

New York wastewater cybersecurity preparation

Separate permit-wide incident reporting, POTW control requirements and individual operator training. Keep the facility, design flow, permit and responsible municipal authority attached to the preparation record. The operator retains process and safety authority.

Scope first. DEC identifies reporting provisions effective March 26, 2026; ERP/control provisions effective March 11, 2027; and first annual certifications due March 28, 2027. Some training provisions begin with certifications expiring from January 1, 2027. Scope and current instructions still need entity-specific review.

Review period: _____ Responsible role: _____

Item	Records and next decisions	Working status
WW-01	Permit and facility scope Record the SPDES permit, POTW status, design flow and legally responsible party. Next: Distinguish all-permittee reporting duties from POTW controls and flow-dependent provisions. Source: DEC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
WW-02	Reporting and escalation route Gather the incident triage route, authorized contacts and current reporting instructions. Next: Have the responsible team validate deadlines; this tool does not send incident reports. Source: DEC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
WW-03	ERP and cybersecurity IRP Locate the emergency response and cyber incident plans and their controlled copies. Next: Identify gaps, owners and the correct phase-in dates for each document. Source: DEC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
WW-04	Access and vendor-control records Gather account inventories, remote-support methods, approvals and termination records. Next: Reconcile access rules with actual authorized paths to treatment and collection systems. Source: DEC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*

Statuses are self-reported and unverified. Gathered means a record was located, not that a control passed. *Document the basis for any not-applicable choice in the editable CSV.

CONTINUE / EVIDENCE AND OPEN DECISIONS

Item	Records and next decisions	Working status
WW-05	Vulnerability-management method Gather the approved method, device constraints, findings and corrective-action register. Next: Plan safe evidence review before any operator-approved production interaction. Source: DEC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
WW-06	Network and monitoring boundaries Gather secure-network documentation and the monitoring/logging scope decision. Next: Confirm how design flow affects specific requirements; do not presume all facilities share a tier. Source: DEC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
WW-07	Recovery, training and exercises Gather restore/exercise records and the operator certification/training schedule. Next: Confirm course approval and certification timing with DEC; a generic course may not count. Source: DEC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
WW-08	Certification and unresolved decisions Prepare an index of evidence, exceptions, open work and authorized signatories. Next: Only the appropriate responsible official evaluates the filing; GDF preparation is not certification. Source: DEC1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*

Finish the preparation record

In the companion CSV, record an owner, evidence reference and open question for each item. Keep actual files in your approved repository. Ask the responsible technical, compliance and legal teams to resolve scope, phase-in dates and signatory authority. This worksheet performs no audit, scan, filing or legal determination.

Official sources

DEC1 - [NYS DEC Wastewater Cybersecurity Resources](#)

Discuss technical scope: newyorkcomputerforensics.com/contact/ | 212-561-5860. Do not send operational records or evidence through the public form.