Public Water System Cyber Hygiene Basics

Public water systems run operational technology (OT) and information technology (IT) systems that can be vulnerable to cyberattacks. Take the actions outlined below to reduce risk and increase resiliency.

Reduce Internet Exposure

OT devices can be easy targets when connected to the internet. Reduce the exposure of key assets by keeping controllers and remote terminal units disconnected from the public-facing internet.

Conduct an Inventory of IT/OT Assets

Create a list of hardware and software assets. The most important assets to inventory are the devices connected to the internet and those where manual operations are not possible.

Always Change Default Passwords

Passwords for all water system components and computers should be strong, unique, and complex. Default passwords are easy for malicious actors to discover. Passwords should be changed regularly.
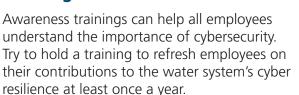
Conduct Regular Assessments

Do regular cybersecurity assessments to track and understand the existing vulnerabilities within IT and OT systems. Once vulnerabilities are known, take steps to address them.

Create Response and Recovery Plans

Create an incident response plan for a cybersecurity event. Exercise the plan by testing it out at least once a year. See the Cybersecurity Infrastructure & Security Agency (CISA) factsheet *Incident Response Plan Basics*.

Backup IT/OT Systems

Do regular backups of IT and OT systems so you can recover if the water system is compromised. Keep backups isolated from network connections.

Reduce Exposure to Vulnerabilities

Mitigate known vulnerabilities and keep all software patches and security up-to-date. CISA has a Known Exploited Vulnerabilities Catalog that can be used to help water systems prioritize IT updates. The catalog can be found online.

Cybersecurity Awareness Trainings

Awareness trainings can help all employees understand the importance of cybersecurity. Try to hold a training to refresh employees on their contributions to the water system's cyber resilience at least once a year.