CYBERSECURITY PROGRAM

Purpose: To establish a cybersecurity program that outlines activities, personnel roles, and policies and procedures for the purpose of ensuring reasonable and appropriate cybersecurity safeguards that protect a public water system.

This document should be reviewed for updates annually and kept confidential by the system for its use and purposes. Systems serving more than 50,000 people are required to certify their cybersecurity program every five years in accordance with Subpart 5-1.33(e).

A cybersecurity program must be made available upon the request of the New York State Department of Health (the Department).

Version: 001

Sections:

I. FACILITY INFORMATION

Instructions: Fill in the facility and Designated Individual or Primary Contact Information.

COMMUNITY WATER SYSTEM INFORMATION	
System Name:	
PWS ID Number	NY
Population Served:	
Street Address:	
City, State, Zip Code	
Phone #:	
Email Address:	

DESIGNATED INDIVIDUAL OR PRIMARY CONTACT INFORMATION *(Designated individual **required** for systems serving more than 50,000 people)*	
Individual Name:	
Individual Email:	
Individual Phone #:	

II. IDENTITY AND ACCESS MANAGEMENT

Purpose: To support and address access management protocols as required by the cybersecurity program requirements (Title 10 NYCRR Part 5, Subpart 5-1, Section 5-1.33 and Subpart 5-1, Appendix 5-E).

a. User Rights and Access Management

Instructions: Use this table to define and standardize user roles, their scope of work, and access privileges to Operational technology (OT) and Information Technology (IT) networks and systems.

USER ROLE	SCOPE OF WORK	ACCESS PRIVILEGES

b. Roles & Responsibilities

Instructions: Fill in employee name, user role, current responsibilities, and account access privileges.

***Note**: Compare this table to the "User Rights and Access Management" table to highlight where user roles may not be aligned with access privileges and where access privileges could be made more stringent* [1].

NAME	USER ROLE (e.g., Admin, Management, Operator, etc.)	RESPONSIBILITIES	ACCESS PRIVILEGES

III. CYBERSECURITY PROGRAM DOCUMENTS AND ACTIVITIES

Purpose: To outline the required cybersecurity program documents for community water systems.

Part 1 - Cybersecurity Program Required Documents

[1] Following the principle of least privilege is recommended.

Instructions: Complete and sign the table below to verify that all cybersecurity program documents and activities have been reviewed and updated, as necessary. Verify that all documents required for submission to the Department were submitted in accordance with 10 NYCRR Part 5, Subpart 5-1, Section 5-1.33 and Subpart 5-1, Appendix 5-E.

- ☐ *Cybersecurity Vulnerability Analysis (CVA)*
- ☐ *Cybersecurity Incident Response Plan (CIRP)* (This may be part of the Community Water System's Emergency Response Plan (ERP))

***only required for public water systems serving more than 50,000 people:*

- ☐ ***Cybersecurity Program Certification*[2]
- ☐ ***Cybersecurity Annual Written Report*[3]

Note: *The CVA, the CIRP, and the **Cybersecurity Program Certification must be submitted to the Department every five years alongside the water system ERP.*

Document	Required outcomes	Date Last Reviewed	Date Last Updated	Date Last Submitted to the Department	Assessor Signature
Cybersecurity Vulnerability Analysis (CVA)	☐ Vulnerabilities are identified and reported to the Department within 48 hours of detection ☐ Actions established to mitigate or remediate vulnerabilities ☐ Identification and assessment of cyber risks to OT and nonpublic information				
Cybersecurity Incident Response Plan	☐ Response activities mitigate the impacts on normal operations ☐ Response activities limit physical or structural damage				

[2] Only required for systems serving >50,000 people

[3] Only required for systems serving >50,000 people. Submission to governing body required annually.

Document	Required outcomes	Date Last Reviewed	Date Last Updated	Date Last Submitted to the Department	Assessor Signature
**Cybersecurity Program Certification	☐ Submitted along with Emergency Response Plan (ERP) to verify compliance of regulatory requirements				
**Cybersecurity Annual Written Report	☐ Annual written report sent to relevant governing body				

Part 2 - Cybersecurity Program Required Activities

Instructions: Complete and sign the table below to demonstrate that your facility incorporates the following required activities into its cybersecurity program. This template describes the elements necessary for your cybersecurity program and can be useful internally for assessing the strength and quality of activities being done to improve cybersecurity posture.

Ensure that the following required processes, policies, and procedures are included in your Cybersecurity Program:

- ☐ Identity and Access Management
- ☐ Remote Access Architecture
- ☐ Asset Inventory
- ☐ Defensive Architecture
- ☐ Cybersecurity Basic Training
- ☐ Cybersecurity Vulnerability Reporting
- ☐ Cybersecurity Incident Reporting
- ☐ Restoring Normal Operations
- ☐ **Network logging and monitoring[4]

[4] Only required for systems serving >50,000 people

***Note**: Review **Appendix A: Other Recommended Policies, Procedures or Components**, as guidance for strengthening your water system's cybersecurity resilience.*

