**Community Water System**

**Emergency Response Plan Template**

**[CWS Name]**

**Emergency Response Plan**

.

**CWS and ERP Information**

Please fill in the information below as indicated. Text in italics in all the tables in this template represents examples – be sure to delete italicized text as necessary as you fill out the tables in this template.

|  |  |
| --- | --- |
| PWSID | 123456 |
| Street Address | 12 Main Street |
| City, State, Zip Code | Anytown, XX, 98765 |
| Phone number | 555-555-5555 |
| Population Served | 7,500 |
| Prepared by | April Smith |
| Reviewed by | Joe Jones |
| Date completed | MM/DD/YYYY |

**Plan Distribution**

Please fill in the recipient’s name and title, the person who gave them the plan and on what date.

| Recipient/Title | Distributed By | Date |
| --- | --- | --- |
| Joe Jones, ERP Lead | April Smith | DD/MM/YYYY |
| Other |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Change History**

Please describe the changes made to this plan since its original development, who made the changes and on what date the changes were incorporated into this plan.

| Description of Change | Name/Title | Date |
| --- | --- | --- |
| Updated External Response Partner Contact List | Joe Jones, ERP Lead | DD/MM/YYYY |
| Updated Power Loss SOP based on Hurricane Jane | Joe Jones, ERP Lead | DD/MM/YYYY |
| Other |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**TABLE OF CONTENTS**

[UTILITY INFORMATION 1](#_Toc198553285)

[i Utility Overview 1](#_Toc198553286)

[ii Personnel Information 2](#_Toc198553287)

[iii Primary Utility Components 3](#_Toc198553288)

[iv Industry Chemical Handling and Storage Facilities 4](#_Toc198553289)

[v Safety 5](#_Toc198553290)

[vi Response Resources 5](#_Toc198553291)

[vii Key Local Services 6](#_Toc198553292)

[1 RESILIENCE STRATEGIES 7](#_Toc198553293)

[1.1 Emergency Response Roles and Responsibilities 7](#_Toc198553294)

[1.2 Incident Command System (ICS) Roles 8](#_Toc198553295)

[1.3 Communication Contact Lists 9](#_Toc198553296)

[1.4 Media Outreach Contact List 12](#_Toc198553297)

[1.5 Public Notification Templates 12](#_Toc198553298)

[2 EMERGENCY PLANS AND PROCEDURES 13](#_Toc198553299)

[2.1 Core Response Procedures 13](#_Toc198553300)

[2.2 Incident-Specific Response Procedures 16](#_Toc198553301)

[3 MITIGATION ACTIONS 17](#_Toc198553302)

[3.1 Alternative Source Water Options and Interconnected Utilities 17](#_Toc198553303)

[3.2 Cybersecurity Mitigation Actions 17](#_Toc198553304)

[3.3 Other Mitigation Actions 22](#_Toc198553305)

[4 DETECTION STRATEGIES 23](#_Toc198553306)

# UTILITY INFORMATION

During an incident, you need to have system information about your water utility readily available for your personnel, first responders, repair contractors/vendors, the media, and other response partner agencies.

## i Utility Overview

Provide basic information about your utility.

Utility Information

|  |  |
| --- | --- |
| PWSID | 123456 |
| Utility name and address | ABC Water Utility  12 Main Street  Anytown, XX, 98765 |
| Owner | Town of Anytown |
| Directions to utility from major roadway, include lat./long. coordinates | Take Exit 12 on I-555 and head south on County 12. In two miles County 12 becomes Main Street and ABC Water Utility admin offices will then be 500 feet ahead on the right. Lat is 69° 38' 7.50" N and long is -42° 10' 25.29" W. |
| Total population served and total service connections | 7,500 served - 2,500 connections |
| Name, title, phone number of primary contact (e.g., ERP Lead) | Joe Jones, 555-555-5555 |
| Alternate contact | Debby Doe, 555-555-6666 |
| Location of treatment, distribution, collection schematics and operation manuals | Please see attached maps and drawings; operation manuals are stored in Chief Operator’s office. |

Use this checklist to ensure the following additional utility information (as applicable) is included as a part of your ERP.

