Security Vulnerability & Emergency Response Plan Self-Assessment for Small Wastewater Systems



Produced by Minnesota Rural Wastewater Association in conjunction with National Rural Wastewater Association

A Note about Security for this Document

This document contains sensitive information about the security of your wastewater system. Therefore, it should be treated as **Confidential Information** and should be stored in a secure place at your wastewater system. A duplicate copy should also be stored in a secure off-site location.

Security Vulnerability & Emergency Response Plan Self-Assessment Guide for Small Wastewater Systems

Introduction

Wastewater systems are critical to every community. Protection of public wastewater systems should be a high priority for local officials and wastewater system owners and operators to ensure proper sanitation of their community to prevent disease outbreaks which is essential for the protection of public health. Adequate security measures will help prevent loss of service through terrorist acts, vandalism, or pranks. If your system is prepared, such actions may even be prevented. The appropriate level of security is best determined by the wastewater system at the local level.

This Security Vulnerability Self-Assessment Guide is designed to help small wastewater systems determine possible vulnerable components and identify security measures that should be considered. A "vulnerability assessment" (VA) is the identification of weaknesses in wastewater system security, focusing on defined threats that could compromise its ability to provide adequate potable wastewater, and/or wastewater for firefighting. This document is designed particularly for systems that serve population of 3,300 or less. This document is meant to encourage smaller systems to review their system vulnerabilities, but it may not take the place of a comprehensive review by security experts.

The Self-Assessment Guide has a simple design. Answers to assessment questions are "yes" or "no", and there is space to identify needed actions and actions you have taken to improve security. For any "no" answer, refer to the "comment" column and/or contact the Minnesota Rural Water Association.

How to use this Self-Assessment Guide

This document is designed for use by wastewater system personnel. Physical facilities pose a high degree of exposure to any security threat. This self-assessment should be conducted on all components of your system (lift stations, pump stations, treatment plant, pumps, collection system, and other important components of your system).

The Assessment includes a basic emergency contact list for your use. The list included as Attachment 2 will help you identify who you need to contact in the event of an emergency or threat and will help you develop communication and outreach procedures. You may be able to obtain sample Emergency Response Plans from your state wastewater primacy agency or your state rural water association. Development of the emergency response plan should be coordinated with the Local Emergency Planning Committee (LEPC).

Security is everyone's responsibility. This document should help you to increase the awareness of all your employees, governing officials, and customers about security issues. Once you have completed the questions, review the actions you need to take to improve your system's security. The goal of the vulnerability assessment is to develop a system-specific list of priorities intended to reduce risks to threats of attack. Make sure to prioritize your actions based on the most likely threats to your system. Once you have developed your list of priority actions, you have completed your vulnerability assessment.

Before Starting the Assessment

Systems should make an effort to identify critical services and customers, such as hospitals, schools or prisons, as well as critical areas of their wastewater system that if attacked could result in a significant disruption of vital community services, result in a threat to public health, cause an explosion that would cause harm to the public or cause a release of hazardous chemicals that could cause catastrophic results. When prioritizing the potential wastewater system vulnerabilities and consequences factor into the decision process the critical facilities, services, and single points in the system that if debilitated could result in significant disruption of vital community services or health protection. To help identify priorities for your system, the table on page 5 provides a column where you can categorize the assets that you consider critical into one of three categories – high (H), medium (M), or low(L).

When evaluating a system's potential vulnerability, systems should attempt to determine what type of assailants and threats they are trying to protect against. Systems should contact their local law enforcement office to see if they have information indicating the types of threats that may be likely against their facility. Some of the typical threats to your facility may be vandalism, an insider (i.e. disgruntled employee), a terrorist, or a terrorist working with a system employee.

Every wastewater utility will have unique circumstances they will encounter and will have priorities that the community will designate as critical for protection. However, some typical critical facilities that you may think about may include easily accessible or hidden manholes, manholes that provide access to facilities with large quantity (hospitals, schools, etc.) or critically important people (military, government offices, etc), electric suppliers or standby generators, fuel storage or gas supply, chemical storage areas (particularly gaseous chlorine facilities and anhydrous ammonia), and critical lift or pumping stations.

