[Water System Name]

# CYBERSECURITY PLAN

Just as with any critical enterprise or corporation, cyberattacks pose a threat to drinking water systems, and therefore must be considered. Cyberattacks may interrupt treatment and/or distribution by manipulating valves, overriding alarms, disabling pumps, or even taking over industrial controls systems that may remotely monitor the system or automate treatment and distribution. Should a cyber threat access the system’s online records, even the security of customer personal data is threatened. The following cybersecurity plan is to assist in implementing cybersecurity practices that help prevent, detect, respond, and recover from cyber incidents.

## Key Contacts

The following are the personnel/resources imperative to a cyberattack. Refer to the water system’s Emergency Response Plan (ERP) for additional reporting contacts and procedures should the water system be notably impacted as a result of a cyberattack. For guidance on the proper procedures for **reporting cyber incidents,** **see the EPA Fact Sheet attached to the end of this cyber security plan**.

| Role/Resource | Name  | Contact (phone/email/etc.) |
| --- | --- | --- |
| System Designated IT person |  |  |
| Other |  |  |
| Internet Service Provider |  |  |
| Police | Local Department |  |
| **CISA** - Federal Asset Response | Cybersecurity and Infrastructure Security Agency (CISA) | (888) 282-0870[www.us-cert.cisa.gov/forms/report](http://www.us-cert.cisa.gov/forms/report)  |
| **EPA** - Federal Centralized Response | EPA’s Water Infrastructure and Cyber Resilience Division (WICRD) | WICRD-outreach@epa.gov[Contact Us about Water Resilience](https://www.epa.gov/waterresilience/forms/contact-us-about-water-resilience)  |
| **FBI** - Federal Threat Response | Internet Crime Complaint Center (IC3) | OKC (405) 290-7770[www.ic3.gov](http://www.ic3.gov)  |

## Best Management Practices

In order to maintain good cybersecurity, the following best practices should be implemented:

* Identify an overall Information Technology (IT) security lead to be the primary point of local contact during a cyber incident.
* Change all passwords to something besides the default password. These passwords should only be known by necessary personnel.
* Update the system’s Emergency Response Plan to include response procedures for cyber incidents and ensure the proper government and local emergency contacts are included.
* Identify all susceptible technologies in/at the system to consider potential cyber targets via an asset inventory.
* Maintain physical security measures to prevent unauthorized physical access.
* Ensure computer systems have updated anti-virus software installed.
* Conduct a detailed assessment of vulnerabilities. EPA as well as CISA offer tools and services in completing these assessments (see “Additional Resources”).
* Train staff on what cybersecurity is, the best practices to be implemented at the facility, and how to respond to a cyberattack should one occur.

## Susceptible Technologies

| Asset Name (cont.) |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |

The following is a list of all the technologies related to the water system that would be susceptible to a cyberattack (PLCs, laptops, tablets, automatic pumps/valves/etc.).

| Asset Name |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |

## Physical Security

Maintaining physical security can reduce the risk of unauthorized access to technology. Below are the physical security measures of note at the water system.

| Topic | Description |
| --- | --- |
| Perimeter Controls(Fences, gates, etc.) |  |
| Access Controls(Guards, locks, key cards, passwords, etc.) |  |
| Other |  |

## Threat Identification/Training

Training will be provided annually to employees that educates on cybersecurity associated with the system. The end goals of the training shall be that:

* Staff can identify a cyber threat;
* Staff know who to notify in the event of a cyber threat/attack;
* Staff know what immediate actions to take to isolate the targeted technology in the event of an attack.

## Response Procedure

In the event of a cyberattack, the following response procedures shall be followed:

* Disconnect compromised computers from the network to isolate breached components and prevent further damage, such as the spreading of malware.
* Properly report event to governing bodies (refer to EPA’s “Reporting Process” flyer).
* Notify IT personnel/IT vendor of the incident and the need for emergency response assistance.
* Assess any damage to utility systems and equipment, along with disruptions to utility operations.
* Implement actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary) and provide public notification (if required).
* Document key information on the incident, including any suspicious calls, emails, or messages before or during the incident, damage to utility systems, and steps taken in response to the incident (including dates and times).

## Additional Resources

Complete a Cybersecurity Assessment with the EPA:

Through EPA’s “Cybersecurity Evaluation Program”, this system can work with a cybersecurity professional virtually to complete an assessment using EPA’s Water Cybersecurity Assessment Tool.

* [Cybersecurity Evaluation Program](https://www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program)
* [EPA’s Water Cybersecurity Assessment Tool (WCAT)](https://www.epa.gov/system/files/documents/2023-03/EPA%20Water%20Cybersecurity%20Assessment%20Tool%201.0_0.xlsx)

Technical Assistance from the EPA:

The system can submit cybersecurity questions and receive one-on-one remote assistance from a cybersecurity subject matter specialist.

* [Cybersecurity Technical Assistance Program for the Water Sector | US EPA](https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector)

EPA’s Cybersecurity Webinar:

This webinar is a good introduction to the basic principles of cybersecurity.

* [Cybersecurity 101 Training for Water Systems Webinar (youtube.com)](https://www.youtube.com/watch?v=e2QDbgrojb0)

CISA Cyber Risk and Resources:

Infographic that highlights cyber risks and provides available resources that support the Water and Wastewater Systems Sector.

* [Cyber Risks & Resources for the Water and Wastewater Systems Sector – Supply Water National Critical Function Infographic (cisa.gov)](https://www.cisa.gov/sites/default/files/2023-02/infographic-supply-water-national-critical-function-102021-508.pdf?utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term=)

CISA’s Multi-Asset and System Assessment:

Document outlining CISA’s Multi-Asset and System Assessment (MASA). This assessment provides an output that includes a criticality ranked asset list, attack types by asset, and vulnerabilities.

* [Multi-Asset and System Assessment (MASA) Fact Sheet 2023.pdf (cisa.gov)](https://www.cisa.gov/sites/default/files/2023-06/Multi-Asset%20and%20System%20Assessment%20%28MASA%29%20Fact%20Sheet%202023.pdf)

CISA Guide to Getting Stated with a Cybersecurity Risk Assessment:

* [Guide to Getting Started with a Cybersecurity Risk Assessment, Dec. 2022 (cisa.gov)](https://www.cisa.gov/sites/default/files/2023-02/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508-r1.pdf)

Office of Water (4608T) EPA 810-F-23-003

January 2023

WHAT TO REPORT TO THE FEDERAL GOVERNMENT

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include:

* Who you are,
* Who experienced the incident,
* What sort of incident occurred,
* Details of incident impact,
* How and when the incident was initially detected,
* What response actions have already been taken, and
* Who has been notified.

WHEN TO REPORT TO THE FEDERAL GOVERNMENT

Utilities are encouraged to report all cyber incidents when there is any:

* Loss of data, system availability, or control of systems;
* Impact to any number of victims;
* Detection of unauthorized access to, or malicious software present on, critical information technology systems;
* Affected critical infrastructure or core government functions; or
* Impact to national security, economic security, or public health and safety.

CYBER INCIDENT

REPORTING PROCESS

WHERE TO REPORT:

WHY IS IT IMPORTANT TO REPORT CYBER INCIDENTS?

A cyber incident could jeopardize drinking water and wastewater utilities by allowing access to private customer/employee information, changing chemical levels in water treatment processes, or denying access to critical systems. Cyber incidents resulting in disruptions of operational processes are of particular concern to the Federal Government. The attacker is a criminal, and reporting an incident allows individuals to look out for suspicious activity and enables them to take steps to protect themselves.

# REPORT TO THE FBI FOR THREAT RESPONSE

Submit an internet crime complaint form to the FBI at [*www.ic3.gov*](http://www.ic3.gov)or contact your local field office at [*www.fbi.gov/contact-us/field*.](http://www.fbi.gov/contact-us/field) The FBI will conduct the investigation.

OR

# REPORT TO CISA FOR ASSET RESPONSE

Submit a computer security incident form to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System at [*www.us-cert.cisa.gov/forms/report*.](http://www.us-cert.cisa.gov/forms/report) CISA can be contacted by phone at 888-282-0870 and by email at *Central@cisa.gov*.

CISA will provide technical assets and assistance to mitigate vulnerabilities and reduce the impact of the incident.

OR

# CONTACT EPA FOR CENTRALIZED RESPONSE

Please reach out to the U.S. Environmental Protection Agency (EPA) Water Infrastructure

and Cyber Resilience Division (WICRD) at *WICRD-outreach@epa.gov*. EPA’s WICRD will act as a centralized federal point of contact between the affected parties/stakeholders and all appropriate federal agencies incorporated in the incident response.