STATE of CONNECTICUT
DEPARTMENT of PUBLIC HEALTH
Cybersecurity Self-Assessment Checklist for PWS

The CT DPH Drinking Water Section is providing this Cybersecurity Self-Assessment Checklist for PWS use to assist in the preparation of the cybersecurity prevention and response component of the required Emergency Response Plans (ERPs) pursuant to the American Water Infrastructure Act of 2018 and State regulations**.** Public Water Systems should strive to answer "Yes" to all questions below.

Public Water System Information			
PWS ID:		**PWS Name:**	

Does your Public Water System:		**YES or NO**
1.	Keep an inventory of control system devices and ensure this equipment is not exposed to networks outside the utility? • *Never allow any machine on the control network to "talk" directly to a machine on the business network or on the Internet.*	
2.	Segregate networks and apply firewalls? • *Classify IT assets, data, and personnel into specific groups, and restrict access to these groups. Be alert for unusual behavior in Operational Technology (OT) and IT systems, such as unexpected reboots of digital controllers and other OT hardware and software, and delays or disruptions in communication with field equipment or other OT devices. Enhance logging to investigate anomalous activity – including collecting more logs and increasing storage capacity and retention time.*	
3.	Use secure remote access methods? • *A secure method, like a virtual private network, should be used if remote access is required.*	
4.	Establish roles to control access to different networks and log system users? • *Role-based controls will grant or deny access to network resources based on job functions.*	
5.	Backup Data? • *Implement and test data backup procedures on both IT and OT networks and ensure copies of backups are isolated (stored offline) from the network.*	
6.	Require strong passwords and password management practices? • *Use strong passwords and have different passwords for different accounts.*	
7.	Stay aware of vulnerabilities and implement patches and updates when needed? • *Monitor for and apply IT system patches and updates. CISA maintains a catalog of Known Exploited Vulnerabilities that utilities are encouraged to review to identify vulnerable systems.*	
8.	Implement multi-factor authentication? • *After changing passwords, make implementing multi-factor authentication (MFA) a priority. MFA significantly reduces your risk from almost all opportunistic attempts to gain entry into your systems.*	
9.	Enforce policies for the security of mobile devices? • *Limit the use of mobile devices on your networks and ensure devices are password protected.*	

10.	Have an employee cybersecurity training program? • *All employees should receive regular cybersecurity training.*	
11.	Involve utility executives in cybersecurity? • *Organizational leaders are often unaware of cybersecurity threats and needs.*	
12.	Incident Response Plans? • *Create, maintain, and exercise a cyber incident response and continuity of operations plans.*	
13.	Monitor for network intrusions? • *Be capable of detecting a compromise quickly and executing an incident response plan. Malicious cyber actors are known to target organizations on weekends and holidays when there are gaps in organizational cybersecurity. Identify surge support for responding to an incident.*	
14.	Manual Operations? • *Have a resilience plan that addresses how to operate your system if you lose access to or control of critical OT or IT systems – including the ability to sustain manual operations for extended periods.*	

NOTE: For more information about each of these questions, see WaterISAC *15 Cybersecurity Fundamentals for Water and Wastewater Utilities* at https://www.waterisac.org/fundamentals.