CHECKLIST
FOR PRIVATE UTILITIES
TO STRENGTHEN CYBERSECURITY POSTURE OVER THE NEXT 90 DAYS

INTEGRATED WATER SERVICES

Here's a practical 10-point checklist for private utilities to strengthen their cybersecurity posture over the next 90 days. This is designed for operators of decentralized water and wastewater treatment systems, whether you're running an MBR plant, industrial pretreatment system, or remote telemetry network.

YOUR CHECKLIST:

1. CHANGE ALL DEFAULT PASSWORDS

- [ ] Audit every device, controller, and interface, especially SCADA systems, routers, and HMIs. Change default login credentials, and eliminate shared usernames.
- [ ] Use strong, unique passwords or passphrases for each login. Better yet, adopt a password manager.

2. IMPLEMENT ROLE-BASED ACCESS

- [ ] Give staff and vendors access only to the systems they need. Don't let a chemical delivery vendor have remote access to your PLC. Don't let seasonal maintenance techs retain login privileges all year.
- [ ] Use tiered permission levels: operator, supervisor, integrator, admin.

3. INSTALL A FIREWALL (AND SEGMENT YOUR NETWORK)

- [ ] Place your control systems behind a hardware firewall—and separate them from the business/office network. This is foundational.
- [ ] Flat networks are easy targets. Segmented networks are firebreaks for attackers.

4. CREATE A VENDOR ACCESS POLICY

- [ ] Document how and when third parties can access your system remotely. Require temporary VPN credentials, scheduled access windows, and a central access log. No more "set-it-and-forget-it" vendor VPN tunnels.

5. UPDATE SCADA AND PLC FIRMWARE

- [ ] Outdated firmware is a known vulnerability. Contact your OEM or system integrator to confirm current versions and apply any security patches.
- [ ] Schedule this as part of routine preventive maintenance.

6. BACK UP YOUR CONFIGURATIONS—OFFLINE

- [ ] Back up your PLC programs, SCADA configuration, and site-specific parameters to an external drive stored offsite.
- [ ] Cloud backups are good. Offline backups are better.

7. CONDUCT A TABLETOP CYBER DRILL

- [ ] Run a one-hour mock scenario with your team: "What happens if our SCADA interface goes dark?" Walk through who gets called, what systems are affected, and what fallback plans exist.
- [ ] Even simple drills build resilience and highlight blind spots.

8. LOCK DOWN USB PORTS

- [ ] Disable USB ports on HMIs and operator workstations, or require admin permission to use them.
- [ ] USBs are a leading infection vector in industrial systems.

9. CREATE A CYBER INCIDENT RESPONSE PLAN

- [ ] You don't need a 40-page policy—but you do need a one-page cheat sheet:

10. SCHEDULE A SCADA SECURITY ASSESSMENT

- [ ] Bring in a third-party (or your system integrator) to evaluate your system architecture, identify vulnerabilities, and prioritize upgrades.
- [ ] Ask about air-gapping, intrusion detection, and patch management schedules.

INTEGRATED WATER SERVICES

IWS Website

www.integratedwaterservices.com
info@integratedwaterservices.com
(833) 758-3338