Map of distribution systems

Pressure boundary map

Process flow diagram

Site plans and “as built” drawings for the following components of your system (as applicable):

* + Pumping and storage facilities
  + Reservoir facilities
  + Water treatment facilities
  + Chemical storage locations
  + Booster pump stations
  + Pressure-regulating valve (PRV) sites

Distribution system diagrams and instrumentation information

Equipment specifications and operation instructions

Emergency power and light generation operation specifications

Supervisory Control and Data Acquisition (SCADA) system operation instructions

Communications systems operation instructions

## ii Personnel Information

Attach your personnel roster here or fill out the table below.

Personnel

| Name and Title | Job Duties and Responsibilities | Contact Information | Emergency Information |
| --- | --- | --- | --- |
| Joe Jones, ERP Lead | Leads incident response and serves as Deputy Operator | 555-555-5555; jjones@anytownwater.org | Backup phone: 555-555-7777 |
| Other |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## iii Primary Utility Components

List all the components necessary to maintain effective operation of your utility. Simply add more rows to the tables below or add tables if you have additional components.

Wells

| Well Name | Depth/Location | Available Yield | Treatment Requirements/Associated Treatment Plant |
| --- | --- | --- | --- |
| #1 | 80 ft below ground surface/end of Water Rd | 200 gpm | pH adjustment and chlorination/treated in well house. |
| Other |  |  |  |
|  |  |  |  |
|  |  |  |  |

Intakes

| Intake Name | Depth/Location | Capacity | Treatment Requirements/Associated Treatment Plant |
| --- | --- | --- | --- |
| Clear River | 30 ft below surface/ center of river at Larry’s Landing | 800 gpm | Coagulation, flocculation, sedimentation, filtration and disinfection/Anytown Water Treatment Plant. |
| Other |  |  |  |
|  |  |  |  |
|  |  |  |  |

Treatment Plants

| Treatment Plant Name | Location | Capacity | Treatment Train |
| --- | --- | --- | --- |
| Anytown Water Treatment Plant | 1 Water Utility Drive | 1.2 MGD | Pre-treatment, primary treatment, post-treatment |
| Other |  |  |  |
|  |  |  |  |
|  |  |  |  |

Storage and Distribution System – Tanks, Primary Mains and Pumping Stations

| Type and Location | Area Served | Comments |
| --- | --- | --- |
| Elevated Tank at 5th and Main | Business Zone 1 | 150,000-gallon capacity |
| Other |  |  |
|  |  |  |
|  |  |  |

Treatment Chemical Storage Facilities

| Storage Facility | Chemical(s) | Comments |
| --- | --- | --- |
| Well House #1 | NaOH and Chlorine | Both in liquid form and there is both an eye wash and shower station in the pump house. |
| Other |  |  |
|  |  |  |
|  |  |  |

Other Key Facilities

| Facility | Function | Comments |
| --- | --- | --- |
| Town Tower | Houses pump for Clear River intake | Fenced and locked, patrolled regularly by town police. |
| Other |  |  |
|  |  |  |
|  |  |  |

## iv Industry Chemical Handling and Storage Facilities

List surrounding chemical production, handling or storage industries that could impact your utility during incidents such as accidental releases, hurricanes, or earthquakes.

Industry Chemical Handling Facilities

| Facility Name | Location | Distance | Chemical and Exposure Pathway |
| --- | --- | --- | --- |
| Shiny Stuff Factory | 54 Grove Street | 0.15 miles to the north of the utility admin building | Facility uses large amounts of highly volatile chemicals. If power failure occurs, evaporation of these chemicals may occur, causing air pollution in areas surrounding the factory. |
| Other |  |  |  |
|  |  |  |  |

Industry Chemical Storage Tanks

| Facility Name | Location | Distance | Chemical and Exposure Pathway |
| --- | --- | --- | --- |
| Metro Gas Station | 25 Main Street | 0.2 miles west of the utility wellfield | 20,000-gallon underground storage tank (UST) holding gasoline. Earthquakes may cause disruption or leaking of the tank. |
| Other |  |  |  |
|  |  |  |  |

## v Safety

List safety materials and important safety information to help protect utility personnel during an incident. You may also reference your utility Health and Safety Plan, if available.

