

New York drinking-water cyber assessment preparation

Build a preparation record for the actual drinking-water system and its operating constraints. Determine the relevant DOH system tier and current instructions before selecting a deadline or signing a statement. Keep sensitive engineering and vulnerability records in the operator's approved repository.

Scope first. DOH publishes drinking-water-specific guidance, a requirements table and templates. Those instructions are distinct from DEC wastewater requirements and PSC utility IT rules. Confirm the system category, covered population and current dates directly with DOH.

Review period: _____ Responsible role: _____

Item	Records and next decisions	Working status
DW-01	System category and responsible role Record system classification, population, ownership and the designated decision maker. Next: Confirm the applicable DOH tier and any other authority; do not copy wastewater deadlines. Source: DOH1; DOH2	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
DW-02	Treatment and supply dependencies Prepare a restricted map of treatment, pumping, storage, communications and supporting IT. Next: Identify consequences of lost visibility, control or water-quality records. Source: DOH1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
DW-03	Vulnerability analysis inputs Gather the existing analysis, approved scope, asset inventory and unresolved findings. Next: Confirm the current review/submission instructions rather than treating a scan as the whole assessment. Source: DOH2	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
DW-04	Remote access and service accounts List authorized support paths, vendors, remote-access approvals and account owners. Next: Have the operator review exposed or poorly controlled paths before testing. Source: DOH1	☐ 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
DW-05	Operating limits and test permission Document approved methods, windows, stop conditions, communications and rollback authority. Next: Start from records and passive observations; do not run unapproved active tests on live controls. Source: DOH1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
DW-06	Program and response documents Gather the current cybersecurity program, contact chain and incident procedures. Next: Reconcile the written procedure with how the on-duty operator obtains help. Source: DOH1; DOH2	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
DW-07	Recovery and manual-operation records Locate controlled backups, restore instructions, spares and operator-approved fallback plans. Next: Record the date and scope of any restoration exercise; do not assume a backup restores the process. Source: DOH1	☐ Unknown ☐ Gathered ☐ Review ☐ N/A*
DW-08	Training and evidence register Gather relevant training records and index evidence, owners, dates and unresolved decisions. Next: Confirm current accepted training and certification instructions with the responsible authority. Source: DOH1; DOH2	☐ 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

DOH1 - [NYS DOH Cybersecurity for Public Water Systems](#)

DOH2 - [NYS DOH Drinking Water Cybersecurity Requirements Table](#)

Confirm the complete current DOH instructions, system classification and timing before selecting a deadline or signing a statement. This worksheet does not determine the applicable system tier.

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