OT Vendor Remote Access Checklist

A practical checklist for locking down third-party access to industrial systems without slowing down the plant. From 01001 HUB, OT Security & Zero Trust from the field.

1. Find every path in

You can't secure access you don't know about.

- [ ] List every VPN account that can reach OT networks, and who owns each one
- [ ] Check HMIs and engineering workstations for remote desktop and screen-sharing tools
- [ ] Look for cellular modems or gateways installed in cabinets or remote sites
- [ ] Review inbound firewall rules into OT and remove any that have no clear owner or purpose
- [ ] Use passive network monitoring to spot undocumented remote connections

2. One front door

Vendors should never land directly on the OT network.

- [ ] Route all third-party access through a single controlled entry point in the IT/OT DMZ
- [ ] Use a ZTNA gateway, privileged access tool or hardened jump host as that entry point
- [ ] Block and alert on any remote access path that bypasses it

3. Named identities, with MFA

No shared "vendor" accounts.

- [ ] Give every technician an individual account
- [ ] Enforce MFA on every remote session
- [ ] Tie each account to a vendor contract so access ends when the relationship does
- [ ] Review active vendor accounts at least quarterly and disable unused ones

4. Per-asset, just-in-time access

Reach the machine you're fixing, and nothing else.

- [ ] Limit each vendor to the specific assets they support
- [ ] Require approval from someone on site before a session starts
- [ ] Grant access for a set time window that expires automatically
- [ ] Restrict protocols to what the task needs (for example, HMI only, no file transfer)

5. Watch and record

Visibility protects the plant and settles disputes.

- ☐ Record privileged remote sessions
- ☐ Log every connection: who, what asset, when and for how long
- ☐ Alert on access outside approved windows or to unapproved assets

6. Give operations the off switch

Operators should always be in control.

- ☐ Show operators who is connected right now
- ☐ Let operators end any remote session instantly
- ☐ Agree in advance on when a session must be ended for safety

7. Put it in the contract

Technology covers half of it.

- ☐ Write approved remote access methods into vendor agreements
- ☐ Require vendors to notify you of staff changes and security incidents
- ☐ Make vendors accountable for protecting their technicians' credentials

More practical OT and Zero Trust guides every week at **01001hub.wordpress.com**. Read the full guide: "Securing Third-Party Remote Access to OT Without Slowing Down the Plant."

This checklist is general guidance, not a substitute for a site-specific risk assessment. Views are the author's own and don't necessarily reflect those of his employer.