Safety Materials

| Material Type | Location |
| --- | --- |
| Toxic material detection and testing supplies |  |
| Emergency food and water supplies |  |
| Emergency PPE (note what PPE are present at each location) |  |
| Other equipment (note what is present at each location) |  |
|  |  |
|  |  |

Safety Information

| Topic | Description |
| --- | --- |
| Wind speed | Utility personnel may not work outdoors when the sustained wind speed is 45 mph or greater. |
| Other |  |
|  |  |
|  |  |

## vi Response Resources

Provide an inventory of available resources (e.g., equipment, supplies) either maintained on site or readily available off site (e.g., neighboring water system) in the table below, or insert an existing inventory sheet.

***Resources***

| Resource Kind | Resource Type | Quantity | Location |
| --- | --- | --- | --- |
| Generator | Portable, 10000 watts | 1 | Utility warehouse |
| Fuel | Gasoline | 500 gal | Tank behind warehouse |
| Pump |  |  |  |
| Other |  |  |  |
|  |  |  |  |

## vii Key Local Services

Note the closest locations of key logistical and medical services that you or mutual aid and assistance providers may need during an incident. Include a map if available.

Essential Services

| Facility | Location/Description |
| --- | --- |
| Hospital | 10 Spaulding Drive/40-bed facility with ER but no trauma center. |
| Gas station |  |
| Pharmacy |  |
| ATM |  |
| Grocery store |  |
| Other |  |
|  |  |

# 1 RESILIENCE STRATEGIES

This section contains strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system.

## 1.1 Emergency Response Roles and Responsibilities

Describe the roles and responsibilities for key utility and external response partner personnel in the tables below. You can add, edit, or delete rows as necessary.

Water Utility and Partner Roles

| Name/Title | Emergency Response Role | Responsibilities |
| --- | --- | --- |
| Wendy Smith/ Superintendent | Emergency Response Lead | Responsible for all incident response activities, including developing strategies and tactics and ordering and releasing resources. |
| John Doe/Operations Chief | Alternate Emergency Response Lead | Perform duties as assigned by ER Lead; assumes duties listed above when ER Lead is not available. |
| Jim Rogers/County Public Affairs Officer | Public Information | Responsible for leading the public information effort based on information supplied by either the ER or Alternate ER Lead. |
| Jane Kelly/Chief of Police | Security | Will provide incident security as needed once notified by ER Lead. |
| Other |  |  |
|  |  |  |

External Response Partner Roles

| Name/Title | Organization | Responsibilities During an Incident |
| --- | --- | --- |
| **Local Partners** | | |
| Anita Johnson, EMD Director | County Emergency Management/EOC | Can assist in getting response resources and help notify public of water use advisories. |
|  | 911 |  |
|  | Police |  |
|  | Fire/HazMat |  |
|  | LEPC |  |
|  | Elected officials |  |
|  | Neighboring Wastewater utility |  |
|  | Neighboring Water utility |  |
|  | Power utility |  |
|  | Health department |  |
|  | Contractor/vendor |  |
|  | Industry representative |  |
| David Jones, Town Manager | Mutual aid | Can help find response resources at other water utilities in the Tri-County Mutual Aid Agreement. |
|  | Other |  |
|  |  |  |
| **State Partners** | | |
| Greg McGregor, Regional Engineer | Primacy Agency | Can provide technical assistance during a response. |
|  | Health department |  |
|  | Police |  |
| Bob Smith, WARN Chair | WARN | Can help find response resources at other WARN water utilities throughout the state. |
|  | Laboratories |  |
|  | Other |  |
|  |  |  |
| **Federal Partners** | | |
|  | EPA regional office |  |
| Lisa Olson, Special Agent | FBI field office | Can assist with a cyber incident. |
|  | CDC |  |
|  | Other |  |
|  |  |  |

## 1.2 Incident Command System (ICS) Roles

ICS is used to organize both near-term and long-term field-level operations for a broad spectrum of emergencies, from small to complex incidents, both natural and manmade. An ICS Incident Organization Chart (ICS Form 207), available at FEMA’s [ICS Resource Center](https://training.fema.gov/emiweb/is/icsresource/index.htm), may be completed for your utility and inserted here or attached to your ERP.

