Cybersecurity Resources For Public Water Systems

Have You Done Your Cybersecurity Assessment Yet?

All Public Water Systems Must Complete a Cybersecurity Assessment & Continue to Operate & Maintain Their Systems to Ensure Safe Drinking Water.

Introduction

MassDEP/DWP considers cybersecurity as a vital and routine part of Emergency Response Plan (ERP) requirements pursuant to 310 CMR 22.04(13) and expects all PWS to include cybersecurity in routine operations and maintenance, perform a cybersecurity assessment as part of their emergency planning responsibilities and to be prepared for MassDEP/DWP to evaluate the results of their cybersecurity assessments and their ERPs during sanitary surveys or as requested by MassDEP/DWP.

All PWS that have operational technology (OT) equipment with a cybersecurity risk must complete a cybersecurity assessment and be ready to present the cybersecurity assessment report during the sanitary survey process or as requested by MassDEP/DWP.

OT equipment is defined as hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise.

OT equipment presenting a cybersecurity risk includes equipment that is or may occasionally be connected after initial installation:

- to a computer (for any reason including alarm reporting and patching) or
- to a network (local, wide area, or internet) or
- is remotely accessible (either for control or monitoring)

Note: A PWS may determine that they do not have OT equipment presenting a cybersecurity risk. If a PWS makes that determination, it must provide MassDEP/DWP with its determination in writing by completing and returning the ERP-CS-OT form https://www.mass.gov/doc/cybersecurity-statement-no-ot-risks-erp-cs-ot/download to MassDEP/DWP at programm.director-dwp@mass.gov. Subject: "Cybersecurity Assessment Statement No Operational Technology-OT Risk".

Resources

MassDEP/DWP strongly encourages water systems to take advantage of free cybersecurity assessments to identify potential cybersecurity risks and ensure that their systems are adequately protected.

EPA

FREE

Cybersecurity Evaluation Program

Water Sector Cybersecurity Evaluation Program: EPA considers cybersecurity best practices as critical for water utilities to reduce the risk of cybersecurity threats and has developed resources to support states and PWS cybersecurity needs including the Water Sector Cybersecurity Evaluation Program: EPA's Cybersecurity Evaluation Program will conduct a cybersecurity assessment for PWS. The assessment will follow the checklist in the guidance on Evaluating Cybersecurity in PWS Sanitary Surveys which will then generate a report that will highlight gaps in cybersecurity.

How to Apply

Use the following link or scan the barcode:

tinyurl.com/EPACYBER-FREE-EVALUATION

SCAN ME

Additional Resources

- **MassDEP DWP Cybersecurity Improvement Grant for PWS** Click Here
- **EPA: Cybersecurity Technical Assistance Program for the Water Sector:** Subject matter expert available to answer questions regarding cybersecurity matters. https://www.epa.gov/waterriskassessment/forms/cybersecurity-technical-assistance-program-water-sector

Self-Assessment Resources

- **EPA WCAT Tool:** Water Cybersecurity Assessment Tool and Risk Mitigation Plan Template (xlsx)
- **EPA Checklist**: Guidance on Evaluating Cybersecurity During Public Water Sanitary Surveys (pdf) (Checklist in Appendix)
- **AWWA Cybersecurity Tool** AWWA Water Sector Cybersecurity Risk Management Tool

FREE CISA Cybersecurity Resources

- **CISA CPGs self-assessments with CSET:** https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- **CISA Vulnerability Scanning** https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services
- **CISA Region 1 Cybersecurity resources:** https://www.cisa.gov/about/regions
- **CISA Region 1 Cybersecurity Advisors contact:** CISARegion1@hq.dhs.gov

Cybersecurity Resource Hub

Resources for PWS to improve cybersecurity defenses, mitigate cyberattack risks, and enhance overall resiliency and compliance.

Click Here

SCAN ME

For questions and technical assistance on cybersecurity MassDEP/DWP can be contacted at program.director-dwp@mass.gov.
Subject: Cybersecurity.

1. **Think Before You Click, Recognize and Report Phishing**: If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
2. **Update Your Software**: Don't delay - If you see a software update notification, act promptly. Better yet, turn on automatic updates.
3. **Use Strong Passwords:** Make sure it's long – at least 15 random characters, and avoid using common or easily guessable passwords, such as simple keyboard patterns or slightly modified words, when creating your passwords. Don't share your password with anyone or use the same or similar password for multiple accounts.
4. **Enable Multi-Factor Authentication:** You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked.