Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/water-remote-access-checklist/

STANDARDS PREPARATION CHECKLIST

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.

Baseline: NIST SP 1800-45, final, June 2026. Prepared November 1, 2026.

Use the questions to prepare the review

These are preparation questions for water/wastewater systems. NIST demonstrates example architectures, and the utility chooses the products that fit them. Other sectors adapt the questions through their own engineering review.

For this water utility access review, keep the answers you can tie to a located record apart from those still being confirmed. Name an owner for every open question and record why anything is out of scope.

Protect remote access credentials and utility network details. The checklist records the responsible owner and the evidence reference, and passwords and live access information stay in the utility's controlled systems.

Use these selected water utility access review questions to prepare a discussion. The references support the topics.

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

RA-01

Has the utility decided which functions should be remotely accessible?

Separate remote alarming, remote observation and two way process control. Each remote connection is weighed for its effect on safety related functions. 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 the record

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.

To complete the record

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:

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

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 the record

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 to legacy controllers as well as to devices that implement MFA directly.

Evidence to gather

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

To complete the record

Have the architecture owner address each gap through a tested design that suits the control equipment.

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

Answer:

Owner, evidence reference and follow up date:

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

RA-05

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 the record

Identify each path that needs protection 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?

Each remote user reaches the process network through a controlled path. 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 the record

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:

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

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 access closes when a service visit is complete.

Evidence to gather

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

To complete the record

Review persistent vendor access with the utility owner and supplier.

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

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 response accounts for the process impact of removing a link, and an approved isolation procedure builds on the labels.

Evidence to gather

Connection inventory, labels, incident procedure and engineering authority.

To complete the record

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:

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

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 the record

Document current logging coverage and agree on feasible additions 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 is part of the access path. 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.

To complete the record

Agree supported endpoint and 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:

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

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 the record

Agree on testing and a safe change window for each 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 the record

Clarify each responsibility, then extend or renew 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:

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

RA-13

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 the record

Ask the process and architecture owners to confirm the purpose of each permission and remove any that are surplus.

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.

Evidence to gather

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

To complete the record

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

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

Answer:

Owner, evidence reference and follow up date:

Web Addresses for the Sources Cited

1. NIST SP 1800-45; Section 3.1; PDF page 15: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-45.pdf#page=15

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

2. NIST SP 1800-45; Section 3.3, Table 3; PDF page 17: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-45.pdf#page=17
3. NIST SP 1800-45; Section 3.3, Table 3; PDF page 16: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-45.pdf#page=16
4. NIST SP 1800-45; Sections 3.3 and 4.1; PDF page 19: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-45.pdf#page=19
5. NIST SP 1800-45; Section 3.3, Table 3; PDF page 18: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-45.pdf#page=18
6. NIST SP 1800-45; Section 3.3; section 4.1; PDF page 20: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-45.pdf#page=20
7. NIST SP 1800-45; Sections 2.2 and 4.1-4.3; PDF page 12: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-45.pdf#page=12

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

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