Cybersecurity Program Required Activities	Sub - Activities	Related Policies, Procedures or Plans (*write in*)	Brief description of current capabilities or compensating controls in place	Assessor Signature
Identity and Access Management	☐ Identity and access management procedures, including change management and periodic review of user accounts. ☐ Separate and unique IT and OT user accounts or compensating controls ☐ Multi-factor authentication ☐ Remote-access technology is limited to need-only ☐ All OT default passwords are replaced for unique passwords or compensating controls are in place			
Remote Access Architecture	☐ Implementation of secure configurations for remote access to OT and nonpublic information ☐ Remote-access technology is limited to need-only			
Asset Inventory *(An Asset Inventory verification template is available in Section IV.)*	☐ Cybersecurity Asset Inventory is maintained and reviewed annually			

Defensive Architecture	☐ Proactively and continuously monitor system activities			
Cybersecurity Basic Training	☐ All operators hold a minimum of one hour approved Cybersecurity Training			
Reporting	☐ Incidents are reported within 24 hours of detection ☐ Vulnerabilities are reported within 48 hours of detection			
Restoring Normal Operations	☐ Procedures for restoring normal operations and services are in place			
**Monitor and log Network activity	☐ Monitor and log network activity procedures are in place			

IV. VERIFICATION OF ASSET INVENTORY

Purpose: To verify the existence and maintenance of an asset inventory.

Instructions: Complete and sign the table below to verify the water system maintains an asset inventory. The guidelines below may be used to assess and improve the quality of your system's asset inventory. The Inventory is held in a central repository that is secure and accessed only by facility personnel with applicable clearance.

a. The inventory is inclusive of all IT and OT assets that are owned or hosted by the facility to the best of the facility's knowledge.
b. The inventory is updated alongside major infrastructure changes that alter IT or OT assets, or as inventory changes.

a. ASSET INVENTORY VERIFICATION

DATE	NAME	ASSESSOR SIGNATURE

APPENDIX A: OTHER RECOMMENDED POLICIES, PROCEDURES, OR COMPONENTS

Instructions: Use this checklist to evaluate additional processes that can be included in your system's cybersecurity program to improve cybersecurity posture. These components are not required but are strongly recommended for enhanced cybersecurity resilience. The table below is provided to document these additional policies, procedures and components in place at your water system. Alternative wording may be used.

- ☐ *Cybersecurity Program Evaluation Policy and Review Schedule*
- ☐ *Cyber Incident Business Continuity and Recovery Plan*
- ☐ *Cybersecurity Vulnerability Mitigation Policy*
- ☐ *Corrective and Preventive Action Procedure*
- ☐ *Vulnerability Risks Register*
- ☐ *System or Device End of Life Policy*
- ☐ *Network Activity Monitoring and Logging Policy*
- ☐ *Network Activity Monitoring and Logging review Schedule*
- ☐ *Visitor Education and Facility Restrictions Policy*
- ☐ *Compliance Policy*
- ☐ *Network Diagrams*
- ☐ *Vulnerability Scanning Software*
- ☐ *Remote Access Policy*

Document	Date Last Reviewed	Date Last Updated

APPENDIX B: TERMS AND DEFINITIONS

Purpose: Terms and Definitions as defined in Part 5-1 cybersecurity regulations (Title 10 NYCRR part 5 appendix E).

Control	Any mechanism, safeguard, policy or security measure that is put in place pursuant to an implementation specification to satisfy the requirement for a security measure.
Compensating control	Any alternative measure that is put in place to satisfy the requirement for a security measure.
Cyber asset Inventory	An inventory of: (1) operational technology assets that are reachable or accessible by a management, control, or communications protocol; and (2) information technology assets that are physically or logically connected to operational technology.
Cybersecurity event	any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse a covered water system's operational technology.
Cybersecurity incident	a cybersecurity event or attack that, directly or indirectly: (1) has an adverse impact on any operations of the covered water system that affect the ability of the covered water system to comply with the requirements of this Subpart; or (2) has a reasonable likelihood of compromising any operations of the covered water system or any of its components; or (3) actually or imminently jeopardizes the confidentiality, integrity, or availability of nonpublic information related to the covered water system, or results in loss or damage to the covered water system's normal operations.
Cybersecurity vulnerability analysis (CVA)	The analysis of vulnerability to cyber-attack that each covered water system shall conduct in accordance with Public Health Law section 1125(2)(k) and subdivision 5-1.33(c) of this Subpart.
Department	the New York State Department of Health.
Information Technology	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or

	disposition of electronic information, provided that information technology does not include operational technology.
Multifactor Authentication	User identity authentication that requires a user to provide at least two of the following distinct factors for successful authentication: (1) something the user knows; or (2) something the user has; or (3) something the user is.
Nonpublic information	all electronic information that is not publicly available information and is: (1) a covered water system's business-related information, where compromise to its confidentiality, integrity, or availability would impact that system's ability to comply with the requirements of this Subpart; or (2) information determined by the covered water system to pose a security risk to the operation of the water system in accordance with subdivision 5-1.33(h) of this Subpart.
Operational Technology	Hardware, software, and firmware that detect or cause changes in physical processes through the direct control and monitoring of industrial equipment, assets, processes, and events in the covered water system.
Principle of least privilege	A security principle that restricts the access privileges of users, or processes acting on behalf of users, to the minimum necessary to accomplish assigned tasks.
User	Any employee, contractor, agent or other person that operates a covered water system and is authorized to access and use any operational technology and data of such covered water system.

Resources for additional Terms and Definitions:

Glossary | NICCS