New York Water Duty and Source Reference

Edition November 18, 2026

The same duty records used in the HTML toolkit, editable workbook and CSV. Review applicability before assigning work. The companion guide explains the audit path.

Requirement text paraphrases the cited authority. Evidence requests, examination steps and acceptance descriptions are GDF planning methods, not regulator approval. Unknown scope or unexamined evidence stays unresolved. A completed worksheet does not certify compliance.

Community water cybersecurity controls

Community water system serving more than 3,300 people. Evaluate Appendix 5-E.2 exclusions against documented physical and logical connections. Municipal ownership alone is not an exclusion.

NYDOH-APP5E 5-E.1(a), 5-E.2

Additional duties above 50,000 people

Covered community water system with combined wholesale and retail population greater than 50,000. Do not substitute service connections or customer accounts for population.

NYDOH-APP5E 5-E.1(a), 5-E.4, 5-E.5(b), 5-E.6(b), 5-E.6(c)(2)(iv), 5-E.6(c)(6)

Covered water systems including isolated systems

Written incident response planning and qualifying incident reporting continue for covered systems using the no connection exclusion. Operator training also remains applicable under its own scope.

NYDOH-APP5E 5-E.1(a), 5-E.2(a), 5-E.8, 5-E.9

Certified drinking water operators

All drinking water operators certified under Subpart 5-4. Population and Appendix 5-E.2 exclusions do not remove this training duty.

NYDOH-APP5E 5-E.1(a), 5-E.7

All SPDES permittees

Cyber incident reporting applies to all SPDES permittees, including private facilities. Apply the defined incident criteria rather than assuming every security alert is a reportable incident.

NYDEC-750-2026 750-1.2(a)(27), 750-2.7(h)

Publicly owned treatment works

ERP and cybersecurity controls apply to POTWs of all sizes. Contracting operations does not transfer the municipality's responsibility for compliance.

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

NYDEC-750-2026 750-1.2(a)(78), 750-2.9(d) through (f)

Network monitoring at larger POTWs

Design flow at least 10 million gallons per day. The specific no connection and outward only device exceptions concern monitoring and logging, not the other POTW controls.

NYDEC-750-2026 750-2.9(e)(2)

Certified wastewater operators

Part 650 training requirements apply by operator grade and certification renewal period. January 1, 2027 is the expiration date threshold, not a universal course completion date for every operator.

NYDEC-650-2026 650.8, 650.12

Federal community water assessment and planning

Community drinking water systems serving more than 3,300 people, separately identified by PWSID. Wastewater systems do not become subject to these federal certification duties merely by using the toolkit.

USEPA-AWIA SDWA 1433

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

New York Drinking Water

Record the water system scope

NY-DW-SCOPE · Requirement · NYDOH-APP5E 5-E.1(a); 5-E.2

Applies when: Community water systems serving more than 3,300 people; separate operator training scope.

What to do: Determine coverage and any supported exclusion. The no connection exclusion retains incident response planning and incident reporting. Excluded municipal billing or other IT must not affect Subpart compliance.

When: Before selecting duties; reassess when population, system boundaries or connectivity changes.

Responsible role: System owner with the responsible technical reviewer

Evidence to retain: PWSID, population basis, network diagram, connection inventory and signed scope decision.

Safe examination: Compare drawings with approved configuration records and interview the operator about vendor and remote paths.

Result criterion: Each selected or excluded duty has a supported scope decision; unknown connections remain unresolved.

Next review: On material scope or connection changes; review with the CVA.

Designate a qualified cybersecurity lead

NY-DW-PERSONNEL · Requirement · NYDOH-APP5E 5-E.4(a)

Applies when: Covered systems serving a combined wholesale and retail population greater than 50,000, subject to applicable exclusions.

What to do: The owner designates the responsible individual based on demonstrable cybersecurity knowledge and practical system protection or risk management experience. The rule does not require a named professional certification.

When: By January 1, 2027 and while this scope applies.

Responsible role: System owner

Evidence to retain: Designation, qualification basis, duties and current contact details.

Safe examination: Read the designation and compare documented experience with responsibility for the system's program.

Result criterion: An owner designated, qualified individual is responsible for the program.

Next review: On role or personnel changes.

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

Put the cybersecurity lead in the emergency plan

NY-DW-LEAD-CONTACT · Requirement · NYDOH-APP5E 5-E.4(a)(1)

Applies when: Covered systems with combined wholesale and retail population greater than 50,000, subject to applicable exclusions.

What to do: Include the designated individual's name and contact information in the water supply emergency plan.

When: By January 1, 2027; keep current.

Responsible role: Emergency plan owner

Evidence to retain: Current controlled emergency plan and contact verification record.

Safe examination: Compare the designation with the plan and verify contact details without making an emergency report.

Result criterion: The current designated individual can be identified and reached from the plan.

Next review: On personnel or contact changes.

Report program risks to the governing body

NY-DW-BOARD-REPORT · Requirement · NYDOH-APP5E 5-E.4(a)(2)

Applies when: Covered systems with combined wholesale and retail population greater than 50,000, subject to applicable exclusions.

What to do: The designated individual provides a confidential written report on the cybersecurity program and material risks to the governing body at least annually.

When: At least annually after the January 1, 2027 compliance date.

Responsible role: Designated cybersecurity lead

Evidence to retain: Dated report, controlled distribution record and governing body receipt.

Safe examination: Confirm the report covers the program and material risks and was delivered to the correct governing body.

Result criterion: A timely confidential report has a documented recipient and evidence supported conclusions.

Next review: At least annually.

Complete the CVA and carry findings into the plan

NY-DW-CVA-PLAN · Requirement · NYDOH-APP5E 5-E.1(c)(1); 5-E.5(a)

Applies when: Covered water systems subject to the CVA provisions.

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

What to do: Prepare and submit a cybersecurity vulnerability analysis and incorporate its findings into the water system emergency plan submitted to the State.

When: By January 1, 2027; then follow review and submission triggers.

Responsible role: Authorized system representative and assessment lead

Evidence to retain: CVA edition, emergency plan cross references and State submission receipt.

Safe examination: Trace selected material findings from the CVA into the submitted emergency plan.

Result criterion: The CVA exists, was submitted, and its findings inform the emergency plan.

Next review: With updated CVA findings and plan submissions.

Obtain the correct CVA approval

NY-DW-CVA-APPROVAL · Requirement · NYDOH-APP5E 5-E.5(b)

Applies when: Covered water systems subject to CVA provisions.

What to do: An authorized representative approves the CVA. Above 50,000 combined wholesale and retail population, the designated cybersecurity lead approves it.

When: When the CVA is completed or revised for approval.

Responsible role: Authorized representative or designated cybersecurity lead

Evidence to retain: Approval date, approver identity, authority and CVA version.

Safe examination: Compare the recorded population and designation with the CVA approval record.

Result criterion: The correct authorized person approved the identifiable CVA edition.

Next review: Each CVA approval.

Assess risk to operations and protected information

NY-DW-CVA-RISK · Requirement · NYDOH-APP5E 5-E.5(c)

Applies when: Relevant IT, OT and nonpublic information that may affect Subpart compliance.

What to do: Assess known vulnerabilities using likelihood of exploitation and consequences for normal operations.

When: By January 1, 2027 and during CVA review.

Responsible role: Assessment lead with plant operations

Evidence to retain: Asset and information scope, vulnerability register, likelihood and operational consequence rationale.

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

Safe examination: Trace representative treatment and support dependencies into the risk analysis using records and interviews.

Result criterion: Relevant vulnerabilities have supported likelihood and consequence assessments; missing evidence is visible.

Next review: During CVA review and material changes.

Evaluate controls across the water system

NY-DW-CVA-CONTROLS · Requirement · NYDOH-APP5E 5-E.5(d)

Applies when: Controls associated with supply, treatment, disinfection, pipes and valves, storage and operations management.

What to do: Evaluate control effectiveness for maintaining Subpart compliance during a water supply emergency caused by a cyber incident.

When: By January 1, 2027 and during CVA review.

Responsible role: Assessment lead and operations owner

Evidence to retain: Control tests, sample basis, observed results and unexamined dependencies.