Keep this Document

This is a working document. Its purpose is to start you process of security vulnerability assessment and security enhancements. Security is not an end point, but a goal that can be achieved only through continued efforts to assess and upgrade your system. This is a sensitive document. It should be stored separately in a secure place at your wastewater system. A duplicate copy should also be retained at a secure off-site location. Access to this document should be limited to key wastewater system personal. Others should only have access to information contained in this document on a need to know basis.

SVA & ERP Self-Assessment Identification

The following information should be completed by the individual conducting the self-assessment and/or any additional revisions.

Name	
Title	
Area of Responsibility	
System Name	
NPDES Permit No.	
State Permit No.	
Source of Wastewater	
Discharge Point (Receiving system)	
Designed Flow	
Address	
City	
County	
State	
Zip Code	
Telephone	
Fax	
E-mail	
Date Completed	

Inventory of Small Wastewater System Critical Components

Component	Number & Location (if applicable)	Description
Collection System		
Lift Stations		
Pumps		
Blowers		
Manholes		
Cleanouts		
Pipes		
Treatment Plant (Note: Describe from headworks to point of discharge)		
Pumps		
Primary Treatment (e.g. lagoon, clarifier, wetland)		
Pumps		
Tertiary Treatment (e.g. chemical, filtration)		
Pumps		
Other Treatment		
Disinfection (e.g. gaseous chlorine)		
Discharge		
Bio-solids Handling		
Other Sludge Handling Facilities/Equipment		
Laboratory Chemicals		
Power		
Primary Power		
Auxiliary Power		

Offices		
Buildings		
Computers		
Files/Facility Maps or Diagrams		
Transportation/Work Vehicles		
Communications		
Telephone		
Cell Phone		
Radio		
Computer Control Systems (SCADA)		

Section 1: Notification/Contact Information – Local/State/Federal Notification List

Responders

ORGANIZATION	CONTACT NAME/TITLE	DAY PHONE	NIGHT PHONE	EMAIL
Emergency Event	911	911		*n/a*
Chemical or Environmental Release : MN State Duty Officer	24 hour hotline	800-422-0798		*n/a*
Hazardous Chemical Release: National Response Center	24 hour hotline	800-424-8802		*n/a*
MN State Duty Officer	24 hour hotline	1-800-422-0798		*n/a*
Fire Department/ HAZMAT				
Minnesota Pollution Control Agency				
Minnesota Department of Health				
MnWarn Officer (if member)				
FEMA				
Sherriff Department				
County Emergency Manager				
National Spill Response Center	24 hour hotline	1-800-424-8802		*n/a*
Local / Regional Laboratory				
Wastewater System Operator				
Minnesota Rural Water Association				
Other				

Local Notification List

ORGANIZATION	CONTACT NAME/TITLE	DAY PHONE	NIGHT PHONE	EMAIL
Government Officials				
Emergency Planning Committee				
Hospitals				
Pharmacy				
Nursing Homes				
Schools				
Jail / Prison				
Neighboring Wastewater Systems				
Water Systems Downstream from Effluent Discharge				
Critical Industrial / Commercial Wastewater Users				
Others				

Service/Repair Notification List

ORGANIZATION	CONTACT NAME/TITLE	DAY PHONE	NIGHT PHONE	EMAIL
Electrician				
Electric Utility Company				
Gas Utility Company				
Telephone Utility Company				
Plumber				
Pump Specialist				
Pump Supplier				
Gopher State 1 Call- 811				
Soil Excavator/Backhoe Operator				
Equipment Rental (Power Generators)				
Equipment Rental (Chlorinators)				
Equipment Rental (Portable Fencing)				
Equipment Repairman				
Equipment Repairman (Chlorinator / other)				
Radio / Telemetry Repair Service				
Pipe Supplier				
Chemical or Microbe Supplier				
Septic Pumper				

