New York Drinking Water Cybersecurity Preparation Guide

For owners, operators and IT and OT teams at New York community water systems.

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

10 NYCRR Appendix 5-E covers community water systems serving more than 3,300 people and adds duties above a combined wholesale and retail population of 50,000. Covered systems have until January 1, 2027 to comply; operator training and DOH incident reporting took effect on adoption, March 11, 2026. Use this guide to organize the CVA, the cybersecurity program, training and reporting records, and use the companion CSV to assign owners and evidence references.

DOH actions and timing

Requirement	Timing and rule	Record to keep
Review and update the CVA	At least annually, and within 30 days after major water facility infrastructure changes are made operational. Submit to DOH every five years and after major changes under 5-1.33(e).	CVA, review dates and submission record
Cybersecurity program	Established from the CVA findings by January 1, 2027 and updated as technology, staff or the system change. Above 50,000: the designated individual certifies the program every five years and reports to the governing body at least annually.	Program, CVA link, certification and annual report
Operator training	At least one hour of cybersecurity training every three years for every certified drinking water operator, with no exclusions. In effect since March 11, 2026; each operator completes it by the end of the first full registration cycle after that date.	Approved course and completion records
Vulnerability reporting	From January 1, 2027, within 48 hours of identifying a CVA vulnerability that may affect Subpart 5-1 compliance or pose a risk to public health.	Notification record and updated CVA
Incident reporting	As soon as possible and no later than 24 hours after determining that a cybersecurity incident has created or may create a public health hazard. 5-E.9	DOH incident report and response chronology
Significant deficiencies	Consult DOH within 30 days and start or complete corrective action within 120 days under 5-1.71(c).	Mitigation plan, owner, dates and correction evidence

Preparation checklist

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

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

ID	Topic	Record to gather	Next step	Source
DW-01	System scope and accountable roles	Record community system status, population served, ownership and the authorized representative.	Above a combined population of 50,000, name the qualified designated individual and schedule the annual governing body report.	10 NYCRR Appendix 5-E, 5-E.1 and 5-E.4
DW-02	Cyber assets and connections	Map treatment, pumping, storage, communications and every IT or external connection to OT.	If the system claims the exclusion for no physical or logical OT connection, document the basis and keep training, the emergency response plan and reporting in place.	10 NYCRR Appendix 5-E, 5-E.2 and 5-E.6
DW-03	CVA review and submission	Gather the CVA, its approval, review dates, major infrastructure changes and submission history.	Schedule the annual review and a review within 30 days after any major change is made operational.	10 NYCRR Appendix 5-E, 5-E.5; DOH requirements table
DW-04	Program and access controls	Gather the cybersecurity program, account inventory, remote access controls, MFA or documented compensating controls and the annual access review.	Close gaps before January 1, 2027, and schedule control tests within operator approved windows.	10 NYCRR Appendix 5-E, 5-E.6
DW-05	Vulnerability reporting and correction	Record each qualifying CVA finding, when it was identified, the DOH notice, the mitigation owner and correction evidence.	From January 1, 2027, report within 48 hours, consult DOH within 30 days and track the 120 day correction period.	10 NYCRR Appendix 5-E, 5-E.1(c) and (d); DOH requirements table
DW-06	Incident escalation and DOH reporting	Gather the incident definition, the authorized reporter, escalation contacts and the DOH reporting method.	Notify DOH no later than 24 hours after determining that an incident created or may create a public health hazard.	10 NYCRR Appendix 5-E, 5-E.9
DW-07	Response and recovery	Locate the cyber incident response plan, protected backups, restoration steps, manual fallback plans and exercise records.	Name the owner who restores each critical function and test the plan.	10 NYCRR Appendix 5-E, 5-E.6 and 5-E.8
DW-08	Operator training	Gather DOH approved training records for every certified operator.	Complete the first hour by the end of each operator's first full registration cycle after March 11, 2026, then every three years, and keep completion records ready for DOH.	10 NYCRR Appendix 5-E, 5-E.7

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

Sources

- 10 NYCRR Subpart 5-1, Appendix 5-E, Cybersecurity Requirements for Public Water Systems. Applicability, exclusions, CVA, cybersecurity program, training, emergency response plan and DOH reporting. Checked 2026-11-03. https://healthweb-back.health.ny.gov/regulations/nycrr/title_10/part_5/docs/appendix_5e.pdf
- NYS Department of Health, Drinking Water System Cybersecurity Requirements Table (revised March 2026). The six DOH actions with responsible party, frequency and documentation. Checked 2026-11-03. https://www.health.ny.gov/environmental/emergency/water/drinking/cybersecurity/cybersecurity_requirements_table.htm
- NYS Department of Health, Overview of Cybersecurity Regulation for drinking water systems. Covered system populations, program elements, reporting contacts and exclusions. Checked 2026-11-03. https://www.health.ny.gov/environmental/emergency/water/drinking/cybersecurity/cybersecurity_overview.htm

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.