Safe examination: Review approved records and safe demonstrations; agree operational limits before any live test.

Result criterion: The analysis evaluates effectiveness across relevant functions rather than only listing policies.

Next review: During CVA review.

Report qualifying CVA vulnerabilities

NY-DW-VULN-NOTICE · Requirement · NYDOH-APP5E 5-E.1(c)(2); 5-E.5(e)

Applies when: CVA vulnerabilities that may affect Subpart compliance, or a situation that may pose a public health risk.

What to do: Report qualifying vulnerabilities or situations to NYSDOH in accordance with section 5-1.77.

When: Within 48 hours of identification of the qualifying vulnerability or situation.

Responsible role: Authorized reporting lead with the operator

Evidence to retain: Identification time and timezone, criteria decision, submitted report and receipt.

Safe examination: Trace the recorded trigger to the reporting deadline and evidence of delivery.

Result criterion: The qualifying trigger is preserved and the required report is timely; an ordinary security finding is not automatically assigned this clock.

Next review: Each qualifying identification.

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

Keep the CVA current

NY-DW-CVA-REVIEW · Requirement · NYDOH-APP5E 5-E.1(c)(1); 5-E.5(f)

Applies when: Covered systems subject to CVA provisions.

What to do: Review and update the CVA for technology developments and evolving threats, including after major water facility infrastructure becomes operational.

When: At least annually and within 30 days after major infrastructure changes become operational.

Responsible role: CVA owner and change manager

Evidence to retain: Review history, change commissioning dates, updated CVA and approval.

Safe examination: Compare the last review and major operational changes with recorded CVA updates.

Result criterion: Both the annual and change driven deadlines are met and their results are documented.

Next review: Annual and each qualifying infrastructure change.

Identify action for each vulnerability

NY-DW-CVA-ACTIONS · Requirement · NYDOH-APP5E 5-E.5(g)

Applies when: Vulnerabilities identified by the CVA.

What to do: Identify the actions needed to mitigate or remediate the vulnerabilities.

When: During completion and review of the CVA.

Responsible role: CVA owner and assigned action owners

Evidence to retain: Finding IDs, proposed actions, operational dependencies and assigned responsibility.

Safe examination: Follow each identified vulnerability to a specified action or documented unresolved decision.

Result criterion: The CVA states what action is needed for the identified vulnerabilities.

Next review: When a vulnerability or its treatment changes.

Use the department approved CVA form

NY-DW-CVA-FORM · Requirement · NYDOH-APP5E 5-E.5(h)

Applies when: Covered systems subject to CVA provisions.

What to do: Prepare the CVA in a form approved by NYSDOH. The GDF worksheets organize supporting work and do not replace that approved form.

When: Before submission.

Responsible role: CVA owner

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

Evidence to retain: Approved form version or written department approval and submitted CVA.

Safe examination: Compare the form used with the department's current approved submission instructions.

Result criterion: The submission format has department approval.

Next review: Each submission and form change.

Build the program from the CVA findings

NY-DW-PROGRAM · Requirement · NYDOH-APP5E 5-E.6(a)

Applies when: Covered systems subject to cybersecurity program provisions.

What to do: Establish a cybersecurity program based on the findings of the system's CVA.

When: By January 1, 2027 and maintained as risks change.

Responsible role: System owner and program lead

Evidence to retain: Program edition, CVA mapping, procedures and allocated responsibilities.

Safe examination: Trace material CVA findings into program decisions and work assignments.

Result criterion: The program addresses the system's actual CVA findings.

Next review: When CVA findings or program design changes.

Certify the program through the required submission

NY-DW-PROGRAM-CERT · Requirement · NYDOH-APP5E 5-E.6(b)

Applies when: Covered systems serving more than 50,000 combined wholesale and retail population, subject to applicable exclusions.

What to do: The designated lead certifies compliance with 5-E.6(c) on a department approved form as part of the water system emergency plan submission. This is a program certification, not a professional credential.

When: As part of the plan submission required by 5-1.33(e).

Responsible role: Designated cybersecurity lead

Evidence to retain: Approved form, supported certification, signatory and submission receipt.

Safe examination: Trace certification statements to the program's supporting evidence and the correct signer.

Result criterion: The required signed form accompanies the submission and does not claim unsupported compliance.

Next review: With required emergency plan submissions.

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

Maintain separate reporting duties

NY-DW-REPORTING-PROGRAM · Requirement · NYDOH-APP5E 5-E.6(c)(1); 5-E.9

Applies when: Applicable statutory and regulatory reporting obligations.

What to do: Make reporting part of the cybersecurity program and preserve other required notices alongside the DOH cyber incident notice.

When: By January 1, 2027; incident reporting is already effective.

Responsible role: Reporting lead and legal or compliance owner

Evidence to retain: Notification register with separate authority, trigger, recipient and receipt fields.

Safe examination: Walk through an exercise without transmitting and confirm that one notice does not close another authority's task.

Result criterion: The program can identify and execute each applicable notice separately.

Next review: On rule, contact or incident changes.

Protect external access to operational technology

NY-DW-MFA · Requirement · NYDOH-APP5E 5-E.6(c)(2)(i)

Applies when: Individuals accessing covered OT from an external network.

What to do: Require multifactor authentication unless the authorized representative or designated cybersecurity lead approves compensating controls in writing.

When: By January 1, 2027 and for each access route.

Responsible role: Technical access owner and authorized approver

Evidence to retain: Remote route inventory, authentication configuration and written compensating control approvals.

Safe examination: Inspect configuration and an authorized demonstration; do not attempt unauthorized access or change plant operation.

Result criterion: Every reviewed external route enforces MFA or has the specified written approval and implemented compensating controls.

Next review: On access or control changes; include in CVA review.

Limit access to assigned work

NY-DW-LEAST-PRIVILEGE · Requirement · NYDOH-APP5E 5-E.6(c)(2)(ii)

Applies when: User access to OT and nonpublic information.

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

What to do: Restrict privileges to those needed for the user's assigned tasks.

When: By January 1, 2027 and when access is granted or changed.

Responsible role: Access owner and user's manager

Evidence to retain: Role definitions, access approvals and effective permission records.

Safe examination: Compare sampled user permissions with documented duties and approvals.

Result criterion: Sampled privileges match assigned work; unexplained access becomes a finding.

Next review: On role changes and access reviews.

Separate OT and IT user accounts

NY-DW-ACCOUNT-SEPARATION · Requirement · NYDOH-APP5E 5-E.6(c)(2)(iii)

Applies when: User accounts authorized for OT and IT.

What to do: Separate accounts authorized to access OT from accounts authorized to access IT.

When: By January 1, 2027 and during account administration.

Responsible role: Identity and access administrator

Evidence to retain: Account directories, role mappings and access architecture.

Safe examination: Compare approved account identities and authorizations across the OT and IT boundary.

Result criterion: Separate accounts are used for the respective environments.

Next review: On identity design and account changes.

Give OT users unique credentials

NY-DW-UNIQUE-CREDENTIALS · Requirement · NYDOH-APP5E 5-E.6(c)(2)(iv)

Applies when: OT capable of supporting unique user credentials; compensating controls for incapable OT.

What to do: Use unique credentials where supported. Implement compensating controls where not supported; above 50,000 combined population, the designated lead documents those controls in writing.

When: By January 1, 2027 and when equipment or access changes.

Responsible role: OT access owner and designated lead where applicable

Evidence to retain: Capability evidence, account inventory, compensating control records and required written documentation.

Safe examination: Inspect account settings and vendor capability documentation without exposing passwords.

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

Result criterion: Unique accounts exist where supported and required compensating controls are implemented and documented.

Next review: On equipment and user changes.

Review access at least annually

NY-DW-ACCESS-REVIEW · Requirement · NYDOH-APP5E 5-E.6(c)(2)(v)

Applies when: All user access privileges within the covered program.

What to do: Review privileges and remove or disable accounts and access no longer needed for the user's job.

When: At least annually.

Responsible role: Access owner and managers

Evidence to retain: Complete account population, dated review, decisions and completed removals.

Safe examination: Compare the review population with active accounts and trace removal decisions to completion.

Result criterion: The annual review covers the relevant population and unnecessary access is removed or disabled.

