IMPLEMENTING A CYBERSECURITY PROGRAM AT YOUR WATER OR WASTEWATER UTILITY

Steps for Responding to a Suspected Cyber Incident at a Water or Wastewater Utility

Response

1. Disconnect compromised computers from the network. Do *not* turn off or reboot systems.
2. Assess the scope of the compromise, and isolate all affected IT systems.
3. Open a ticket with your antivirus software or security service vendor.
4. Assess any potential damage, including impacts to treatment processes or service disruptions.
5. Initiate manual operation of equipment if control systems have been compromised.
6. Distribute any advisories or alerts to customers as needed, including customers whose records may have been compromised.
7. Identify methods to scan all IT assets to eradicate malicious code. Assess and implement recovery procedures.

Reporting

1. Report the incident to local law enforcement and the primary oversight agency (typically, the state).
2. Contact the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870 or NCCIC@hq.dhs.gov. NCCIC can assist your utility with identifying and restoring affected systems, coordinating federal assistance, and improving security.
3. Submit an incident report through WaterISAC (analyst@waterisac.org; 866-H2O-ISAC).

Important Contact Information

Role	Point of Contact	Phone Number	Email
IT service vendor			
Local law enforcement			
State agency			
National Cybersecurity and Communications Integration Center (NCCIC)		888-282-0870	NCCIC@hq.dhs.gov
WaterISAC		866-426-4722 (866-H2O-ISAC)	analyst@waterisac.org

For More Information

For more information on available cybersecurity guidance and resources:

- WaterISAC 10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks
- Department of Homeland Security Critical Infrastructure Cyber Community Voluntary Program
- American Water Works Association (AWWA) Cybersecurity Guidance and Tool