Drinking Water and Wastewater Systems

Cybersecurity Incident Response Plan Template

**[Water/Wastewater System Name]**

**Cybersecurity Incident Response Plan**

Version [X]

[**Date**]

This document and associated electronic files may contain sensitive or confidential information. Please maintain the document/electronic files in a manner that will help safeguard the information.

**PLAN INFORMATION**

**APPROVALS**

The Incident Response Lead has reviewed this Cybersecurity Incident Response Plan and acknowledges that responsibility for managing the cybersecurity incident is entrusted to the Incident Response Lead or their delegate.

|  |  |
| --- | --- |
| Incident Response Lead Name and Title | Incident Response Lead Signature |
|  |  |

**REVISION HISTORY**

This Cybersecurity Incident Response Plan has been modified as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modification | Modifier |
| *[2024-01-01]* | *[1.0]* | *[Plan created]* | *[Author]* |
|  |  |  |  |

**PLAN DISTRIBUTION**

This Cybersecurity Incident Response Plan has been distributed to the following people:

|  |  |  |
| --- | --- | --- |
| Recipient/Title | Distributed By | Date |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Table of Contents**

[1.0 PURPOSE 1](#_Toc195530075)

[2.0 INCIDENT HANDLING PROCESS 1](#_Toc195530076)

[2.1. Identification 1](#_Toc195530077)

[2.2. Containment 3](#_Toc195530078)

[2.3. Eradication 3](#_Toc195530079)

[2.4. Recovery 4](#_Toc195530080)

[2.5. Lessons Learned 5](#_Toc195530081)

[3.0 CONTACT LIST 6](#_Toc195530082)

[4.0 INCIDENT DATA COLLECTION 8](#_Toc195530083)

[5.0 APPLICABLE REGULATIONS AND REQUIREMENTS 11](#_Toc195530084)

[6.0 TESTING AND UPDATES 11](#_Toc195530085)

[APPENDIX A – OT/IT System Overview 12](#_Toc195530086)

# PURPOSE

This Cybersecurity Incident Response Plan (CIRP) describes the overall approach for responding to cybersecurity incidents at [Water/Wastewater System Name]. It identifies the structure, roles and responsibilities, incident types, and the approach to preparing for, identifying, containing and eradicating threats, recovery, and conducting post-incident lessons learned debriefings.

This CIRP applies to all networks, systems, and data, as well as the employees and contractors that access the networks, systems, and data. Staff who may be called upon to lead or participate as part of the Incident Response Team must familiarize themselves with this plan and be prepared to collaborate.

This CIRP references and incorporates the following plans, policies, and procedures.

*[Update the table below and list the existing plans, policies, procedures, and other documents that your water system will reference during a cybersecurity incident.]*

| Plan/Policy/Procedure/Document Name | Version Number | Last Date Updated |
| --- | --- | --- |
| *[Emergency Response Plan]* | *[Version 1.1]* | *[April 15, 2025]* |
|  |  |  |
|  |  |  |

# INCIDENT HANDLING PROCESS

During and after an incident, the Incident Response Lead/Incident Response Team will follow the Identification, Containment, Eradication, Recover, and Lessons Learned process:

## Identification

*[Update the table below and insert the specific actions that your utility will follow to* ***identify*** *and determine that a cyber incident is taking place.]*

| Action | Responsible Staff Member or Team |
| --- | --- |
| Notify Incident Response Lead, Incident Response Team, and/or OT/IT staff as applicable when a deviation from normal operations is detected. | All |
| Identify and document key information about the incident (see incident report form Section 4.0), including any suspicious calls, emails, or messages before or during the incident. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor |
| Identify and document damage to utility systems. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor |
| Identify and document steps taken in response to the incident (including dates and times). | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor |
| Review system and network logs. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor |
| Use virus and malware scans to identify affected equipment, systems, accounts, and networks. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor |
| If possible, identify any malware used in the incident. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor/DHS CISA |
| If possible, identify any remote servers to which data may have been sent during the incident. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor/DHS CISA |
| If possible, identify the origin of the incident. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor/DHS CISA |
| Report the cyber incident to law enforcement and regulatory agencies (e.g., local and state government authorities, FBI, DHS CISA, EPA). See the contact list in Section 3.0. | Incident Response Lead |
| Notify any external entities (e.g., contractors, vendors, other local departments) that may have remote connections to the affected network(s). | Incident Response Lead |
| Notify utility personnel of the incident. | Incident Response Lead/Incident Response Team |
| Restore mission critical processes (e.g., switch to manual operation), and notify the public (as needed/required). | Incident Response Lead/Incident Response Team |