Next review: At least annually.

Remove access immediately when it is no longer needed

NY-DW-LEAVER-ACCESS · Requirement · NYDOH-APP5E 5-E.6(c)(2)(v)

Applies when: Departing users and users whose changed role no longer requires access.

What to do: Immediately terminate unnecessary account access. Change shared credentials immediately or implement compensating controls that prevent the former user's unauthorized OT access.

When: Immediately following the departure or relevant role change.

Responsible role: Personnel notifier and access administrator

Evidence to retain: Event time, access removal records and shared credential control record.

Safe examination: Trace sampled departure and role changes to the effective removal of each access path.

Result criterion: No unaddressed route remains solely because it uses shared credentials.

Next review: Each departure or qualifying role change.

Disable unnecessary remote access

NY-DW-REMOTE-NEED · Requirement · NYDOH-APP5E 5-E.6(c)(2)(vi)

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

Applies when: Remote access to covered OT.

What to do: Disable remote access that is unnecessary for monitoring or operating the system.

When: By January 1, 2027 and when need ends.

Responsible role: OT owner

Evidence to retain: Remote path inventory, operational justification and disabled access records.

Safe examination: Compare enabled paths with approved operational needs using configuration review.

Result criterion: Each enabled path has a monitoring or operating need.

Next review: On vendor, network and operational changes.

Limit remote functions

NY-DW-REMOTE-FUNCTION · Requirement · NYDOH-APP5E 5-E.6(c)(2)(vii)

Applies when: Allowed remote access to covered OT.

What to do: Limit remote functionality to what is necessary to monitor or operate the system.

When: By January 1, 2027 and on configuration changes.

Responsible role: OT access owner

Evidence to retain: Remote role settings, approved functions and restrictions.

Safe examination: Inspect whether sampled remote accounts can perform functions beyond their documented need.

Result criterion: Enabled remote functions match the necessary monitoring or operating work.

Next review: On remote role and configuration changes.

Secure remote access protocols

NY-DW-REMOTE-CONFIG · Requirement · NYDOH-APP5E 5-E.6(c)(2)(viii)

Applies when: Protocols permitting remote access to OT or nonpublic information.

What to do: Securely configure the protocols that permit remote access.

When: By January 1, 2027 and throughout operation.

Responsible role: Technical access owner

Evidence to retain: Protocol inventory, approved configuration basis and configuration records.

Safe examination: Compare approved settings with read only configuration evidence and record unexplained deviations.

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

Result criterion: A supported security configuration is implemented for each reviewed protocol.

Next review: On protocol, vendor or configuration changes.

Remove default OT passwords

NY-DW-DEFAULT-PASSWORDS · Requirement · NYDOH-APP5E 5-E.6(c)(2)(ix)

Applies when: All covered OT, including equipment with technically unchangeable passwords.

What to do: Disallow default passwords. Where technology cannot change them, implement compensating controls.

When: By January 1, 2027 and when equipment enters service.

Responsible role: OT equipment owner

Evidence to retain: Configuration attestation, vendor capability record and compensating control evidence.

Safe examination: Review records and authorized demonstrations without recording actual passwords.

Result criterion: Defaults are removed or technically unavoidable defaults have implemented compensating controls.

Next review: On installation, reset and equipment changes.

Maintain the cyber asset inventory

NY-DW-INVENTORY · Requirement · NYDOH-APP5E 5-E.3(c); 5-E.6(c)(3)

Applies when: OT reachable by management, control or communications protocols and IT physically or logically connected to OT.

What to do: Maintain an inventory covering the defined cyber assets.

When: By January 1, 2027 and maintained thereafter.

Responsible role: OT asset owner with IT support

Evidence to retain: Asset inventory, system boundaries, owners and connection records.

Safe examination: Reconcile approved drawings, procurement and maintenance records with representative assets; no unsolicited scanning.

Result criterion: The inventory covers the defined asset population, including relevant legacy and third party equipment.

Next review: When assets or connections change.

Protect OT and nonpublic information

NY-DW-DEFENSIVE-ARCHITECTURE · Requirement · NYDOH-APP5E 5-E.6(c)(4)

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

Applies when: Covered OT and nonpublic information.

What to do: Use defensive architecture, controls, compensating controls, policies and procedures against unauthorized disclosure, alteration or destruction.

When: By January 1, 2027 and maintained thereafter.

Responsible role: Technical security owner and operations owner

Evidence to retain: Architecture, control design, approved rules and supporting effectiveness records.

Safe examination: Trace selected critical dependencies through documented boundaries and authorized control evidence.

Result criterion: Protection measures address confidentiality, integrity and availability for the relevant assets and information.

Next review: With architecture changes and CVA reviews.

Assess internal and external threats

NY-DW-ONGOING-RISK · Requirement · NYDOH-APP5E 5-E.6(c)(5)

Applies when: OT and nonpublic information relevant to Subpart compliance.

What to do: Identify and assess internal and external cybersecurity risks that may threaten the system's ability to comply.

When: By January 1, 2027 and as risks change.

Responsible role: Program lead and operations owner

Evidence to retain: Risk register, threat inputs, dependencies and decisions.

Safe examination: Check whether vendor, insider, remote access and external exposure are considered where relevant.

Result criterion: The program considers relevant internal and external risks, with unsupported areas left open.

Next review: With new risks and CVA reviews.

Monitor and retain useful network logs

NY-DW-LOGGING · Requirement · NYDOH-APP5E 5-E.6(c)(6)

Applies when: Covered systems above 50,000 combined wholesale and retail population. Apply the specific outward only device exception and relevant 5-E.2 exclusion using evidence.

What to do: Monitor and log network activity and be prepared to produce the logs for examination after a cyber incident.

When: By January 1, 2027 and maintained thereafter.

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

Responsible role: Network monitoring owner

Evidence to retain: Logging scope, retained sample, access controls and any supported exception decision.

Safe examination: Inspect logs and retrieval capability through a safe demonstration; verify device capability before relying on an outward only exception.

Result criterion: Required activity is monitored and logs are retrievable, or a supported specific exception is recorded.

Next review: On network changes and program review.

Respond with operations and safety in view

NY-DW-RESPONSE · Requirement · NYDOH-APP5E 5-E.6(c)(7)

Applies when: Cybersecurity incidents affecting the covered system.

What to do: Respond to reduce disruption, address compliance impacts and limit physical or structural damage.

When: When responding to a cyber incident; prepare capability by January 1, 2027.

Responsible role: Incident lead and operating authority

Evidence to retain: Response procedures, operating decisions and incident or exercise records.

Safe examination: Use a discussion exercise to trace response authority and operational dependencies without changing live controls.

Result criterion: Response decisions account for service, regulatory and physical consequences.

Next review: After incidents and material plan changes.

Restore safe operations and services

NY-DW-RECOVERY · Requirement · NYDOH-APP5E 5-E.6(c)(8)

Applies when: Covered system recovery following cyber incidents.

What to do: Recover from cybersecurity incidents and restore normal operations and services.

When: Prepare capability by January 1, 2027 and use it when needed.

Responsible role: Recovery lead and operating authority

Evidence to retain: Recovery dependencies, approved restoration steps and verification records.

Safe examination: Review an isolated restore demonstration or existing approved evidence; confirm the operator authorizes return to service.

Result criterion: The recovery approach can restore needed services with verification of the operating state.

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

Next review: With recovery changes and after incidents.

Complete approved operator cyber training

NY-DW-TRAINING · Requirement · NYDOH-APP5E 5-E.1(a) and (b); 5-E.7

Applies when: All drinking water operators certified under Subpart 5-4, independent of system population or isolation.

What to do: Complete at least one hour of cybersecurity training using a curriculum approved by NYSDOH every three years.

When: Already effective upon adoption; confirm each operator's applicable training period.

Responsible role: Certified operator and training coordinator

Evidence to retain: Operator certification, approved course record, attendance and next training date.

Safe examination: Compare the course approval and completed hours with the operator's training period.

Result criterion: The operator has the required approved cybersecurity training within the applicable three year period.

Next review: Every three years.

Write the cyber incident response plan

NY-DW-IRP · Requirement · NYDOH-APP5E 5-E.8; 5-E.2(a)

Applies when: All covered water systems, including systems using the no connection exclusion.

What to do: Establish a written plan describing tasks during and after a cyber incident to maintain or restore Subpart compliance, consistent with 5-1.33(b)(6).

When: By January 1, 2027 and kept current.

Responsible role: Emergency plan owner and operating authority

Evidence to retain: Controlled plan, notification roster, operating tasks and corrective follow up.

Safe examination: Walk a fictional incident through roles, communications and restoration tasks without sending messages.

Result criterion: The written plan gives responsible personnel an executable sequence for maintaining or restoring compliance.

Next review: With plan and operational changes.

Notify DOH of a qualifying cyber incident

NY-DW-INCIDENT-NOTICE · Requirement · NYDOH-APP5E 5-E.3(e); 5-E.9

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

Applies when: A defined cybersecurity incident that has created or may create a public health hazard, including at otherwise excluded covered systems.

What to do: Notify NYSDOH using the prescribed 5-1.77(a) process. Preserve separate State and federal notification obligations.

When: As soon as possible, no later than 24 hours after determining that the qualifying incident occurred. Already effective upon adoption.

Responsible role: Authorized reporting lead with operating authority

Evidence to retain: Event chronology, determination basis and time, report and delivery receipt.

Safe examination: Compare the recorded determination with the reporting time; do not substitute detection alone for the defined trigger.

Result criterion: The qualifying incident is reported on time through the prescribed process and parallel duties remain tracked.

Next review: Each qualifying incident.

Consult after a State deficiency notice

NY-DW-DEFICIENCY-CONSULT · Requirement · NYDOH-SUBPART51 5-1.71(c); Appendix 5-E.1(d)

Applies when: State notification that a significant deficiency exists; section 5-1.71 also has broader public water system application.

What to do: Consult with the State regarding corrective action after receiving its significant deficiency notice.

When: Within 30 days of the State notification.

Responsible role: Supplier of water and authorized compliance representative

Evidence to retain: State notice, receipt date, consultation record and agreed actions.

Safe examination: Trace the dated State notice to documented consultation.

Result criterion: Consultation occurred within the required period and any earlier State direction is recorded.

Next review: Each State significant deficiency notification.

Correct the deficiency or comply with its action plan

NY-DW-DEFICIENCY-CORRECT · Requirement · NYDOH-SUBPART51 5-1.71(c) and (d); Appendix 5-E.1(d)

Applies when: State notified significant deficiency and any applicable public health hazard.

What to do: Correct the deficiency or comply with a corrective action plan specifying needed changes. Public health hazards require State directed or approved action and Tier 1 notification; failure to correct or begin correction as required can be a treatment technique violation.

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

When: Within 120 days of the State notice, or earlier when the State requires action to protect public health. Follow the actual State direction and plan.

Responsible role: Supplier of water and corrective action owner

Evidence to retain: State notice, action plan, milestones, completion evidence and State correspondence.

Safe examination: Compare the notice and required schedule with demonstrated progress and completed corrections.

Result criterion: The deficiency is corrected or the system is in compliance with the applicable action plan; opening a work ticket alone is insufficient.

Next review: Through required correction and verification.

Keep State emergency plan submissions current

NY-DW-ERP-RECURRENCE · Requirement · NYDOH-SUBPART51 5-1.33(e)

Applies when: Community water systems supplying more than 3,300 people; other systems may be directed to prepare a plan under 5-1.33(f).

What to do: Keep the emergency plan current, submit it for State review and supply updated communication and notification information.

When: Plan review submission at least every five years and within 30 days after major infrastructure changes have been made; contact information to the State by December 31 each year.

Responsible role: Emergency plan owner

Evidence to retain: Plan versions, State receipts, major change dates and annual contact submission.

Safe examination: Reconcile plan submissions with the five year cycle, changes and annual contact update.

Result criterion: Each separate submission and update trigger is tracked and met.

Next review: Five year, change driven and annual duties remain separate.

Handle plan comment and protected information correctly

NY-DW-ERP-PUBLIC-REVIEW · Requirement · NYDOH-SUBPART51 5-1.33(d) and (h); Appendix 5-E.10

Applies when: Required emergency plan public review and submitted information.

What to do: Before final plan submission, publish the required local notice in two successive weeks and accept comments for at least 14 days after first publication. Submit comments with the plan. Determine and handle security risk information under the applicable disclosure provisions.

When: Before final emergency plan submission.

Responsible role: System owner with counsel or records officer

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

Evidence to retain: Publication record, comment period, comments and protected information determination.

Safe examination: Check the publication dates and comment record; verify sensitive technical details were handled under the correct authority.

Result criterion: Public review requirements and documented security protections are both addressed; confidentiality is not assumed for every record.

Next review: Before relevant final submissions.

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

New York Wastewater

Separate permit reporting from POTW controls

NY-WW-SCOPE · Requirement · NYDEC-750-2026 750-1.2(a)(27), (78), (94); 750-2.7(h); 750-2.9(d) through (f)

Applies when: All SPDES permittees for reporting; POTWs for the additional plans and controls.

What to do: Identify the permittee, permit, POTW status, design flow and systems holding SPDES program data before selecting obligations.

When: Before planning and when permit or ownership facts change.

Responsible role: Legally responsible party and permit coordinator

Evidence to retain: SPDES permit, ownership record, design flow basis and data system inventory.

Safe examination: Compare the facility profile with the permit and adopted definitions.

Result criterion: Private permittees retain reporting duties and small POTWs retain plans and controls; no drinking water threshold is substituted.

Next review: On permit, ownership or design changes.

Report a wastewater cyber incident promptly

NY-WW-NOTIFY-ORAL · Requirement · NYDEC-750-2026 750-1.2(a)(27); 750-2.7(h)(1)

Implementation guidance: NYDEC-IMPLEMENTATION

Applies when: All SPDES permittees when a defined cybersecurity incident occurs.

What to do: Report orally to the regional water engineer. Current DEC instructions also require the initial online incident form followed immediately by oral notification; use the regional contact or DEC Dispatch if the regional contact cannot be reached.

When: As soon as possible, no later than 24 hours from permittee awareness. Effective March 26, 2026.

Responsible role: Permittee's reporting lead

Evidence to retain: Awareness time and timezone, initial facts, online receipt, call record and recipient.

Safe examination: Trace the defined incident and awareness time to both the initial filing and oral notification record.

Result criterion: The notice uses known facts without waiting for a complete examination and meets the oral reporting deadline.

Next review: Each qualifying incident.

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

Complete the written wastewater incident report

NY-WW-NOTIFY-WRITTEN · Requirement · NYDEC-750-2026 750-2.7(h)(2)

Implementation guidance: NYDEC-IMPLEMENTATION

Applies when: All SPDES permittees after a defined cybersecurity incident.

What to do: Provide the written report with discovery time and person, incident description, affected IT or OT, actual or expected disruption and duration, data or physical loss and remediation or mitigation measures. Use DEC's current online process.

When: Within 30 days from permittee awareness of the incident.

Responsible role: Permittee's reporting lead

Evidence to retain: Eight required subject areas, supporting facts, approved report version and submission receipt.

Safe examination: Check the report against each statutory information category and the awareness based deadline.

Result criterion: The written report covers every required category and is submitted on time.

Next review: Each qualifying incident.

Keep other incident notices open

NY-WW-PARALLEL-NOTICES · Requirement · NYDEC-750-2026 750-2.7(h)(3)

Applies when: Other reporting and notification duties applicable under 750-2.7 and the permit.

What to do: Complete other applicable reporting duties alongside the cyber incident reports. Review permit conditions and separate sewage, spill and municipal cyber reporting duties with the responsible specialist.

When: Each applicable authority's own trigger and deadline.

Responsible role: Permit coordinator and reporting lead

Evidence to retain: Parallel notice register, scope decisions and receipts.

Safe examination: Check whether a cyber incident with operational or discharge effects has been screened for other notices.

Result criterion: The cyber report is not treated as satisfying every other reporting duty.

Next review: Each incident and permit or rule change.

Establish the wastewater emergency plan

NY-WW-ERP · Requirement · NYDEC-750-2026 750-2.9(d)(1)

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

Applies when: All POTWs.

