CyberSecurity Tips for Public Water Systems

**Password hygiene** – Use a strong password. Change passwords frequently and prohibit sharing of passwords.

**Use secure networks only** and consider installing a virtual private network (VPN).

**Secure remote access methods** – All remote access should be subject to monitoring and audit.

**Risk assessment** – Identify system components and network connections to assess risk (i.e., know what you’re protecting).

**Train staff** to identify, respond and report cyberattacks. Implement an employee cybersecurity training program.

**Restrict all remote connections to SCADA systems**, specifically those that allow physical control and manipulation of devices within the SCADA network. One-way unidirectional monitoring devices are recommended to monitor SCADA systems remotely.

**Keep computers, devices, and applications**, including Supervisory Control and Data Acquisition (SCADA) /industrial control systems (ICS) software, *patched and up to date*.

**ADDITIONAL RESOURCES**
- MassDEP Cybersecurity Page
- EPA Cybersecurity Best Practices for the Water Sector
- EPA Cyber Incident Action Checklist
- AWWA Resources on Cybersecurity
- Water ISAC 15 Cybersecurity Fundamentals