## 1.3 Communication Contact Lists

Communication during an incident is critical to relay information to employees, response partners and critical customers about potential risks to health, infrastructure, and the environment.

List all utility emergency response team members, their response role, title and contact information below.

Internal Contact List

| Name | Role/Title | Phone | Alternate Phone | Email |
| --- | --- | --- | --- | --- |
| Joe Jones, ERP Lead | Leads incident response and serves as Deputy Operator | 555-555-5555 | 555-555-7777 | jjones@anytownwater.org |
| Other |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

List all external response partners, their response role or position as well as contact information below.

External Response Partner Contact List

| Organization or Department | Point Person Name or Position | Phone | Alternate Phone | Email or Website |
| --- | --- | --- | --- | --- |
| Local Partners | | | | |
| *County Emergency Management/EOC* | Anita Johnson, EMD Director | 555-555-9999 | 555-555-2222 | ajohnson@county.org |
| *911* |  |  |  |  |
| *Police* |  |  |  |  |
| *Fire/HazMat* |  |  |  |  |
| *LEPC* |  |  |  |  |
| *Elected officials* |  |  |  |  |
| *Wastewater utility* |  |  |  |  |
| *Water utility* |  |  |  |  |
| *Power utility* |  |  |  |  |
| *Health department* |  |  |  |  |
| *Contractor/vendor* |  |  |  |  |
| *Industry rep.* |  |  |  |  |
| *Mutual aid* |  |  |  |  |
| *Other* |  |  |  |  |
|  |  |  |  |  |
| State Partners | | | | |
| *Primacy agency* | Greg McGregor, Regional Engineer | 777-777-1234 | 777-777-4321 | gmcgregor@state.us |
| *Health department* |  |  |  |  |
| *Police* |  |  |  |  |
| *WARN* |  |  |  |  |
| *Laboratories* |  |  |  |  |
| *Other* |  |  |  |  |
|  |  |  |  |  |
| Federal Partners | | | | |
| *EPA regional office* |  |  |  |  |
| *FBI field office* | Lisa Olson, Special Agent | 123-456-7890 | 123-456-9988 | lolson@fbi.gov |
| CDC |  |  |  |  |
| Other |  |  |  |  |
|  |  |  |  |  |

List critical customers below who should be given priority notification due to their reliance on the water supply either for medical reasons, based on usage, public health mission or because they may serve customers considered to be sensitive sub-populations.

Critical Customer Contact List

| Organization or Department | Point Person Name or Position | Contact Instructions | Phone | Alternate Phone | Email or Website |
| --- | --- | --- | --- | --- | --- |
| Wholesale customer | Don Dawkins, Superintendent, Village Water | Use alternate phone for after hours, weekends, and holidays | 555-555-4444 | 555-555-1111 | ddawkins@vwater.com |
| Senior living center |  |  |  |  |  |
| Nursing home |  |  |  |  |  |
| Hospital |  |  |  |  |  |
| Dialysis clinic |  |  |  |  |  |
| Hotel |  |  |  |  |  |
| Transportation center |  |  |  |  |  |
| School |  |  |  |  |  |
| University |  |  |  |  |  |
| Daycare center |  |  |  |  |  |
| Factory |  |  |  |  |  |
| Government building |  |  |  |  |  |
| Large water user |  |  |  |  |  |
| Other |  |  |  |  |  |
|  |  |  |  |  |  |

Inventory your utility’s communication equipment below.

Communication Equipment Inventory

| Type | Assigned to | Location | Number/Frequency/Channel |
| --- | --- | --- | --- |
| Digital handheld radio | Joe Jones | Operations office charger stand | 800-900 MHz/2 for water department |
| Other |  |  |  |
|  |  |  |  |

## 1.4 Media Outreach Contact List

List contact information for all media outlets that your utility may coordinate with during notification efforts. Additionally, include existing risk communication procedures, such as composing and delivering messages (e.g. message mapping), or reference an existing Risk Communication Plan.