What to do: Establish, maintain and implement a written ERP. A plan existing before March 11, 2027 may qualify if it covers preparation and response strategies, resources and procedures plus responsible titles and contacts. Otherwise use the incorporated EPA template.

When: By March 11, 2027 and maintained thereafter.

Responsible role: POTW operating authority and emergency plan owner

Evidence to retain: Dated plan, eligibility decision for existing plan or template basis, roles and resources.

Safe examination: Trace the required plan elements to actual site procedures, contacts and resource availability.

Result criterion: A qualifying written plan is established, maintained and implemented.

Next review: Maintain continuously and update when required.

Incorporated documents and sections: sourceId: IBR-EPA-WWERP-2021
locator: Introduction and facility planning sections

Update changed emergency contacts

NY-WW-ERP-CONTACT · Requirement · NYDEC-750-2026 750-2.9(d)(2)

Applies when: Titles and contact information in the POTW emergency plan.

What to do: Update the emergency plan after its responsible titles or contact details change.

When: Within 30 days of the change.

Responsible role: Emergency plan owner

Evidence to retain: Change date, revised plan, distribution record and current roster.

Safe examination: Compare recent personnel and contact changes with the controlled plan and its distributed copies.

Result criterion: Changed titles and contacts are corrected within 30 days.

Next review: Each title or contact change.

Keep secure printed plans on and off site

NY-WW-ERP-COPIES · Requirement · NYDEC-750-2026 750-2.9(d)(3)

Applies when: POTW emergency plan including its incorporated cyber plan.

What to do: Keep printed ERP copies in secure locations on and off the premises, accessible only to appropriate people under the access rules.

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

When: By March 11, 2027 and maintained thereafter.

Responsible role: Emergency plan custodian

Evidence to retain: Copy register, version dates, location and authorized access record.

Safe examination: Have the custodian demonstrate retrieval of current copies without publishing their sensitive contents.

Result criterion: Current printed copies exist in both required locations with controlled access.

Next review: On plan revision or custody changes.

Incorporated documents and sections: sourceId: IBR-NIST-80082R3
locator: Page 114; response plan availability
sourceId: IBR-EPA-WWERP-2021
locator: Introduction; plan copies

Certify the ERP requirements annually

NY-WW-ERP-CERT · Requirement · NYDEC-750-2026 750-2.9(d)(4); 750-2.9(f)

Applies when: All POTWs.

What to do: Certify compliance with ERP establishment, contact updating and printed copy requirements using the required authorized signer and filing process.

When: By March 28 each year; first certification March 28, 2027.

Responsible role: Principal executive officer, ranking elected official or qualifying authorized municipal representative

Evidence to retain: Supporting work, signed certification, signer authority and DEC receipt.

Safe examination: Trace the certification to evidence for 750-2.9(d)(1) through (3) and verify the signer.

Result criterion: A supported ERP certification reaches DEC by the deadline.

Next review: Annually by March 28.

Write and apply least privilege access rules

NY-WW-ACCESS · Requirement · NYDEC-750-2026 750-2.9(e)(1)(i)(a)

Applies when: OT, SPDES program data, IT permitting direct or indirect access to either, and the ERP.

What to do: Establish, maintain and implement written access rules or procedures consistent with least privilege.

When: By March 11, 2027 and maintained thereafter.

Responsible role: Access owner with operations and data owners

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

Evidence to retain: Written rules, role approvals, account population and actual permissions.

Safe examination: Compare sampled users with assigned duties across all four required asset and information categories.

Result criterion: Written rules govern actual access and reviewed permissions are limited to assigned work.

Next review: Annual policy review and event updates are separate duties.

Incorporated documents and sections: sourceId: IBR-NIST-80053R5
locator: Page 36, AC-6
sourceId: IBR-NIST-80082R3
locator: Pages 98 and 99

Set and implement password rules

NY-WW-PASSWORDS · Requirement · NYDEC-750-2026 750-2.9(e)(1)(i)(b)

Applies when: Authentication within the required access rules.

What to do: Address password security, complexity and management using the incorporated documents. Record the selected method and any technical constraints rather than inventing one universal password rule.

When: By March 11, 2027 and maintained thereafter.

Responsible role: Identity and OT access owners

Evidence to retain: Password rules, supported configuration, feasibility decisions and exception handling.

Safe examination: Compare policy to configuration without collecting passwords; check the chosen method against the incorporated guidance.

Result criterion: The written approach addresses all three password subjects and is implemented for its scope.

Next review: With access policy review and changes.

Incorporated documents and sections: sourceId: IBR-EPA-CYBER-2024
locator: Question 2.B and related factsheet; minimum length as feasible
sourceId: IBR-NIST-80053R5
locator: Page 139; password based authentication

Require MFA for allowed remote OT access

NY-WW-MFA · Requirement · NYDEC-750-2026 750-2.9(e)(1)(i)(c)

Applies when: Remote access to OT allowed under the POTW's access rules.

What to do: Require multifactor authentication for permitted remote OT access. Do not import the drinking water rule's written compensating control exception into this wastewater criterion.

When: By March 11, 2027 and for every allowed remote route.

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

Responsible role: Remote access owner

Evidence to retain: Route inventory, authentication configuration and authorized demonstration record.

Safe examination: Inspect each selected permitted route's authentication controls without conducting an unauthorized connection.

Result criterion: Allowed remote OT access requires MFA; unsupported routes remain unresolved.

Next review: On remote route or authentication changes.

Incorporated documents and sections: sourceId: IBR-EPA-CYBER-2024
locator: Question 2.H
sourceId: IBR-NIST-80082R3
locator: Page 106
sourceId: IBR-NIST-80053R5
locator: Pages 132 and 133

Disallow preset and default credentials

NY-WW-DEFAULTS · Requirement · NYDEC-750-2026 750-2.9(e)(1)(i)(d)

Applies when: Assets covered by the POTW's access and authentication rules.

What to do: Disallow preset or default credentials. Resolve incapable legacy equipment with the responsible authority rather than assuming a drinking water exception applies.

When: By March 11, 2027 and on commissioning or reset.

Responsible role: Asset and access owners

Evidence to retain: Credential configuration attestations, vendor capabilities and remediation decisions.

Safe examination: Review records or an authorized demonstration without disclosing the credentials.

Result criterion: Default or preset credentials are not allowed by the implemented rules.

Next review: On equipment installation, reset and review.

Incorporated documents and sections: sourceId: IBR-EPA-CYBER-2024
locator: Question 2.A
sourceId: IBR-NIST-80082R3
locator: Page 123
sourceId: IBR-NIST-80053R5
locator: Page 140

Review access rules annually

NY-WW-ACCESS-REVIEW · Requirement · NYDEC-750-2026 750-2.9(e)(1)(i)(e)

Applies when: Written access control and authentication rules or procedures.

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

What to do: Review the access rules and procedures at least annually.

When: At least annually by March 28, beginning in 2027.

Responsible role: Access policy owner

Evidence to retain: Dated review, participants, conclusions and resulting changes.

Safe examination: Compare the last review with the current policy edition and open changes.

Result criterion: A documented review occurs by the annual deadline.

Next review: At least annually by March 28.

Update access rules after an incident or assessment

NY-WW-ACCESS-UPDATE · Requirement · NYDEC-750-2026 750-2.9(e)(1)(i)(f)

Applies when: Written access control and authentication rules or procedures.

What to do: Update the rules after a cyber incident or a cybersecurity assessment or audit.

When: Within 90 days after the triggering incident, assessment or audit.

Responsible role: Access policy owner

Evidence to retain: Trigger date, findings, revised procedures and implementation record.

Safe examination: Trace recent incidents and assessments to the dated policy updates.

Result criterion: Required updates occur within 90 days of each relevant trigger.

Next review: Each incident, assessment or audit.

Include the full cyber asset inventory

NY-WW-INVENTORY · Requirement · NYDEC-750-2026 750-1.2(a)(25); 750-2.9(e)(1)(ii)(a)

Applies when: Reachable OT and IT connected to OT or serving as the system of record for SPDES program data.