## Containment

*[Update the table below and insert the specific actions that your utility will follow to* ***contain*** *a cyber incident.]*

| Action | Responsible Staff Member or Team |
| --- | --- |
| Isolate the infected computer(s) or system(s) by disconnecting from the network (unplug connecting cables and turn off Wi-Fi) but leave power on. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor |
| Use contingency measures to safeguard critical operations, such as continuous monitoring tools and fail-safe mechanisms, for OT systems that cannot be isolated due to operational dependencies. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor |
| Determine if there is evidence that the malware or threat actor has spread across the network.  Note: this includes any physical access control systems, HVAC systems, etc. that may be connected to the network. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor |
| Take a “forensic image” of the affected OT/IT systems to preserve evidence, if possible. | Incident Response Lead/Incident Response Team/OT&IT Staff/Contractor/Law Enforcement |

## Eradication

*[Update the table below and insert the specific actions that your utility will follow to* ***eradicate*** *a cyber threat.]*

| Action | Responsible Staff Member or Team |
| --- | --- |
| Scan affected systems for malware using anti-malware software, or Next-Generation Antivirus (NGAV), if available. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Remove any malware, corrupted files and other changes made to OT/IT systems by the incident. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Restore systems back to previous configuration settings to eradicate unwanted changes. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Disable breached user accounts. | Incident Response Lead/Incident Response Team/Contractor |
| Install patches/updates. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Disable unused services. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Perform other mitigation actions to harden against known vulnerabilities that may have been exploited. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Restore compromised files from a clean system back-up. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Block communication to any identified domains or IP addresses that were used by the threat actors. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |

## Recovery

*[Update the table below and insert the specific actions that your utility will follow to* ***recover*** *from a cyber incident.]*

| Action | Responsible Staff Member or Team |
| --- | --- |
| Restore OT/IT systems as required (e.g., re-image hard drives, reload software). | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Change account passwords (both administrators and users). | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Identify how the attacker(s) gained access to your systems/network. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor/Law Enforcement |
| Increase network perimeter security accordingly. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Review segmentation and boundary rules for maintaining network security and isolating critical systems. | Incident Response Lead/Incident Response Team/ OT&IT Staff/Contractor |
| Test and verify that impacted systems are clean and fully functional. | OT&IT Staff/Contractor |
| Return affected systems to an operationally ready state. | OT&IT Staff/Contractor |
| Notify affected employees and customers if any PII was compromised. | OT&IT Staff/Contractor |
| Notify the state regulatory agency if required by state privacy laws (See Section 5.0). | OT&IT Staff/Contractor |

## Lessons Learned

*[Update the table below and insert the specific actions that your utility will follow to capture and document* ***lessons learned*** *following a cyber incident. The overall goal is to learn from incidents and improve response performance while providing reference materials in the event of a similar future incident.]*

| Action | Responsible Staff Member or Team |
| --- | --- |
| Hold a debrief meeting lead by the Incident Response Lead involving members of the Incident Response Team and other key stakeholders that were involved in the incident response efforts, no more than two weeks after the incident. | Incident Response Lead |
| Develop a lessons learned document and/or an after action report (AAR) to document your utility response activities, successes, and areas for improvement. | Incident Response Lead/Incident Response Team |
| Update this CIRP based on the lessons learned document and or AAR. | Incident Response Lead/Incident Response Team |

# CONTACT LIST

The following table shows cybersecurity response and recovery priority points of contact and their contact information.