Media Notification List

ORGANIZATION	CONTACT NAME/TITLE	DAY PHONE	NIGHT PHONE	EMAIL
Designated Wastewater System Spokesperson				
Newspaper – Local				
Newspaper – Regional/State				
Radio				
Other				

General Questions for the Entire Wastewater System The first 13 questions in this vulnerability self-assessment are general questions designed to apply to all components of your wastewater treatment and collection system (collection system, wastewater discharge points, treatment plant, pumps, and offices). These are followed by more specific questions that look at individual system components in greater detail.			
Question	*Answer*	*Comment*	*Risk Assess/Action Taken*
1. Do you have a written emergency response plan (ERP)?	Yes ❑ No ❑	An emergency response plan is vital in case there is an incident that requires immediate response. Your plan should be reviewed at least annually (or more frequently if necessary) to ensure it is up-to-date and addresses security emergencies including ready access to laboratories capable of analyzing wastewater samples. You should coordinate with you local emergency planning committee (LEPC). As a first step in developing your ERP, you should develop your Emergency Contact List (see page 5). You should designate someone to be contacted in case of emergency regardless of the day of the week or time of day. This contact information should be kept up-to-date and made available to all wastewater system personnel and local officials (if applicable). Share this ERP with police, emergency personnel, and your state primacy agency. Posting contact information is a good idea only if authorized personnel are the only ones seeing the information. These signs could pose a security risk if posted for public viewing since it gives people information that could be used against the system. By completing this software in its entirety, this software will generate an emergency response plan for your use. You should check with your State Primacy Agency and State Rural Development Office to ensure you meet any specific requirements that they may need.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
2. Is access to the critical components of the wastewater system (i.e., a part of the physical infrastructure of the system that is essential for collecting and/or treating wastewater) restricted to authorized personnel only?	Yes ❑ No ❑	You should restrict or limit access to the critical components of your wastewater system to authorized personnel only. This is the first step in security enhancement for your wastewater system. Consider the following: • Issue wastewater system photo identification cards for employees, and require them to be displayed within the restricted area at all times. • Post signs restricting entry to authorized personnel and ensure that assigned staff escorts people without proper ID.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:

Question	*Answer*	*Comment*	*Risk Assess/Action Taken*
3. Are all critical facilities fenced, including lift stations and storm sewer outfalls, and are gates locked where appropriate?	Yes ❑ No ❑	Ideally, all facilities should have a security fence around the perimeter. Disabled lift stations can create many problems in the wastewater system. Secure access points and control panels at lift stations with tamper-resistant locks. Structures can be protected from collision with concrete bollards or jersey barriers. Lift stations can be alarmed and should be tested regularly. Storm sewer outfalls may also provide access to the collection system. When appropriate, access to storm-sewer outfalls should be restricted without interrupting the flow. The fence perimeter should be walked periodically to check for breaches and maintenance needs. All gates should be locked with chains and a tamper-proof padlock that at a minimum protects the shank. Other barriers such as concrete "jersey" barriers should be considered to guard certain critical components from accidental or intentional vehicle intrusion.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
4. Are all critical doors, windows, and other points of entry such as process tank hatches, vents and fill pipes kept closed and locked?	Yes ❑ No ❑	Lock all building doors and windows, hatches and vents, fill pipes, gates, and other points of entry to prevent access by unauthorized personnel. Consider securing fill pipes to prevent contamination of chemicals or fuel (especially fuel for back-up generators). Check locks regularly. Dead bolt locks and lock guards provide a high level of security for the cost. A daily check of critical system components enhances security and ensures that an unauthorized entry has not taken place. Doors and hinges to critical facilities should be constructed of heavy-duty reinforced material. Hinges on all outside doors should be located on the inside. To limit access to wastewater systems, all windows should be locked and reinforced with wire mesh or iron bars, and bolted on the inside. Systems should ensure that this type of security meets with the requirements of any fire codes. Alarms can also be installed on windows, doors, and other points of entry.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
5. Are vents and overflow pipes properly protected with screen and/or grates?	Yes ❑ No ❑	Air vents and overflow pipes are direct conduits to the finished wastewater in storage facilities. Secure all vents and overflow pipes with heavy-duty screens and/or grates.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
6. Is there external lighting around the critical components of your wastewater system?	Yes ❑ No ❑	Adequate lighting of the exterior of wastewater systems' critical components is a good deterrent to unauthorized access and may result in the detection or deterrence of trespassers. Motion detectors that turn lights on or trigger alarms also enhance security.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:

Question	*Answer*	*Comment*	*Risk Assess/Action Taken*
7. Are warning signs (tampering, unauthorized access, etc.) posted on all critical components of your wastewater system?	Yes ❑ No ❑	Warn signs are an effective means to deter unauthorized access. "Warning-Tampering with this facility is prohibited" should be posted on all wastewater facilities. "Authorized Personnel Only" "Unauthorized Access Prohibited" and "Employees Only" are examples of other signs that may be useful.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
8. Do you patrol and inspect all buildings, outfalls, lift stations and critical manholes?	Yes ❑ No ❑	Frequent and random patrolling of the wastewater system by utility staff may discourage potential tampering. It may also help identify problems that may have arisen since the previous patrol. All systems are encouraged to initiate personal contact with the local law enforcement to show them the waste wastewater facility. The tour should include the identification of all critical components with an explanation of why they are important. Systems are encouraged to review, with local law enforcement, the NRWA/ASDWA Guide for Security Decisions or similar state document to clarify respective roles and responsibilities in the event of an incident. Also consider asking the local law enforcement to conduct periodic patrols of your wastewater system.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
9. Is the area around all the critical components of your wastewater system free of objects that may be used for breaking and entering?	Yes ❑ No ❑	When assessing the area around your wastewater system's critical components, look for objects that could be used to gain entry (e.g., large rocks, cement blocks, pieces of wood, ladders, valve keys, and other tools).	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
10. Are the entry points to all of your wastewater systems easily seen?	Yes ❑ No ❑	You should clear fence lines of all vegetation. Overhanging or nearby trees may also provide easy access. Avoid landscaping that will permit trespassers to hide or conduct unnoticed suspicious activities. Trim trees and shrubs to enhance the visibility of your wastewater system's critical components. If possible, park vehicles and equipment in places where they do not block the view of your wastewater system's critical components.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
11. Do you have an alarm system that will detect unauthorized entry or attempted entry at all critical components?	Yes ❑ No ❑	Consider installing an alarm system that notifies the proper authorities or your wastewater system's designated contact for emergencies when there has been a breach of security. Inexpensive systems are available. An alarm system should be considered whenever possible for tanks, pump houses, and treatment facilities. You should also have an audible alarm at the site as a deterrent and to notify neighbors of a potential threat.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:

Question	*Answer*	*Comment*	*Risk Assess/Action Taken*
12. Do you have a key control and accountability policy?	Yes ❑ No ❑	Keep a record of locks and associated keys, and to whom the keys have been assigned. This record will facilitate lock replacement and key management (e.g., after employee turnover or loss of keys). Vehicle and building keys should be kept in a lockbox when not in use. You should have all keys stamped (engraved) "DO NOT DUPLICATE"	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
13. Are entry codes and keys limited to wastewater system personnel only?	Yes ❑ No ❑	Suppliers and personnel from co-located organizations (e/g/. organizations using your facility for other purposes or contractors who perform routine maintenance) should be denied access to codes and/or keys. Codes should be changed frequently if possible. Entry into any building should always be under the direct control of wastewater system personnel.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:

Wastewater Collection System

In addition to the above general checklist for your entire wastewater system (question 1-13), you should give special attention to the following issues Related to carious wastewater system components. Ask the public to be vigilant and report suspicious activity