What to do: Include the defined cyber asset inventory in a written vulnerability management process. Relevant assets without IP addresses are not automatically excluded.

When: By March 11, 2027 and maintained thereafter.

Responsible role: Asset owner and vulnerability process owner

Evidence to retain: Inventory with asset identity, role, owner, connectivity and data function.

Safe examination: Reconcile drawings and maintenance or procurement records with representative OT and SPDES data assets; avoid unapproved scanning.

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

Result criterion: The inventory covers the regulatory definition and supported asset boundaries.

Next review: When assets are added or decommissioned.

Incorporated documents and sections: sourceId: IBR-EPA-CYBER-2024
locator: Question 1.A; apply DEC's broader asset definition
sourceId: IBR-NIST-80053R5
locator: Pages 107 through 110

Identify remotely accessible assets

NY-WW-REMOTE-INVENTORY · Requirement · NYDEC-750-2026 750-2.9(e)(1)(ii)(b)

Applies when: Assets in the cyber asset inventory.

What to do: Identify which inventoried assets can be accessed remotely.

When: By March 11, 2027 and as access changes.

Responsible role: Asset owner and remote access owner

Evidence to retain: Remote accessibility field, path references and vendor access records.

Safe examination: Compare network and vendor records with the inventory's remote access classification.

Result criterion: Remote capability is identified for the relevant population, with unknown paths marked unresolved.

Next review: On asset or connection changes.

Incorporated documents and sections: sourceId: IBR-EPA-CIRP-2025
locator: Page 4; remote OT systems and personnel

Identify known asset vulnerabilities

NY-WW-VULNERABILITIES · Requirement · NYDEC-750-2026 750-2.9(e)(1)(ii)(c)

Applies when: Assets within the cyber asset inventory.

What to do: Identify known cybersecurity vulnerabilities in inventoried assets.

When: By March 11, 2027 and as vulnerability information changes.

Responsible role: Vulnerability process owner with vendor support

Evidence to retain: Asset versions, dated advisories, applicability decisions and findings.

Safe examination: Match a sample of inventory entries to relevant vendor and authoritative advisories using read only research.

Result criterion: Known relevant vulnerabilities are identified and unsupported version information stays unresolved.

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

Next review: When new vulnerabilities are identified.

Incorporated documents and sections: sourceId: IBR-NIST-80082R3
locator: Page 94; vulnerability information
sourceId: IBR-EPA-CYBER-2024
locator: Questions 1.G/H

Assess likelihood and operating consequences

NY-WW-RISK · Requirement · NYDEC-750-2026 750-2.9(e)(1)(ii)(d)

Applies when: Known vulnerabilities identified for inventoried assets.

What to do: Assess the likelihood of exploitation and consequences for the POTW's normal operations.

When: During vulnerability assessment and review.

Responsible role: Vulnerability owner and operating authority

Evidence to retain: Risk rationale, affected process, data dependencies and supporting facts.

Safe examination: Trace selected findings through their likelihood and operational consequence rationale.

Result criterion: Both likelihood and consequence inform the assessment; a vendor severity score alone is not the entire analysis.

Next review: When exposure or consequences change.

Incorporated documents and sections: sourceId: IBR-NIST-80082R3
locator: Page 95; OT risk strategy

Prioritize vulnerabilities by assessed risk

NY-WW-PRIORITY · Requirement · NYDEC-750-2026 750-2.9(e)(1)(ii)(e)

Applies when: Known vulnerabilities with assessed risks.

What to do: Prioritize vulnerabilities using the assessed risks.

When: During vulnerability management.

Responsible role: Vulnerability process owner and operating authority

Evidence to retain: Prioritized register, rationale and dependency decisions.

Safe examination: Compare work priorities with assessed likelihood and operational consequences.

Result criterion: The sequence follows supported risk decisions and material exceptions have a recorded rationale.

Next review: When the risk picture changes.

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

Incorporated documents and sections: sourceId: IBR-NIST-80082R3
locator: Page 95

Mitigate or remediate in risk order

NY-WW-REMEDIATE · Requirement · NYDEC-750-2026 750-2.9(e)(1)(ii)(f)

Applies when: Prioritized vulnerabilities.

What to do: Mitigate or remediate vulnerabilities according to the established priority.

When: As part of the implemented vulnerability process; use actual risk and authorized operational schedules.

Responsible role: Corrective action owner and operating authority

Evidence to retain: Approved changes, mitigations, completion evidence and verification results.

Safe examination: Trace selected priorities into implemented action and safely obtained verification records.

Result criterion: Actions address the prioritized risks; planned work is not recorded as verified completion.

Next review: Until risk treatment and verification are complete.

Incorporated documents and sections: sourceId: IBR-EPA-CYBER-2024
locator: Question 1.E
sourceId: IBR-NIST-80082R3
locator: Page 52

Review the vulnerability process annually

NY-WW-VULN-REVIEW · Requirement · NYDEC-750-2026 750-2.9(e)(1)(ii)(g)

Applies when: Written cybersecurity vulnerability management process.

What to do: Review the written process at least annually.

When: At least annually by March 28, beginning in 2027.

Responsible role: Vulnerability process owner

Evidence to retain: Dated review, participating owners, conclusions and revisions.

Safe examination: Check review dates and whether actual asset and vulnerability changes informed the review.

Result criterion: The process has a documented review by the annual deadline.

Next review: At least annually by March 28.

Update the process when assets or vulnerabilities change

NY-WW-VULN-UPDATE · Requirement · NYDEC-750-2026 750-2.9(e)(1)(ii)(h)

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

Applies when: Written vulnerability management process and cyber asset inventory.

What to do: Update when inventoried assets are added or decommissioned, or a new vulnerability is identified for an inventoried asset.

When: When the specified change occurs; the clause does not give a universal 90 day allowance.

Responsible role: Asset and vulnerability process owners

Evidence to retain: Asset change events, advisory dates and process or register updates.

Safe examination: Trace recent additions, removals and vulnerability discoveries to the corresponding updates.

Result criterion: The process is updated for each applicable trigger rather than waiting for the annual review.

Next review: Each specified asset or vulnerability event.

Document and protect the network structure

NY-WW-NETWORK · Requirement · NYDEC-750-2026 750-2.9(e)(1)(iii)

Applies when: POTW operational technology and its IT or external connections.

What to do: Maintain and implement a written network description that protects OT through physical and logical separation or appropriate controls securing necessary connections.

When: By March 11, 2027 and maintained thereafter.

Responsible role: Network owner and operations owner

Evidence to retain: Current network description, permitted paths, boundary controls and supporting configuration records.

Safe examination: Compare drawings and approved rule sets with the described architecture through a safe review.

Result criterion: The documented protection method matches actual necessary connections and control evidence.

Next review: On network changes and relevant assessments.

Incorporated documents and sections: sourceId: IBR-EPA-CYBER-2024
locator: Questions 2.F, 2.W and 2.X
sourceId: IBR-NIST-80082R3
locator: Pages 67 through 89 and 105

Monitor and log the required network activity

NY-WW-LOGGING · Requirement · NYDEC-750-2026 750-2.9(e)(2)

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

Applies when: POTWs with design flow at least 10 MGD unless the specific no connection or outward only device exception is supported.

What to do: Implement, manage and maintain monitoring and logging. Verify any claimed exception using the actual connection design and device capability; the exception does not remove other POTW duties.

When: By March 11, 2027 and maintained thereafter.

Responsible role: Network monitoring owner

Evidence to retain: Design flow record, network diagram, logging sample, retrieval demonstration or documented exception basis.

Safe examination: Check actual connections, one way device capabilities where relevant, and safe retrieval of sample logs.

Result criterion: Required monitoring and logging are implemented, or the specific exception has adequate technical support.

Next review: On network, design flow or device changes.

Incorporated documents and sections: sourceId: IBR-NIST-80082R3
locator: Pages 73, 92 and 207
sourceId: IBR-NIST-80053R5
locator: Page 30; one way information flow

Incorporate the cyber response plan into the ERP

NY-WW-IRP · Requirement · NYDEC-750-2026 750-2.9(e)(3)

Applies when: All POTWs.