*[Update the table below with your utility’s priority contacts for a cyber incident].*

| **Responsible Staff Member or Team** | **Contact Information** | **When to Notify** |
| --- | --- | --- |
| Incident Response Lead | *[Name, Phone and Email Address]* | The Incident Response Team and any utility staff should contact the Incident Response Lead when they believe that your utility may be the victim of a cyber incident. |
| *Incident Response Team members (as applicable)* | *[Name(s), Phone and Email Addresses]* | The OT or IT staff should contact the Incident Response Team when they suspect that your utility may be a victim of a cyber incident. |
| *OT staff/contractor (as applicable)* | *[Name(s), Phone and Email Addresses]* | Users should contact the OT staff/contractor if there is a suspected incident on an OT device or network. |
| *IT staff/contractor (as applicable)* | *[Name(s), Phone and Email Addresses]* | Users should contact the IT staff/contractor if there is a suspected incident on an IT device or network. |
| *Public Affairs/Public Relations* | *[Name(s), Phone and Email Addresses]* | Notify your utility’s or the state/local/tribal/territorial public affairs/public relations specialist to assist with reporting the details of the incident to employees and the general public. Additionally, they can assist you with any interactions with the news media. |
| *Local law enforcement* | *[Name(s), Phone and Email Addresses]* | Local law enforcement officials should be notified by the Incident Response Lead when they suspect that your utility is a victim of a cyber incident. |
| *Local Emergency Management Agency* | *[Name, Phone and Email Address]* | The local emergency management agency should be notified by the Incident Response Lead when they suspect that your utility is a victim of a cyber incident. |
| *State Primacy Agency* | *[Name, Phone and Email Address]* | The state regulatory agency should be notified by the Incident Response Lead when they suspect that your utility is a victim of a cyber incident that may impact public health or other parameters established by the primacy agency. |
| *State cybersecurity agency (as applicable)* | *[Name, Phone and Email Address]* | The state cybersecurity agency should be notified by the Incident Response Lead when they have confirmed that your organization is a victim of a cyber incident. |
| FBI | <http://www.ic3.gov/> | The FBI should be notified by the Incident Response Lead when they have confirmed that your utility is a victim of a cyber incident. |
| Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) | <https://www.cisa.gov/report>  888-282-0870 and [report@cisa.gov](mailto:report@cisa.gov) | DHS CISA should be notified by the Incident Response Lead when they have confirmed that your utility is a victim of a cyber incident. |
| U.S. EPA | [WICRD-outreach@epa.gov](mailto:WICRD-outreach@epa.gov) | U.S. EPA should be notified if your utility requires any assistance preparing, responding, reporting, and/or recovering from a cyber incident. |
| Multi-State Information Sharing and Analysis Center (MS-ISAC) Security Operations Center (SOC) | 866-787-4722 or [soc@cisecurity.org](mailto:soc@cisecurity.org) | Utilities should consider contacting the MS-ISAC. The MS-ISAC operates a SOC, which is a 24x7x365 joint security operations and analysis unit that monitors, analyzes, and responds to cyber incidents targeting state, local, tribal, and territorial entities. |
| WaterISAC | 866-H2o-ISAC (1-866-426-4722) or <https://www.waterisac.org/report-incident> | Utilities should consider reporting incidents and suspicious activity to WaterISAC. Reporting incidents and suspicious activity helps strengthen sector resilience, because it allows WaterISAC to identify threats and vulnerabilities and to warn other members and partners. |
| State Emergency Management Agency/State National Guard | [State emergency management agencies | USAGov](https://www.usa.gov/state-emergency-management#:~:text=Contact%20your%20state's%20emergency%20management%20agency) | In the event of a cyber incident, utilities should consider contacting their state emergency management agency who in certain cases can leverage the State National Guard to provide cyber response and support services. |

# INCIDENT DATA COLLECTION

[Utility Name] will collect critical information about the incident to have the necessary data available to report and share with the local, state, and federal reporting authorities, law enforcement, and any third party or external entities while also facilitating and expediting the process to receive assistance from these entities.

*[Use the form on the next page to collect and document the necessary information that should be collected and shared with appropriate external parties involved in the cybersecurity incident response process. This form should be completed by the Incident Response Lead/Incident Response Team.]*

**CYBERSECURITY (OT/IT) INCIDENT REPORT FORM**

Use this form to document any cybersecurity issues, breaches, hacks, malware, or any other incidents. **Please note**: Some states may have regulations restricting how and what information can be disclosed to non-state entities.