Media Contact List

| Organization or Department | Point Person Name & Position | Phone | Alternate phone | Email or Website |
| --- | --- | --- | --- | --- |
| Utility social media coordinator | Karen Kim, Communications Director | 555-555-3333 | 555-555-2244 | kkim@anytownwater.org |
| Newspaper - Local |  |  |  |  |
| Newspaper – Regional/State |  |  |  |  |
| Radio station |  |  |  |  |
| TV station |  |  |  |  |
| Advertising agency |  |  |  |  |
| Other |  |  |  |  |
|  |  |  |  |  |

## 1.5 Public Notification Templates

Insert your templates for public notifications here, or reference where they may be found. Ensure that your templates are consistent with the regulatory requirements for public notification contained in the Public Notification Rule (see 40 CFR 141, Subpart Q) and all relevant state regulations.

# 2 EMERGENCY PLANS AND PROCEDURES

This section contains plans and procedures that can be implemented in the event of a malevolent act or natural hazard that threatens your utility’s ability to deliver safe drinking water.

## 2.1 Core Response Procedures

Core procedures are the “building blocks” for incident specific response procedures, as they are typically implemented across a broad variety of incidents (e.g., hurricane, earthquake, flood). List all your core procedures here.

List your access resources and procedures below.

Access

| Item | Description |
| --- | --- |
| Debris clearing | List or reference here any supplies or equipment your utility owns to help with debris clearing; this includes safety items/personal protective equipment, chainsaws, and debris/earth moving equipment. If you do not have it, list where you will get it from. |
| Alternate routes | List or reference here alternate routes (e.g., if there is a bridge that connects your community, what are your travel options if the bridge becomes impassable?). If the alternate routes are too long, consider staging similar critical equipment and resources in different areas of your community. |
| Identification badges | Provide personnel with an official utility ID for access through police barricades or hazmat contaminated zones. If your jurisdiction has an identification program for first responders, be sure to participate. |
| Other |  |
|  |  |
|  |  |

List your physical security measures below.

Physical Security

| Item | Description |
| --- | --- |
| Access control procedures | List or reference your facility access control procedures here, such as key cards are required to access all buildings. Also, list any lockdown procedures as appropriate as well as the process for establishing a security perimeter following a major incident. |
| Restricted areas | List or reference any restricted areas of your facilities here, such as chemical rooms and electrical closets. Also list who may access those areas. |
| Evidence protection measures | Describe or reference your procedures for working with law enforcement if an incident is declared a crime scene. |
| Security culture | Increase organizational attentiveness to security to help reduce vulnerability and enhance preparedness. For example, a “See Something, Say Something” campaign for your utility. List measures your utility implements here. |
| Other |  |
|  |  |
|  |  |

List your cybersecurity procedures below.

Cybersecurity

| Item | Description |
| --- | --- |
| Disconnect procedure | If possible, disconnect compromised computers from the network to isolate breached components and prevent further damage, such as the spreading of malware. |
| Notification | List who should be called in the event of a cyber incident, such as your utility information technology (IT) and/or operational technology (OT) supervisor or your contracted IT/OT service provider. Also list any external entities that may have remote connections to your network.  Include any state resources that may be available such as regulatory agencies, State Police, National Guard Cyber Division or mutual aid programs, as well as the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) (888-282-0870 or Central@cisa.gov). |
| Assess procedure | Assess any damage to utility systems and equipment, along with disruptions to utility operations. |
| Implement response actions | Implement actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary) and provide public notification (if required). Refer to [EPA’s Cybersecurity Incident Action Checklist](https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf) for specific response actions. |
| Documentation | Include forms to 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). |
| Other |  |
|  |  |
|  |  |

List your power loss resources and procedures below.

Power Loss

| Item | Description |
| --- | --- |
| Backup power systems | List or reference your auxiliary power sources (fixed and portable) if you have not already done so elsewhere in your ERP. Provide a summary of critical facility power requirements, generator siting requirements, and the location and capacity of any existing on-site generators at all critical infrastructure components. |
| Power utility | Coordinate with your power utility for expected restoration priorities and timing. Power utility contact information should be listed in Section 3.2 above. |
| Fuel plan | Provide an inventory of on-site fuel supplies and list or reference your procedures to obtain additional fuel from vendors for your backup generators during an incident. |
| Maintenance plan | Maintaining generators during extended outages is critical. List your maintenance procedures for each generator, who is responsible for implementation and include lists of on-hand items such as spare parts and filters. |
| Other |  |
|  |  |
|  |  |