What to do: Establish, maintain and implement a cyber IRP and incorporate it into the ERP. A qualifying plan existing before March 11, 2027 may be used; otherwise use one of the two incorporated EPA cyber response templates.

When: By March 11, 2027 and maintained thereafter.

Responsible role: Incident response owner and emergency plan owner

Evidence to retain: Controlled ERP with incorporated IRP, plan basis, roles, resources and procedures.

Safe examination: Trace a fictional incident through the plan; verify the IRP is incorporated rather than only mentioned as an external document.

Result criterion: The incorporated IRP describes the POTW's preparation and response and satisfies the permitted plan basis.

Next review: On plan and operational changes.

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

Incorporated documents and sections: sourceId: IBR-EPA-INCIDENT-2021
locator: Preparation, response and recovery checklist
sourceId: IBR-EPA-CIRP-2025
locator: Introduction and template instructions
sourceId: IBR-NIST-80053R5
locator: Pages 158 and 159

Use the incorporated document editions

NY-WW-IBR · Requirement · NYDEC-750-2026 750-1.25(j) through (o); 750-2.9(e)(1) and (4)

Applies when: Establishing, maintaining and implementing the specified wastewater controls and plan options.

What to do: Use the six incorporated documents as directed by the adopted clauses. Record the specified edition and relevant method. Separate additional guidance from these required references; not every recommendation in a document becomes a standalone universal legal rule.

When: When developing and maintaining the required controls.

Responsible role: Compliance and technical document owners

Evidence to retain: Edition register, clause mapping, selected methods and supporting control records.

Safe examination: Compare each control's criterion with the adopted rule and the specified incorporated edition.

Result criterion: The selected methods can be traced to the correct editions and legal clause without silently substituting a later version.

Next review: On rule, source or control changes.

Certify the cybersecurity controls annually

NY-WW-CYBER-CERT · Requirement · NYDEC-750-2026 750-2.9(e)(5); 750-2.9(f)

Applies when: Municipalities responsible for POTWs.

What to do: Certify compliance with the controls, applicable logging and incorporated cyber response plan under 750-2.9(e)(1) through (3). Keep this distinct from the ERP certification.

When: By March 28 each year; first certification March 28, 2027.

Responsible role: Authorized municipal certification signer

Evidence to retain: Control evidence, unresolved findings, signed certification and DEC receipt.

Safe examination: Trace the certification to actual evidence and confirm that incomplete work is not represented as compliance.

Result criterion: A supported certification is signed by the correct authority and submitted on time.

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

Next review: Annually by March 28.

Use the authorized municipal signer and filing process

NY-WW-CERT-AUTHORITY · Requirement · NYDEC-750-2026 750-2.9(f)(1) through (3)

Implementation guidance: NYDEC-IMPLEMENTATION

Applies when: Required POTW ERP and cybersecurity certifications.

What to do: Use DEC supplied or approved forms and the required certification. The signer is the principal executive officer, ranking elected official or a qualifying executive level municipal official authorized in writing. Submit that delegation to DEC.

When: Before each certification submission.

Responsible role: Municipal executive or ranking elected official

Evidence to retain: Delegation, role and oversight basis, DEC authorization receipt and certification record.

Safe examination: Confirm the signer is eligible and reviewed information prepared under the required supervision. A contractor is not eligible solely because it performs the work.

Result criterion: The signer and filing method satisfy the rule; current DEC guidance uses nForm.

Next review: Each filing and signer change.

Complete cybersecurity hours for operator renewal

NY-WW-TRAINING · Requirement · NYDEC-650-2026 650.8; 650.12(c)(2)

Implementation guidance: NYDEC-IMPLEMENTATION

Applies when: New York certified wastewater operators with certifications expiring on or after January 1, 2027.

What to do: Complete approved cybersecurity training within the existing five year renewal hours: two hours for Grades 1, 1A, 2 and 2A; four hours for Grades 3, 3A, 4 and 4A. Confirm course approval and the individual renewal period.

When: Within the operator's applicable five year renewal period before renewal; the January date is an expiration threshold.

Responsible role: Certified operator and training coordinator

Evidence to retain: Grade, certification expiration, approved course and completed hours.

Safe examination: Compare the operator's grade and renewal dates with eligible cybersecurity training records.

Result criterion: The required approved hours fall within the applicable renewal period.

Next review: Each five year renewal.

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

Rehearse the response without affecting operations

NY-WW-EXERCISE · Recommended practice · NYDEC-IMPLEMENTATION Cybersecurity Incident Response Plans, exercise question

Applies when: POTW staff and response partners selected by the operating authority.

What to do: Use a clearly labeled discussion exercise to rehearse decisions, communications and recovery. DEC recommends regular exercises, preferably annually; this is not stated here as an additional annual filing or certification requirement.

When: Choose and record a practical exercise schedule.

Responsible role: Incident response owner and operating authority

Evidence to retain: Fictional scenario, participant roles, observations, actions and retest record.

Safe examination: Rehearse with no external transmission and no live control changes; record what was not demonstrated.

Result criterion: The exercise reveals actionable gaps and responsible owners without being treated as proof that every control works.

Next review: Recommended regularly, preferably annually; after material changes as appropriate.

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

Federal Water Planning

Complete the federal risk and resilience assessment

US-DW-RRA · Requirement · USEPA-AWIA SDWA 1433(a); RRA requirements

Applies when: Community drinking water systems serving more than 3,300 people.

What to do: Assess malevolent acts and natural hazards, physical and automated systems including security, monitoring, financial infrastructure, chemicals, operations and maintenance. A cyber worksheet supports this broader assessment but does not replace it.

When: Use the applicable population cohort and five year review cycle; the small system cycle RRA date was June 30, 2026.

Responsible role: Community water system owner and authorized assessment lead

Evidence to retain: Complete RRA scope, review record, certification by PWSID and receipt.

Safe examination: Check that the assessment covers the statutory categories beyond cybersecurity and that the correct system was certified.

Result criterion: The broader RRA and its certification meet the applicable cycle, with omissions identified explicitly.

Next review: Review, revise as needed and certify at least every five years.

Prepare the federal emergency plan from the assessment

US-DW-ERP · Requirement · USEPA-AWIA SDWA 1433(b); ERP requirements

Applies when: Community drinking water systems serving more than 3,300 people.

What to do: Prepare or revise the ERP using RRA findings, with resilience strategies, response procedures and equipment, impact reduction measures and detection strategies. Coordinate with local emergency planning committees to the extent possible.

When: No later than six months after actual RRA certification. December 31, 2026 is the latest listed small system date only when RRA certification occurred on June 30, 2026.

Responsible role: Community water system emergency plan owner

Evidence to retain: Actual RRA certification date, ERP edition, coordination record and ERP certification receipt.

Safe examination: Derive the ERP deadline from the actual RRA certification and trace RRA findings into the plan.

Result criterion: The plan and certification meet the actual six month deadline rather than an assumed common year end date.

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

Next review: After the applicable RRA certification and review cycle.

Submit the federal certifications by PWSID

US-DW-CERTIFICATION · Requirement · USEPA-AWIA-FILING Electronic submission and certification statements

Applies when: Each covered community water system's PWSID.

What to do: Submit the appropriate signed RRA and ERP certification statements using an accepted EPA method. Keep the actual RRA and ERP at the system rather than submitting those sensitive documents with the certification.

When: At the applicable RRA and ERP deadlines.

Responsible role: Authorized certifying official

Evidence to retain: PWSID, signed statements, actual submission dates and available acknowledgments.

Safe examination: Compare the system identifier, signer, statement type and deadline with the saved submission record.

Result criterion: Each system has the correct timely certification and a retained filing record.

Next review: Each required certification cycle.

Retain the federal assessment and plan securely

US-DW-RETENTION · Requirement · USEPA-AWIA ERP requirements; five year review requirements

Applies when: RRA and ERP for each covered community water system.

What to do: Keep a copy of the RRA and ERP for five years after certification and maintain the required review and revision cycle.

When: At least five years after the relevant certification.

Responsible role: System records custodian

Evidence to retain: Controlled document versions, access permissions, retention dates and retrieval record.

Safe examination: Verify secure retrieval of the certified editions and the next scheduled review without disclosing sensitive contents publicly.

Result criterion: Required editions remain retrievable for the retention period and the next review is assigned.

Next review: Each certification and retention review.

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

Reporting Clocks

Report qualifying CVA vulnerabilities

NYDOH-APP5E 5-E.1(c)(2); 5-E.5(e)

Qualifying event: A CVA vulnerability that may affect Subpart compliance, or a situation that may pose a public health risk.

Clock starts: Identification of the qualifying vulnerability or situation, with time and timezone.

Deadline: Within 48 hours of identification.

Recipient and channel: NYSDOH through the applicable section 5-1.77 process; confirm the system's current department contact and channel.

Record to retain: Scope decision, trigger, reporter and alternate, facts known, submitted version, recipient, submission time and receipt.

Notify DOH of a qualifying cyber incident

NYDOH-APP5E 5-E.3(e); 5-E.9

Qualifying event: A defined cybersecurity incident that has created or may create a public health hazard.

Clock starts: Determination that the qualifying incident occurred, with time, timezone and basis. Keep earlier detection times as separate chronology entries.

Deadline: As soon as possible and no later than 24 hours after determination.

Recipient and channel: NYSDOH in the prescribed section 5-1.77(a) manner; keep other applicable notices separate.

Record to retain: Detection and determination times, impact facts, decision owner, submission version, method, time, recipient and receipt.

Report a wastewater cyber incident promptly

NYDEC-750-2026 750-1.2(a)(27); 750-2.7(h)(1)

Implementation guidance: NYDEC-IMPLEMENTATION

Qualifying event: A cyber event causing or reasonably likely to harm normal operations, compromise SPDES program data or physical assets, or delay or prevent permit compliance.

Clock starts: Time the permittee becomes aware of the defined incident.

Deadline: As soon as possible and no later than 24 hours after awareness.

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

Recipient and channel: Regional water engineer. Current DEC instructions: submit the initial online report, then immediately notify the regional water engineer or manager orally. If unreachable, use DEC Dispatch at (844) 332-3267.

Record to retain: Awareness and discovery times, discoverer, known incident facts, affected IT or OT, disruption and duration, data or physical impacts, actions, online receipt and oral call record.

Complete the written wastewater incident report

NYDEC-750-2026 750-2.7(h)(2)

Implementation guidance: NYDEC-IMPLEMENTATION

Qualifying event: Follow up written report for the same defined wastewater cyber incident.

Clock starts: The same permittee awareness time used for the initial notice, not the initial submission time.

Deadline: Within 30 days after awareness.

Recipient and channel: Regional water engineer through DEC's current online report process.

Record to retain: Discovery date and time, discoverer, incident description, affected IT or OT, actual or anticipated disruption and duration, data and physical loss or absence of loss, mitigation or remediation, approved version and receipt.

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

Authority Register

NYDOH-APP5E · NYSDOH Appendix 5-E: Cybersecurity Requirements for Public Water Systems

Adopted regulation. Sections 5-E.1 through 5-E.11. Verified 2026-11-18.

https://healthweb-back.health.ny.gov/regulations/nycrr/title_10/part_5/docs/appendix_5e.pdf

NYDOH-SUBPART51 · NYSDOH Subpart 5-1: Public Water Systems

Agency hosted regulation compilation. Sections 5-1.33, 5-1.71 and 5-1.77; agency compilation revised October 8, 2026. Verified 2026-11-18.

https://healthweb-back.health.ny.gov/regulations/nycrr/title_10/part_5/docs/subpart_5-1.pdf

NYDEC-750-2026 · NYSDEC adopted revised Part 750 express terms

Adopted regulation; adoption published March 11, 2026. 750-1.2(a), 750-1.25(j) through (o), 750-2.7(h), 750-2.9(d) through (f). Verified 2026-11-18.

https://dec.ny.gov/sites/default/files/2026-03/6nycrr_part750_et_rev.pdf

NYDEC-650-2026 · NYSDEC adopted Part 650 express terms

Adopted regulation; training details also checked against agency implementation guidance. 650.8 and 650.12. Verified 2026-11-18.

https://dec.ny.gov/sites/default/files/2026-03/6nycrr_part650_et.pdf

NYDEC-616-2026 · NYSDEC adopted Part 616 express terms

Adopted regulation. 616.7(c)(2)(viii). Verified 2026-11-18.

https://dec.ny.gov/sites/default/files/2026-03/6nycrr_part616_et.pdf

NYDEC-ADOPTION-2026 · NYSDEC adopted wastewater cybersecurity amendments

Official adoption record. Notice of Adoption and rule making documents. Verified 2026-11-18.

https://dec.ny.gov/regulatory/regulations/proposed-emergency-recently-adopted-regulations/water-revisions/adopted-amendments-to-6-nycrr-parts-616-650-750

NYDEC-IMPLEMENTATION · NYSDEC Wastewater Cybersecurity Resources

Agency implementation guidance; adopted text controls legal criteria. Effective dates, applicability, reporting, plans, training and annual certification questions. Verified 2026-11-18.

https://dec.ny.gov/environmental-protection/water/water-quality/wastewater-treatment-resources/wastewater-cybersecurity-resources

NYDEC-COMPENDIUM · NYSDEC Wastewater Cybersecurity Regulations: Compendium of Resources

Agency guidance mapping incorporated documents to adopted requirements. Pages 2 through 24 and regulatory appendices. Verified 2026-11-18.

https://dec.ny.gov/sites/default/files/2026-03/wastewatercyber_compendium.pdf

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

IBR-EPA-CYBER-2024 · EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems

Specified edition incorporated into NY wastewater regulation. EPA 817-B-23-001, August 2024; incorporated by 750-1.25(j). Verified 2026-11-18.

https://www.epa.gov/system/files/documents/2024-08/epa-guidance-on-improving-cybersecurity-at-drinking-water-and-wastewater-systems-1.pdf

IBR-EPA-WWERP-2021 · EPA Wastewater Utility Emergency Response Plan: Template and Instructions

Specified edition incorporated into NY wastewater regulation; archived EPA edition. The older 2021 download URL now serves an October 2025 document and is not used as the edition reference.. EPA 817-B-21-003, July 2021; incorporated by 750-1.25(k). Verified 2026-11-18.

https://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=P1012S6R.txt

IBR-EPA-INCIDENT-2021 · EPA Incident Action Checklist: Cybersecurity

Specified edition incorporated into NY wastewater regulation; older URL filename is retained by EPA. EPA 810-B-17-004, February 2021; incorporated by 750-1.25(l). Verified 2026-11-18.

https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf

IBR-NIST-80082R3 · NIST Guide to Operational Technology Security

Specified edition incorporated into NY wastewater regulation. NIST SP 800-82r3, September 2023; incorporated by 750-1.25(m). Verified 2026-11-18.

https://csrc.nist.gov/pubs/sp/800/82/r3/final

IBR-NIST-80053R5 · NIST Security and Privacy Controls for Information Systems and Organizations

Specified edition incorporated into NY wastewater regulation; do not silently substitute later releases. NIST SP 800-53, December 10, 2020; incorporated by 750-1.25(n). Verified 2026-11-18.

https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

IBR-EPA-CIRP-2025 · EPA Drinking Water and Wastewater Systems Cybersecurity Incident Response Plan Template Instructions

Specified edition incorporated into NY wastewater regulation; publication edition is April 2025 despite URL date. EPA 810-F-25-017, April 2025; incorporated by 750-1.25(o). Verified 2026-11-18.

https://www.epa.gov/system/files/documents/2025-10/250414_cybersecurity-incident-response-plan-template-instructions_508c_0.pdf

USEPA-AWIA · EPA AWIA Section 2013 / SDWA Section 1433

Federal agency explanation of statutory duties. Risk assessment, emergency plan, certification deadlines and five year reviews. Verified 2026-11-18.

https://www.epa.gov/waterresilience/awia-section-2013

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

USEPA-AWIA-FILING · EPA How to Certify Your Risk and Resilience Assessment or Emergency Response Plan

Federal agency filing instructions. Certification statements, PWSID, filing methods and document retention. Verified 2026-11-18.

https://www.epa.gov/waterresilience/how-certify-your-risk-and-resilience-assessment-or-emergency-response-plan

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