Setting Up an Approval Workflow for Remote OT Sessions

When vendors need remote access to operational technology (OT) environments, the stakes are high. A misstep during a remote session can disrupt production, compromise safety systems, or introduce vulnerabilities. That is why many industrial sites now require an approval workflow before any remote session begins. The idea is simple: no vendor connects until the right people have reviewed and authorized the request. The execution, however, takes careful planning.

Approval workflows for remote OT access are not just about checking a box. They help ensure that every session is justified, time-bound, and traceable. When combined with session recording, they create a clear record of who did what and when. This article walks through the steps to build such a workflow, with practical things to watch at each stage.

Step 1: Define Who Can Request and Approve

Start by mapping out the roles involved. Not every vendor request should go to the same person. A routine firmware update from a trusted equipment vendor might only need a shift supervisor's approval. A request to modify a safety-critical controller may require sign-off from the engineering manager and the site safety lead.

What to watch: Keep the list of approvers small enough that requests do not bounce around waiting for a response. At the same time, avoid giving approval authority to someone who does not understand the operational risk of the requested change. A named account system helps here: each request identifies a specific person who will own the session, and each approver is a named individual, not a shared mailbox.

Step 2: Require a Reason and a Time Window

Every remote session request should include a clear purpose and an expected duration. The purpose could be a ticket number from your maintenance system, a brief description of the task, or both. The time window sets when the session will start and when it must end. This prevents open-ended access that lingers long after the work is done.

What to watch: Be realistic about the time window. If a vendor asks for four hours but the task rarely takes more than one, challenge the estimate. A too-long window reduces the value of time-bound approval. Also, make sure the request includes a fallback contact: someone who can be reached if the vendor needs to extend the session while it is in progress.



Step 3: Integrate with Your Access Gateway

The approval workflow is only useful if it actually controls the gateway through which remote sessions pass. Your OT remote access gateway should enforce the workflow automatically: no connection is established until an authorized person has approved the request. The gateway should also enforce the time window and disconnect the session when time expires.

What to watch: Check that the gateway logs every approval action - who approved, when, and for how long. These logs become part of your audit trail. Also, ensure the gateway can handle emergency overrides. Sometimes a critical situation demands immediate access, and your workflow should allow a senior operator to bypass the normal approval process while still logging the override.

Step 4: Layer in MFA and Session Recording

Approval alone does not prove that the right person is at the keyboard. Require multi-factor authentication (MFA) for both the vendor technician and the approver. This adds a second layer of verification beyond the named account and password.

Session recording complements MFA by capturing what happens during the session. When you have an approval workflow in place, the recording becomes the definitive record of whether the vendor followed the approved plan. For example, if the approval was for a view-only session but the recording shows configuration changes, you have clear evidence of a policy violation. This is where OT session recording matters most: it bridges the gap between what was authorized and what actually occurred.

What to watch: Decide whether you want recording to start automatically when the session begins or only after the vendor has authenticated. Starting recording after authentication captures the vendor's actions but might miss the login attempt itself. For most sites, recording the entire session from the moment the gateway opens the connection is the safer choice.

Step 5: Define Session Types and Permissions

Not every remote session needs the same level of access. Your workflow should distinguish between a view-only session, where the vendor can observe but not change anything, and a change session, where modifications are permitted. The approval process should reflect this distinction: a view-only request might need a single approver, while a change session might require two.

What to watch: Make sure the gateway enforces these permissions at the network level, not just by telling the vendor to behave. A view-only mode should actually block write commands to the target device. If your OT equipment does not support such restrictions natively, consider using a jump host or a protocol-aware proxy that can filter commands.

Step 6: Set Retention Policies for Records

An approval workflow generates a lot of data: request logs, approval records, session recordings, and audit logs. Decide how long you need to keep each type. Regulatory requirements may set a minimum retention period for certain industries. Even where no rule applies, keeping recordings for at least a year is a common practice for incident investigations.



What to watch: Storage costs add up, especially for video-style session recordings. Consider compressing recordings or storing them in a separate archive after a few months. Also, define a clear deletion policy and automate it. Manual cleanup often gets forgotten, leaving you with years of recordings that are hard to search and expensive to store.

Step 7: Test the Workflow Regularly

An approval workflow that nobody uses is worse than no workflow at all. Run periodic tests where a vendor requests access and goes through the full process. Include edge cases: what happens when the primary approver is unavailable? What if the session extends past the approved window? Test the override process as well, and verify that overrides are logged.

What to watch: Involve the operations team in the tests. They are the ones who will feel the friction if the workflow is cumbersome. Their feedback will tell you whether the approval steps are practical or just bureaucratic. Adjust the workflow based on what you learn.

Putting It All Together

Building an approval workflow for remote OT sessions is a matter of combining clear roles, time-bound requests, enforced permissions, and thorough recording. Each piece reinforces the others: the approval gives the session legitimacy, MFA confirms identity, and OT session recording provides the evidence that everything stayed within bounds. When done right, the workflow becomes a routine part of operations rather than an obstacle. Vendors get the access they need, and the site keeps control over its most critical systems.