed capacity. Power exchanges & OTC platforms covered (except Regs 6, 11, 12). Entities below 50 MW are encouraged to adopt CERT-In's 15 baseline MSME controls.

GOVERNANCE

Every entity designates a CISO and Alternate CISO (senior management, ≥ 15 yrs' experience, min. 3-year tenure), backed by a 24x7 Information Security Division. Requires a board-approved Cyber Security Policy (reviewed annually) and a Cyber Crisis Management Plan vetted by CERT-In.

OT / IT SEGREGATION

OT systems physically isolated from the Internet and IT systems; logical separation only with risk assessment and head/board approval. Control, operation and real-time data flow over a dedicated channel confined to national boundaries; remote operation permitted only within India via a dedicated isolated channel, with prior approval.

INCIDENT REPORTING & AUDIT

Cyber security incidents reported to CSIRT-Power and CERT-In within 6 hours; cyber sabotage in critical systems within 24 hours. Annual cyber security audit: report within 6 weeks of commencement; critical/high-risk findings closed in 1 month, medium/low in 3 months. Audit gap: 9–15 months between consecutive audits.

VENDOR REQUIREMENTS

Vendors provide documented recovery procedures, digitally-signed patches through the contract/useful life, end-of-life disclosures, Bill of Materials, hardened configurations, and a structured vulnerability disclosure programme with CSIRT-Power.

RECORD RETENTION (FIRST SCHEDULE)

12 categories retained by the CISO — Cyber Security Policy, Crisis Management Plan, Data Retention Policy, ISO 27001/Technical Criteria Certificate, Asset Register, Risk Assessment & Mitigation Plan, Incident Response & Recovery Plan, Incident Register, BOM, Business Continuity Plan, Remote Operation & Remote Access Procedures.

REGULATION STRUCTURE

Ch. I Preliminary • Ch. II CSIRT-Power • Ch. III General Cyber Security Requirements • Ch. IV OT-specific Requirements • Ch. V CISO & Information Security Division • Ch. VI Cyber Security Policy • Ch. VII Cyber Crisis Management Plan • Ch. VIII Vendor Requirements • Ch. IX Cyber Security Audit • Ch. X Miscellaneous • First Schedule (retained documents) • Second Schedule (software update audit triggers)

SOFTWARE UPDATES REQUIRING PRIOR AUDIT (SECOND SCHEDULE)

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

EFFECTIVE DATES & ENFORCEMENT

DEFERRED COMMENCEMENT

Regulations 5(9) [Information Security Division], 5(24) [ISO 27001/Technical Criteria Certificate], 5(33) [mandatory training completion], 5(39) [trusted-source procurement], 6(2) and 6(7) [OT perimeter security & trust-level segmentation] come into force on dates to be separately notified by the Authority, with prior Central Government approval — not from 1 April 2027.

SELF-AUDIT & ESCALATION

Every entity conducts a self-audit each financial year and rectifies non-compliances before the next cycle. CISO–Ministry of Power may call for audit/compliance reports, seek written clarification, and — with the Authority's prior approval — appoint a third-party auditor (cost borne by the entity) or recommend proceedings under the IT Act, 2000 / Section 142 of the Electricity Act.