Date of Report: [DATE]

|  |
| --- |
| **CONTACT PERSON** |

Full Name: [NAME] Address: [ADDRESS]

Job Title: [TITLE]

Phone: [PHONE] E-Mail: [E-MAIL]

|  |
| --- |
| **THE INCIDENT** |

Date of Incident: [DATE] Time: [TIME]  AM  PM

Type of Incident:  Malware  Data Breach  Phishing  Other: [OTHER]

How was the incident detected / discovered? [DESCRIBE]

|  |
| --- |
| **NOTIFICATION** |

Were other personnel notified?  Yes  No

If yes, describe: [DESCRIBE]

|  |
| --- |
| **CONTAINMENT** |

Were any containment measures made?  Yes  No

If yes, describe: [DESCRIBE]

Can systems safely fail-over or continue operating? [DESCRIBE]

|  |
| --- |
| **IMPACTED SERVICES** |

Was anything permanently impacted by the incident?  Yes  No

If yes, describe: [DESCRIBE]

Was there an impact to the utility’s Operational Technology (OT) systems?  Yes  No If yes, describe: [DESCRIBE]

Was there an impact to drinking water or wastewater because of the incident?  Yes  No

If yes, describe: [DESCRIBE]

Was there an impact on the utility’s ability to provide drinking water or process wastewater because of the incident?  Yes  No If yes, describe: [DESCRIBE]

What networks and systems are affected by the attack vector, and can the problem spread to other sites and customers? [DESCRIBE]

|  |
| --- |
| **ATTACK VECTOR** |

Do you know how the attack was made?  Yes  No

If yes, describe: [DESCRIBE]

Was this internal or external to the organization? [DESCRIBE]

|  |
| --- |
| **INFORMATION IMPACT** |

Was there any data, records, or information breached?  Yes  No

If yes, describe: [DESCRIBE]

Are there legal or safety issues caused by the attack?  Yes  No

If yes, describe: [DESCRIBE]

|  |
| --- |
| **OTHER** |

Is there any other information you would like to include in this report?  Yes  No

If yes, describe: [DESCRIBE]

# APPLICABLE REGULATIONS AND REQUIREMENTS

The following applicable requirements will be referenced during a cybersecurity incident:

*[Update the table below based on your utility’s location and corresponding local and state cyber regulations or laws].*

| **Requirement/Standard** | **Relevant Law/Policy** |
| --- | --- |
| *[Notification requirements for PII data breach]* | *[Local/State Code]* |
| *[Notification requirements for incident potentially affecting public health]* | *[State regulatory agency regulation and Public Notification Rule]* |
|  |  |

# TESTING AND UPDATES

[Select one: annual, bi-annually, quarterly] testing of the CIRP using tabletop exercises and practical simulations of potential incident scenarios is necessary to ensure the Incident Response Lead/Incident Response Team, utility staff, OT/IT contractors, and any vendors (e.g., third party billing provider) are aware of their obligations during a cyber incident at [Utility Name], unless actual cyber incidents occur which test the full functionality of the CIRP.

* The CIRP will be tested [Select one: annual, bi-annually, quarterly].
* The Incident Response Lead/Incident Response Team will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects of incident response that need improvement.
* The Incident Response Lead will ensure that the CIRP is updated and distributed to Incident Response Team members (as applicable).

# APPENDIX A – OT/IT System Overview

*[If any of the information listed in this appendix is maintained elsewhere (e.g., in other utility documents), please feel free to reference those information sources in the table in Section 1.0 of this plan. There is no need to duplicate this information here.]*

Network Topology

*[Attach a high-level diagram of the application/system data flow and data storage, including all interconnected OT and IT system names and networks (e.g., public vs. private)]*

System Hardware Inventory

*[Please update the table below with all your utility’s OT and IT network assets and devices. Please add or remove any rows or columns as needed. If you have an external system/software that manages your inventory, feel free to insert the link here or replace the table with a graphical list of the hardware inventory.]*

| Asset or Serial # | Item Description | Make and Model | Contractor | Location | Date Purchased or Leased |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

System Software Inventory

*[Please update the table below with all your utility’s OT and IT device software. Please add or remove any rows or columns as needed. If you have an external system/software that manages your inventory, feel free to insert the link here or replace the table with graphical list of the hardware inventory.]*

| Name | Description | Version | Developer | Date installed |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |