Water and Wastewater Remote Access Review

Review selected decisions and controls for remote access using the guide's sector specific considerations and product agnostic architectures.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/water-remote-access-checklist/

Use the questions to prepare the review

These questions follow NIST SP 1800-45, which demonstrates example remote access architectures for water and wastewater utilities.

For this water utility access review, distinguish records you can locate from answers still to be confirmed. Assign an owner to each open question and explain exclusions.

The checklist records the responsible owner and evidence reference for each item, while remote access credentials and network details stay with their owners.

RA-01

Has the utility decided which functions should be remotely accessible?

Separate remote alarming, remote observation and two way process control. A remote connection can change the exposure of a safety related function. The decision belongs with the utility and its engineering/safety owners.

Evidence to gather

Approved use cases, process/safety review and functions kept on site.

To complete this item

Review the operational need and alternatives before selecting remote access technology.

Topic reference: NIST SP 1800-45; Section 3.1; PDF page 15.

Answer:

Owner, evidence reference and follow up date:

RA-02

Can you distinguish human access from process to process links?

An engineer logging in and a pumping station communicating through a provider network need different controls. Inventory both kinds of connection and the assets reached through each.

Evidence to gather

Interactive access inventory, telemetry/process links and external providers.

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

To complete this item

Identify unmanaged connections and assign a responsible owner to each.

Topic reference: NIST SP 1800-45; Section 3 and section 2.3; PDF page 15.

Answer:

Owner, evidence reference and follow up date:

RA-03

Are remote identities and permissions controlled?

Confirm who is allowed to reach which assets and for what purpose. Include employee, integrator and vendor accounts, how access is granted and how it is removed.

Evidence to gather

Identity/role register, approval records, permitted targets and revocation process.

To complete this item

Reconcile active users with the authorized operational roles.

Topic reference: NIST SP 1800-45; Section 3.3, Table 3; PDF page 17.

Answer:

Owner, evidence reference and follow up date:

RA-04

Is MFA applied to the remote access service?

Review the remote user's authentication path, default credentials and exceptions. Authentication at a suitable gateway protects access for legacy controllers that lack MFA of their own.

Evidence to gather

Access service settings, MFA coverage, identity design and documented exceptions.

To complete this item

Have the architecture owner address gaps with tested changes on control equipment.

Topic reference: NIST SP 1800-45; Section 3.3, Table 3; PDF page 17.

Answer:

Owner, evidence reference and follow up date:

RA-05

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

Is traffic over externally managed infrastructure protected?

Identify where the utility relies on an internet, telecom or other outside network. Confirm how confidentiality and integrity are protected across that path and who maintains the protective service.

Evidence to gather

Connection diagrams, encryption configuration and provider responsibilities.

To complete this item

Identify unprotected paths and have engineering agree on a suitable treatment.

Topic reference: NIST SP 1800-45; Section 3.3, Table 3; PDF page 16.

Answer:

Owner, evidence reference and follow up date:

RA-06

Does the connection terminate at a controlled boundary?

Give each remote user a controlled path into the process network. The traditional example terminates a session in a DMZ and uses a separately controlled connection onward. Other designs need equivalent, justified controls for their use case.

Evidence to gather

Architecture, remote access targets and boundary/traffic control configurations.

To complete this item

Review actual access paths against the approved design before changing rules.

Topic reference: NIST SP 1800-45; Sections 3.3 and 4.1; PDF page 19.

Answer:

Owner, evidence reference and follow up date:

RA-07

Are access windows and session removal defined?

Identify whether access is temporary or continuous and why. Define expiry, revocation and the process for confirming that a completed service visit no longer has unnecessary access.

Evidence to gather

Session/access approvals, expiration settings and completed work revocation records.

To complete this item

Review persistent vendor access with the utility owner and supplier.

Topic reference: NIST SP 1800-45; Section 3.3, Table 3; PDF page 18.

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

Answer:

Owner, evidence reference and follow up date:

RA-08

Can the utility identify and safely disable an unwanted connection?

Know which equipment and service to contact or disconnect. The approved isolation procedure accounts for the process impact of removing a link.

Evidence to gather

Connection inventory, labels, incident procedure and engineering authority.

To complete this item

Agree on the safe response and escalation before the connection is needed in an emergency.

Topic reference: NIST SP 1800-45; Section 3.3, Table 3; PDF page 17.

Answer:

Owner, evidence reference and follow up date:

RA-09

Are remote activities logged and available for review?

Confirm what the access service and boundary devices actually record, where logs are retained and who can use them. Separate a successful login record from evidence of the actions performed afterward.

Evidence to gather

Representative access/activity logs, retention and access controls.

To complete this item

Document visibility gaps and agree on feasible logging at the appropriate access layer.

Topic reference: NIST SP 1800-45; Sections 3.3 and 4.1; PDF page 17.

Answer:

Owner, evidence reference and follow up date:

RA-10

Are remote endpoints and file transfer paths protected?

The device used by a vendor or employee can introduce risk. Review endpoint protection and any controlled file upload route, including how files are checked before reaching OT assets.

Evidence to gather

Endpoint requirements, vendor arrangements and file transfer controls.

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

To complete this item

Resolve unsupported endpoint or transfer practices with the utility and access provider.

Topic reference: NIST SP 1800-45; Section 3.3; section 4.1; PDF page 20.

Answer:

Owner, evidence reference and follow up date:

RA-11

Are maintenance and updates coordinated with operations?

Keep remote service software and hardware under change and vulnerability management. Operations should know about remote activity so authorized work can be distinguished from an unexpected event.

Evidence to gather

Maintenance schedule, advisories, change approvals and operator notifications.

To complete this item

Agree on testing and a safe change window instead of applying an unscheduled update.

Topic reference: NIST SP 1800-45; Section 3.3, Table 3; PDF page 18.

Answer:

Owner, evidence reference and follow up date:

RA-12

Do supplier agreements explain security and operational responsibilities?

For vendor or cloud managed access, identify who administers identities, monitors service, responds to an incident and supports recovery. A service contract should make the handoffs understandable to the utility.

Evidence to gather

Contract/SLA, responsibility assignments, escalation contacts and access conditions.

To complete this item

Clarify unclear responsibilities before extending or renewing the access arrangement.

Topic reference: NIST SP 1800-45; Section 3.3; section 4.2; PDF page 20.

Answer:

Owner, evidence reference and follow up date:

RA-13

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

Do permissions and network rules limit access to what is needed?

Review targets, ports, protocols and directions against actual operational requirements. Keep necessary process communication separate from broad administrative access.

Evidence to gather

Approved flow list, access rules and rationale for exceptions.

To complete this item

Ask the process and architecture owners to resolve unnecessary or unexplained permissions.

Topic reference: NIST SP 1800-45; Section 3.3, Table 3; PDF page 18.

Answer:

Owner, evidence reference and follow up date:

RA-14

Is the chosen architecture supportable by this utility?

Consider staffing, distributed sites, provider dependencies and the effort to operate the safeguards. NIST's examples illustrate options, and the utility chooses the vendor and topology that fit its own sites.

Evidence to gather

Architecture decision, staffing/support plan, dependencies and recovery assumptions.

To complete this item

Review the selected design against the utility's capacity and engineering requirements.

Topic reference: NIST SP 1800-45; Sections 2.2 and 4.1 to 4.3; PDF page 12.

Answer:

Owner, evidence reference and follow up date:

All five checklists are also in one editable workbook: GDF Standards Readiness Checklists (XLSX).

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.