List your alternate drinking water resources below.\*

Emergency Alternate Drinking Water Supplies

| Item | Description |
| --- | --- |
| Bottled water | Provider name: Walmart  Phone: 555-555-9876 (all hours number)  Contract No. (if applicable): 55-42589OX  Available supply: 25 pallets  Distribution point (notify public of location): Regional High School parking lot |
| Bulk water (check with your state first for licensed water haulers) | Provider name:  Phone:  Contract No. (if applicable):  Available supply:  Distribution point (notify public of location): |
| Other |  |
|  |  |
|  |  |

*\*Interconnections are listed and described in Section 3.1*

List your sampling procedures and laboratory capabilities below.

Sampling and Analysis

| Item | Description |
| --- | --- |
| Sampling procedures | Identify proper sampling procedures for different types of contaminants and attach those procedures to your ERP or reference where they can be found. Determine the quantity of required samples. |
| Pre-identified sampling locations | While some sampling sites will be dictated by the emergency, you can pre-plan your ideal sampling locations such as tanks and reservoirs or entry and exit points from pressure zones. |
| Sampling containers and preservatives | Obtain and inventory all sample containers and preservatives and list or reference them here. |
| Sample collection | Confirm who will be responsible for sample collection during an emergency and who can take over if that person is not available. List those names here. |
| Sample transportation | Confirm who will be responsible for transportation during an emergency and who can take over if that person is not available. List those names here. |
| Laboratory capabilities | Confirm what contaminants can be analyzed and your lab’s surge sampling capacity. It may be helpful to have several backup laboratories in case your utility’s lab or preferred contract lab are overwhelmed with high sample volume. Identify contract laboratories in the following table. |
| Interpreting results | Work with the appropriate lab, utility and regulatory agency personnel to interpret sample results. List those names here. |
| Other |  |
|  |  |
|  |  |

List your contract laboratories here. Include state and federal laboratories as appropriate.

Local Contract/State/Federal Laboratory Contact List

| Name | Address | Analytes/Methods | Phone | Email or Website |
| --- | --- | --- | --- | --- |
| XYZ Lab | 364 County 12, Village, XX, 12345 | Metals, VOCs and SVOCs | 555-555-1177 | analyst@xyzlab.com |
| Other |  |  |  |  |
|  |  |  |  |  |

List family and staff wellbeing measures below.

Family and Utility Personnel Well Being

| Item | Description |
| --- | --- |
| Family disaster plan | Implement your family plan to ensure their well-being during an incident. |
| Assembly area | List all the assembly areas and evacuation procedures for personnel. |
| Supplies | List the supplies necessary to maintain personnel health and well-being during an incident (e.g., food, potable water, cots, first aid kit, sanitary products). |
| Alternate work and shelter locations | Personnel may need to work from home. Or they may need to shelter at a hotel or your utility if conditions do not permit travel home. List conditions for which work at home provisions will be triggered and list sheltering locations and procedures here. |
| Extreme temperatures | List or reference here any supplies or equipment your utility owns to mitigate extreme temperatures such as cold weather items (e.g., sand, salt, ice melt, tire chains, snowshoes) and hot weather items (e.g., pop-up shade canopies, water coolers, broad-brimmed hats). |
| Other |  |
|  |  |

## 2.2 Incident-Specific Response Procedures

Insert applicable Incident-Specific Response Procedures (ISRPs), specialized procedures tailored to an incident type. Incidents may include, but are not limited to, the following:

| * Drought * Earthquake * Extreme Cold and Winter Storms * Extreme Heat * Flooding * Harmful Algal Bloom * Hurricane | * Pandemic * Tornado * Tsunami * Volcanic Activity * Wildfire * Source Water Contamination * Distribution System Contamination |
| --- | --- |

EPA’s website provides a number of [incident action checklists](https://www.epa.gov/waterutilityresponse/incident-action-checklists-water-utilities) (IACs) that you can use to help develop your own ISRPs. EPA also published the [Prepared for Contamination in Your Distribution System?](https://www.epa.gov/sites/production/files/2018-12/documents/planning_for_contamination_primer_2.pdf) guidance that can help you develop a distribution system contamination ISRP.

