# New York Power and Energy Cybersecurity Preparation Guide

For utility CISOs, compliance leads, control engineers and DER operators.

Edition 2026-11-03 · Part of the New York Audit Preparation Pack at newyorkcomputerforensics.com/resources/new-york-cybersecurity-audit-preparation/

New York power and energy organizations can answer to three different frameworks at once. The PSC's 16 NYCRR Part 1200 covers the information technology of most public utility companies; NERC CIP covers registered entities and their BES Cyber Systems; and DOE's distribution baselines guide distribution utilities and DER operators on a voluntary basis. Map which ones reach your entity and which systems they cover before you gather records.

## 16 NYCRR Part 1200 at a glance

| Requirement | Timing and rule | Record to keep |
|---|---|---|
| Who is covered | Public utility companies under Public Service Law section 2(23), except among others water works corporations with fewer than 50,001 service connections, electric corporations with fewer than 50,000 service lines, gas corporations that are small businesses, telephone corporations and municipal corporations. 1200.1(c) | Entity determination and any Notice of Exemption |
| Compliance timing | The adopted text sets June 1, 2026 as the effective date. General requirements apply 180 days later, by November 28, 2026; 1200.4(b), 1200.5, 1200.9, 1200.11, 1200.12 and 1200.14(b) by June 1, 2027; 1200.6, 1200.8, 1200.13, 1200.14(a) and 1200.15 by December 1, 2027. 1200.24, 1200.25 | Implementation plan by section |
| Incident notice | To the Department of Public Service as promptly as possible and no later than 72 hours after the utility reasonably believes a cybersecurity incident has occurred or is occurring, with no transition period. 1200.21(a) | Notice record and updates |
| Event log | Every cybersecurity event and incident logged and kept at least three calendar years, available within 10 calendar days of a request. 1200.21(b) | Event and incident log |
| Third party audit | A third party audit of IT and nonpublic information cybersecurity every year. 1200.18 | Audit report and remediation |
| Annual certification | Written statement of compliance for the prior calendar year by June 30, commencing June 30, 2027; supporting records kept five years. 1200.21(c), 1200.24 | Signed certification and its records |

© 2026 Global Digital Forensics, Inc. All rights reserved.

## Preparation checklist

Work through each row with the owner of the record. The companion CSV in this pack (power-energy-preparation-checklist.csv) carries the same rows with columns for status, owner, evidence reference and open questions.

| ID | Topic | Record to gather | Next step | Source |
|---|---|---|---|---|
| PE-01 | Entity and framework map | Record the entity, its PSC status, NERC registrations and contracts, and the compliance owner for each framework. | Decide which of Part 1200, NERC CIP and the DOE baselines reach the entity before choosing requirements. | 16 NYCRR 1200.1(c); NERC CIP standards |
| PE-02 | IT, OT and BES scope | Prepare an asset and function map that separates business IT, plant OT and any BES Cyber Systems. | Apply NERC CIP to the systems it reaches and keep Part 1200 focused on information technology. | 16 NYCRR 1200.1; NERC CIP standards |
| PE-03 | Risk assessment | Gather the risk assessment and the dependencies that affect service, safety, customer information and recovery. | Rank risks with operations and compliance by operational consequence. | 16 NYCRR 1200.9; DOE baselines |
| PE-04 | Access and third party paths | Gather identity records, vendor connections, approvals and privileged access settings. | Have owners confirm who can reach each environment and how sessions are approved. | 16 NYCRR 1200.7, 1200.11, 1200.12 |
| PE-05 | Asset and change records | Reconcile configuration, software, network and engineering change records. | Record owners and baseline differences before selecting a review sample. | DOE baselines; NERC CIP standards |
| PE-06 | Logs and the event record | Gather log coverage, retention, time settings and the cybersecurity event and incident log. | Keep the event log for three calendar years and be ready to produce it within 10 days. | 16 NYCRR 1200.6, 1200.21(b) |
| PE-07 | Safe validation plan | Document authorized test methods, device constraints, test windows, stop conditions and recovery contacts. | Use passive records or controlled replicas first; active production work needs operator approval. | DOE baselines |
| PE-08 | Testing and third party audit | Gather penetration test and vulnerability assessment results and the latest third party audit. | Trace each correction to an observable result before the next audit. | 16 NYCRR 1200.5, 1200.18 |
| PE-09 | Incident notice and recovery | Gather the incident response plan, the DPS notice path, backup and restore evidence and exercise lessons. | Confirm the 72 hour notice path and the owner who authorizes recovery. | 16 NYCRR 1200.16, 1200.21(a) |
| PE-10 | Annual certification | Index the records that support the June 30 certification and any areas needing material improvement. | Prepare for the first certification due June 30, 2027 and keep supporting records five years. | 16 NYCRR 1200.21(c), 1200.24 |

© 2026 Global Digital Forensics, Inc. All rights reserved.

## Sources


- NYS Public Service Commission, Case 25-M-0302, Memorandum and Resolution Approving Adoption of Information Technology Cybersecurity Regulations (16 NYCRR Part 1200), issued April 17, 2026. Covered utilities, program, CISO, testing, third party audits, incident notice, event log and the annual certification. Checked 2026-11-03. https://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7B50419C9D-0000-C957-89B7-5F83A397191B%7D
- NERC Critical Infrastructure Protection (CIP) Reliability Standards. Requirements for registered entities with BES Cyber Systems. Checked 2026-11-03. https://www.nerc.com/standards/reliability-standards/cip
- U.S. Department of Energy, Cybersecurity Baselines for Electric Distribution Systems and DER. Voluntary baselines and implementation guidance for distribution utilities and DER operators. Checked 2026-11-03. https://www.energy.gov/ceser/cybersecurity-baselines-electric-distribution-systems-and-der-and-guidance


### Scope Your Assessment

The first call is a free consultation with a senior security lead. We review the systems, the review or audit you face and its timing, and recommend the assessment depth that answers it. Requests are handled in confidence.

**Call (800) 868-8189, 24/7 · New York office (212) 561-5860**

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.

© 2026 Global Digital Forensics, Inc. All rights reserved.