SOP: Firewall 'Kill-Switch' Toggle

Pro-Tip's

Default-Off:

Never leave a remote access rule in "Standby." A firewall rule should only exist in a Disabled state. Enabling the rule is a manual, conscious act that must be logged in the TAG-OT-FRM-06 Audit Log.

"Security is not about blocking access; it is about controlling the gate."

1. Pre-Configuration Requirements

- Administrative access to the Vessel Gateway/Firewall (e.g., mGuard, FortiGate, Cisco).
- Verified MAC/IP address of the OEM Jump-Host or Remote Access Gateway.
- Approved Change Request (CR) from the Master or Chief Engineer.

2. Implementation: Hardware vs. Logical

OPTION A: Physical Hardware Kill-Switch (Recommended)

The most secure method is a physical key-switch that cuts power to the OEM Gateway or disconnects the network uplink.

- OFF Position: Physical Air-Gap. No data can physically cross the line.
- ON Position: Power/Link restored. Access is only possible during this window.

OPTION B: The Logical Access Gate

If a physical switch is unavailable, create a high-visibility policy. We use a Disabled Status (Off) rather than a “Block Action” to provide a simple one-click toggle for the ETO.

```
1. Create Policy: "OEM_REMOTE_ACCESS_KILL_SWITCH"
2. Source: [WAN_Interface] | [OEM_Static_IP_Only]
3. Destination: [OT_VLAN] | [Target_HMI_IP]
4. Service: [Specific_Ports_Only] (Avoid 'ANY')
5. Action: ALLOW
6. Status: DISABLE (The Critical Step)
```

Pro-Tip's

Default-Off:

Never leave a remote access rule in "Standby." A firewall rule should only exist in a Disabled state. Enabling the rule is a manual, conscious act that must be logged in the TAG-OT-FRM-06 Audit Log.

"Security is not about blocking access; it is about controlling the gate."

SOP: Firewall 'Kill-Switch' Toggle

3. Activation & Session Monitoring

1. **Open the Gate:** Switch physical key to ON or set Firewall Policy Status to Enable.
2. **Monitor Traffic:** Verify traffic is only flowing to the authorized HMI.
3. **Identity Verification**: Confirm the technician's identity via phone/official email before enabling.

Execution: The Hard Kill

Once the vendor signals work is complete, the ETO must execute the "Hard Kill" immediately:

- **Toggle Status:** Return key-switch to OFF or set the firewall rule back to DISABLED.
- **Clear Sessions:** Use the "Kill Session" command to force-drop any active packets.
- **Verify Log:** Confirm the traffic log shows 0 bps for the OEM source address.