# 3 MITIGATION ACTIONS

This section contains actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to your community and individuals, including the development of alternative source water options, relocation of water intakes, cybersecurity measures, and construction of flood protection barriers.

## 3.1 Alternative Source Water Options and Interconnected Utilities

List information on alternative source water options to mitigate impacts during incidents.

Alternative Source Water Options

| Type | Location | Comments |
| --- | --- | --- |
| *Well* | *Municipal golf course* | *This irrigation well can be used to supply water under emergency approval from state. Chlorination is needed and the well can produce up to 300 gpm.* |
| Other |  |  |
|  |  |  |

List information on interconnected utilities to mitigate impacts during incidents.

Interconnected Utilities

| Utility Name | Location | Contact Information | Comments |
| --- | --- | --- | --- |
| *ABC Water* | *Nearby Town* | *Jane Doe: 555-555-1234* | *Plans on file in engineering to construct emergency connection if needed.* |
| Other |  |  |  |
|  |  |  |  |

## 3.2 Cybersecurity Mitigation Actions

Identify the priority cybersecurity mitigation actions that your utility intends to implement to better protect against a cyberattack. To accomplish this, you can use the Checklist of Priority Cybersecurity Practices for Water Systems included on the next page. Be sure to fill in your utility’s intended mitigation actions in the “Notes” column of the checklist for any “no” answers. Just note that you may have already used this checklist if you conducted your risk and resilience assessment (RRA) using the following EPA guidance: Small System RRA Checklist; Vulnerability Self-Assessment Tool (VSAT); Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems; Water Cybersecurity Assessment Tool and Risk Mitigation Template.

|  | **Question**  Does the CWS… | **Answer**  Mark the appropriate check box (“Yes”, “No”, “In progress”, “Not applicable”)  to answer each cybersecurity assessment question. |
| --- | --- | --- |
|  | **Reduce Exposure to Public-Facing Internet** |  |
| 1. | Ensure assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminates connections between OT assets and the Internet? | Yes  No  In progress  Not applicable  *If “No”, EPA recommends that the CWS take the following action: Eliminate unnecessary exposed ports and services on public-facing assets with regular review and eliminate OT asset connections to the public Internet unless explicitly required for operations.* |
|  | **Conduct Regular Cybersecurity Assessments** |  |
| 2. | Conduct regular cybersecurity assessments? | Yes  No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Conduct a cybersecurity assessment on a regular basis to understand the existing vulnerabilities within OT and IT systems. Assessments enable you to identify, assess, and prioritize mitigating vulnerabilities in both OT and IT networks.* |
| 3. | Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the CWS? | ☐Yes  ☐No  ☐In progress  ☐Not applicable    *If “No”, EPA recommends that the CWS take the following action: Identify one role/position/title responsible for cybersecurity within the CWS. Whoever fills this role/position/title is then in charge of all CWS cybersecurity activities.* |
|  | **Change Default Passwords Immediately** |  |
| 4. | Change default passwords and require a minimum length for passwords? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Change all default manufacturer or vendor passwords before equipment or software is put into service and implement a minimum length requirement for passwords through a policy and/or administrative controls set in the system.* |
| 5. | Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access CWS/OT/IT networks? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Deploy MFA as widely as possible for both operational technology (OT) and information technology (IT) networks. At a minimum, MFA should be used for remote access to the OT network.* |
|  | **Conduct Inventory of OT/IT Assets** |  |
| 6. | Maintain an updated inventory of all OT and IT network assets? | Yes  No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Regularly review (no less than monthly) and maintain a list of all Operational Technology (OT) and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment. Create an inventory of software and hardware assets to help understand what you need to protect. Focus initial efforts on internet-connected devices and devices where manual operations are not possible. Use monitoring to identify the devices communicating on your network.* |
| 7. | Maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets? | Yes  No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Maintain accurate documentation of the original and current configuration of OT and IT assets, including software and firmware version* |
|  | **Develop & Exercise Cybersecurity Incident Response & Recovery Plans** |  |
| 8. | Have a written cybersecurity incident response (IR) plan for critical threat scenarios (e.g., disabled or manipulated process control systems, the loss or theft of operational or financial data, exposure of sensitive information), which is regularly reviewed, practiced, and updated? | ☐Yes  Date of last IR plan review/update: *[insert month/day/year]*  ☐No  ☐In progress  ☐Not applicable    *If “No”, EPA recommends that the CWS take the following action: Develop, practice, review, and update an IR plan for cybersecurity incidents that could impact CWS operations. Participate in discussion-based (ex. TTX) and operations-based exercises (ex. Drill) to improve responses to potential cyber incidents.* |
| 9. | Have a written procedure for reporting cybersecurity incidents, including how and to whom? (e.g., phone call, internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, Water Information Sharing & Analysis Center - WaterISAC, cyber insurance provider)? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Document the procedure for reporting cybersecurity incidents to better aid law enforcement, receive assistance with response and recovery, and to promote water sector awareness of cybersecurity threats. (See OW factsheet)* |
|  | **Backup OT/IT Systems** |  |
| 10. | Backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule:*  *3) Keep three copies: one primary and two backups*  *2) Keep the backups on two different media type*  *1) Store one copy offsite.* |
|  | **Reduce Exposure to Vulnerabilities** |  |
| 11. | Patch or otherwise mitigate known vulnerabilities within the recommended time frame? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Identify and patch vulnerabilities in a risk-informed manner (e.g., critical assets first) as quickly as possible* |
| 12. | Require unique and separate credentials for users to access OT and IT networks and separate user and privileged (e.g., System Administrator) accounts? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Require a single user to have two different usernames and passwords; one account to access the IT network, and the other account to access the OT network to reduce the risk of an attacker being able to move between both networks using a single login and restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to ensure accurate information for the individuals who have these privileges.* |
| 13. | Prohibit the connection of unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: When feasible, remove, disable, or otherwise secure physical ports (e.g., USB ports on a laptop) to prevent unauthorized assets from connecting.* |
| 14. | Immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Terminate access immediately to accounts or networks upon a change in an individual’s status making access unnecessary (i.e., retirement, change in position, etc.).* |
|  | **Conduct Cybersecurity Awareness Training** |  |
| 15. | Provide/conduct annual cybersecurity awareness training for all CWS personnel that covers basic cybersecurity concepts? | ☐Yes  ☐No  ☐In progress  ☐Not applicable  *If “No”, EPA recommends that the CWS take the following action: Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.* |

