

OT Vendor Access Review Worksheet

For small and mid-size utilities and the integrators who support their OT systems.

A vendor logging out does not mean their access has ended. Review one connection with operations, controls engineering, and security. Use configurations, logs, and vendor records. Assign unknowns on page 2.

In the last 90 days, how many hours was the vendor working, and how many hours could they connect?

Organization / site _____ Review date _____

Connection ID _____ Review lead _____

1 Identify the access

Vendor, approved work, and equipment they need to reach

Access path from vendor device to OT asset, including gateways and alternate routes

Evidence reviewed and date _____

90-day access comparison

90-day period _____ to _____ Work hours _____ Access hours _____

Work hours are elapsed hours when vendors worked on this path, counting each hour once. Access hours are hours when a vendor could start a session without new approval.

2 Check approval and enforcement

Who approves access, for which named users and devices, and for how long?

What enforces MFA, permitted destinations, privileges, and session monitoring?

3 Record what happens when the work ends

Item	What ends or remains and how you know
Remote session	
Authorization to start another session	
Network path to the OT asset	

4 Identify operational dependencies

What else uses this connection, including alarms, telemetry, control, and support?

Decide what needs to change

Worksheet continuation / Connection ID _____

5 Define the required outcome

What must remain connected between vendor visits, and why?

What access should end, when should it end, and which control will enforce it?

Consider approval and expiry rules, session termination, destination restrictions, segmentation, and physical isolation where appropriate.

6 Check the consequences before changing access

What could fail if this path is disconnected, including loss of remote visibility?

Who approves the change and reconnection, and how can they act if the path is unavailable?

How will you validate safely, and what triggers stopping or reversing the change?

Start with configuration and log review and passive monitoring. Any necessary active test requires an approved maintenance window, operations coordination, and a documented recovery method.

7 Assign unresolved work

Unknown or required change	Owner	Next action and due date

Review outcome _____ Decision owner / date _____

Record the decision, supporting evidence, and change record. Keep completed worksheets in your approved internal repository.

Basis and scope

Based on NSA, Hardening Department of War Critical Operational Technology Environments with Zero Trust Principles, October 2026, version 1.0. Pages 10-11 address remote and third-party access. Pages 16-17 address safe validation.

[Read the NSA guidance](#)

TANDMM interpretation of NSA guidance for defense and national security environments. Use your site’s engineering and change approvals. NSA does not endorse this worksheet or any product.

Worked example

Cedar Bend Water Utility / Fictional worked example

Connection VND-01 links a systems integrator to a remote pumping station. A shared site uplink also carries telemetry and alarms to the control room.

Review date 12 October 2026 Review lead OT manager

1 Identify the access

The integrator diagnoses PLC faults and makes approved logic changes. Access runs from a named vendor laptop through a VPN and jump host to the station’s engineering interface. The site uplink also carries control-room traffic.

Evidence reviewed includes the network drawing, VPN and firewall configuration history, maintenance tickets, and session logs for the 90-day period.

The 90-day comparison

18 hours of authorized vendor work. 2,160 hours when the vendor could connect. Access was available for 120 times the hours worked. Configuration history confirms continuous access availability for this example.

2 Check approval and enforcement

The maintenance supervisor approves each work ticket. Named vendor accounts use MFA and a jump host. Firewall rules restrict destinations, but the reviewed configuration has no automatic expiry tied to work completion. The security team can review session logs. Phishing resistance of the MFA method is unverified.

3 Record what happens when the work ends

Item	Observed behavior in this fictional review
Remote session	The vendor logs out. The sample session log confirms termination of that session.
Authorization to start another session	The account remains enabled and no fresh ticket approval is enforced by the gateway. The vendor could start another session.
Network path to the OT asset	The approved route through the gateway remains configured. The physical uplink remains connected for operational traffic.

4 Identify operational dependencies

Telemetry, alarms, and authorized remote commands share the uplink. Cutting that uplink would remove the control room’s view of the station and its ability to issue remote commands. Local control may continue, but its behavior during communications loss has not been verified.

Unknowns carried forward include alternate vendor routes, loss-of-communications behavior, and whether vendor traffic can use a dedicated maintenance path.

Worked example decision

Cedar Bend Water Utility / Fictional example / Connection VND-01

5 Define the required outcome

Preserve operational telemetry, alarms, and authorized control communications. Require fresh approval for vendor work. End the vendor session and its access grant when work finishes or the approved window expires, whichever occurs first. Log termination and check for remaining sessions.

Propose named accounts, phishing-resistant MFA, enforced access expiry, and restricted destinations. Evaluate physical isolation only for a dedicated maintenance path after dependencies and alternate routes are established. Do not disconnect the shared uplink.

6 Plan validation and reconnection

The OT manager and operations supervisor approve the change. An authorized administrator implements it. Reconnection requires a new approved work request. Any proposed physical control must remain operable through an independent management path when the maintenance path is disconnected.

First review configurations, logs, and passively observed traffic. Test in a representative environment where available. Any production test needs an approved maintenance window, a control-room operator, and a documented restoration procedure. Loss of expected telemetry or alarms, unexpected control behavior, or inability to restore access stops the test and triggers rollback.

7 Assign unresolved work

Unknown or required change	Owner	Next action and due date
Access expiry and MFA method	Security lead	Verify gateway capability and MFA method. Propose enforcement settings by 16 Oct.
Shared traffic and alternate routes	Network engineer	Review routes and passive traffic evidence. Identify a dedicated maintenance option by 19 Oct.
Local behavior and recovery	Controls engineer	Confirm communications-loss behavior with OEM and operations. Document validation and recovery by 20 Oct.

Decision on 12 October 2026

Further investigation required. Keep the shared uplink connected. Submit vendor-access changes through the utility's change process once the evidence and validation plan are complete. Evaluate a separate maintenance path for physical isolation.

Need help establishing what depends on a vendor connection? TANDMM can help review the access path and operational requirements.

MissionSuccess@tandmm.ai | <https://tandmm.ai>