## 3.3 Other Mitigation Actions

List any mitigation procedures or projects implemented at your utility, such as raising facilities and controls or constructing berms to protect against flood damage.

Mitigation Actions

| Type | Location | Comments |
| --- | --- | --- |
| Water intake relocation | Intake 1 | This intake was moved further offshore and deeper to better avoid surface spills and low river levels during drought |
| Watertight doors | Treatment plant | These doors were installed to help ensure floodwaters cannot enter the treatment building and damage control systems |
| Earthquake | All facilities | Anchored equipment (e.g., computers, bookshelves) as well as laboratory equipment and chemical and fuel tanks |
| Cybersecurity | Internet-facing OT equipment | Enrolled in CISA Free Vulnerability Scanning service |
| Other |  |  |
|  |  |  |

# 4 DETECTION STRATEGIES

This section contains strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

List the detection strategies and methods your utility uses to aid in the detection of malevolent acts or natural hazards. Also list the corresponding procedure to be used if the threat is detected.

Detection Strategies

| Threat | Detection Method | Procedure |
| --- | --- | --- |
| Unauthorized entry | Alarm from intrusion detection system | Call 911 |
| Source water contamination | National Response Center notifications  Notification from 911 for releases resulting from transportation accidents | Source Water Contamination Incident Response Plan |
| Distribution system contamination | Customer complaint surveillance  Public health surveillance | Distribution System Contamination Response Procedure |
| Cyber intrusion | Automated IT and operational technology (OT) system intrusion detection monitoring  Notification from utility staff | Cyber Incident Action Checklist |
| Hazardous chemical release | Chlorine gas in air monitors | Call fire department |
| Hurricane | Weather Service alerts | Hurricane Incident Action Checklist |
| Flood | Notification from Army Corp | Flood Incident Action Checklist |
| Power outage | Notification from energy provider  Alarm from line power sensor | Generator Start-up Checklist |
| Other |  |  |
|  |  |  |