Question	Answer	Comment	Risk Assess/Action Taken
14. Are your critical manholes sealed and secured?	Yes ❑ No ❑	Manholes that provide access to pipes that can be easily traversed, or access to critical customers should be a priority for security. A properly sealed manhole decreases the opportunity for the introduction of contaminants. Critical manholes that provide access to pipes large enough to easily maneuver through will prevent unauthorized personnel from placing explosives or other incendiary devises under building or other highly populated areas. Other points of entry that provide access to critical customers such as schools, industry, hospitals or prisons should also be secured. Continuous service to these critical customers is essential to prevent serious health problems in the community. Tamper resistant bolts or other methods may be used to secure manhole covers to rims. Contact Minnesota Rural Water Association for more information or technical assistance.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
15. Are tributary collection systems from neighboring entities secured?	Yes ❑ No ❑	Coordinate with other jurisdictions whose collection systems connect with your system. Vulnerabilities in neighboring systems can be vulnerabilities in your system.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:

Treatment Plant and Suppliers *Some small systems provide easy access to their wastewater system for suppliers of equipment, chemicals and other materials for the convenience of both parties. This practice should be discontinued.*			
Question	**Answer**	**Comment**	**Risk Assess/Action Taken**
16. Are deliveries of chemicals and other supplies made in the presence of wastewater system personnel?	Yes ❑ No ❑	Establish a policy that an authorized person, designated by the wastewater system, must accompany all deliveries. Verify the credentials of all drivers. This prevents unauthorized personnel from having access to the wastewater system.	Action Needed: Scheduled Completion:
17. Have you discussed with your supplier(s) procedures to ensure the security of their products?	Yes ❑ No ❑	Verify that your supplier take precautions to ensure that their products are not contaminated. Chain of custody procedures for delivery of chemicals should be reviewed. You should inspect chemicals and other supplies at the time of delivery to verify they are sealed and in unopened containers. Match all delivered goods with purchase orders to ensure that they were, in fact, ordered by your wastewater system. You should keep a log or journal of deliveries. It should include the driver's name (taken from the driver's photo I.D.), date, time, material delivered, and the supplier's name.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
18. Are chemicals, particularly those that are potentially hazardous (e.g., Chlorine gas) or flammable, properly stored in a secure area?	Yes ❑ No ❑	All chemicals should be stored in an area designated for their storage only, and the area should be secure and access to the area restricted. Access to chemical storage should be available only to authorized employees. Pay special attention to the storage, handling, and security of chlorine gas because of its potential hazard. Facilities that are required to do risk management plans should review the plans and procedures within that document. You should have tools and equipment on site (such as a fire extinguisher, dry sweep, etc.) to take immediate actions when responding to an emergency.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:

Question	Answer	Comment	Risk Assess/Action Taken
19. Are your facility operations specialists trained in the event of a hazardous chemical release?	Yes ❑ No ❑	If you have a chemical release you are required to dial 911 within 15 minutes of event. A critical piece of pre-planning for any water system emergency is having a complete list of emergency contact notifications readily available to you. Notifications that are required at the onset of an accidental chlorine release fall within that category. Three immediate emergency notification calls must then be made. The first call is made at the local level of government (Emergency 911), which alerts local emergency responders. The second notification call occurs at the state level of government. This is the call you will make to the Minnesota State Duty Officer (800-422-0798). The duty officer will share information you have provided among state agencies having emergency response roles through both phone calls and email transmissions. This is the notification call you will make to the National Response Center (1-800-424-8802). This notification is equally critical because a hazardous chemical release may bear impacts with federal considerations (state and national borders, an immediate need for deployment of federal resources, etc.). If you have had a chlorine leak and are absolutely certain that the amount released is less than the RQ, you are still required to make a single call to the Minnesota State Duty Officer to satisfy Minnesota Statute 115.061 (Duty to Notify). But if you're not sure of the amount released, you need to go ahead and make all three calls. Remember: if in doubt, report. The time frame that would be considered allowable and prompt is 15 minutes. All three notification calls should be completed consecutively, one following another. See Attachment 3 "Accidental Chlorine Release Emergency Notifications" for more details.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
20. Do you have a procedure to control septage dumps?	Yes ❑ No ❑	Septage haulers should only be allowed to dump when regular personnel are on duty. Septage should be sampled and tested for compatibility. Record all septage dumps including: amount, sample results, company/hauler, date, time, and location of dump.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:

Question	Answer	Comment	Risk Assess/Action Taken
21. Do you monitor raw and treated wastewater so that you can detect changes in wastewater quality?	Yes ❑ No ❑	Monitoring of raw and treated wastewater can establish a baseline that may allow you to know if there has been a contamination incident. Some parameters for raw wastewater include pH, DO, COD, BOD, and conductivity. These parameter can help identify and can be indicators of excessive organic loading or toxic compounds that may be introduced to the system. Any changes or abnormal observations of the influents color and odor may also be an indicator of potential contamination. Routine parameters for treated wastewater include biological oxygen demand (BOD), total chlorine residual, heterotrophic plate count (HPC), total and fecal coliform, pH, and specific conductivity. Chlorine demand patterns can help you identify potential problems with your treated wastewater. A sudden change in demand may be a good indicator of contamination in your system.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
22. Are tank ladders, access hatches, and entry points secured?	Yes ❑ No ❑	The use of tamper-proof padlocks at entry points (hatches, vents, and ladder enclosures) will reduce the potential for unauthorized entry.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:`

Personnel *You should add security procedures to your personnel policies.*			
Question	Answer	Comment	Risk Assess/Action Taken
23. When hiring personnel, do you request that local police perform a criminal background check?	Yes ❑ No ❑	It is good practice to have all job candidates fill out an employment application. You should verify professional references. Background checks conducted during the hiring process may prevent potential employee-related security issues. If you use contract personnel, check on the personnel practices of all providers to ensure that their hiring practices are consistent with good security practices.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:`

Question	Answer	Comment	Risk Assess/Action Taken
24. Are your personnel issued photo-identification cards?	Yes ❑ No ❑	For positive identification, all personnel should be issued wastewater system photo-identification cards and be required to display them at all times. Photo identification will also facilitate identification of authorized wastewater system personnel in the event of an emergency.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:`
25. When terminating employment, do you require employees to turn in photo IDs, keys, access codes, and other security-related items?	Yes ❑ No ❑	Former or disgruntled employees have knowledge about the operation of your wastewater system, and could have both the intent and physical capability to harm your system. Requiring employees who will no longer be working at your wastewater system to turn in their IDs, keys, and access codes helps limit these types of security breaches.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:`
26. Do you use uniforms and vehicles with your wastewater system name prominently displayed?	Yes ❑ No ❑	Requiring personnel to wear uniforms, and requiring that all vehicles prominently display the wastewater system name, helps inform the public when wastewater system staff is working on the system. Any observed activity by personnel without uniforms should be regarded as suspicious. The public should be encouraged to report suspicious activity to law enforcement authorities.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:`
27. Have wastewater system personnel been advised to report security vulnerability concerns and to report suspicious activity?	Yes ❑ No ❑	Your personnel should be trained and knowledgeable about security issues at your facility, what to look for, and how to report any suspicious events or activity. Periodic meetings of authorized personnel should be held to discuss security issues.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:`
28. Do your personnel have a checklist to use for threats or suspicious calls or to report suspicious activity?	Yes ❑ No ❑	To properly document suspicious or threatening phone calls or reports of suspicious activity, a simple checklist can be used to record and report all pertinent information. Calls should be reported immediately to appropriate law enforcement officials. Checklists should be available at every telephone. Sample checklists are included on page 22. Also consider installing caller ID on your telephone system to keep a record of incoming calls.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:

Information storage/computers/controls/maps *Security of the system, including computerized controls like a Supervisory Control and Data Acquisition (SCADA) system, goes beyond the physical aspects of operation. It also includes records and critical information that could be used by someone planning to disrupt or contaminate your wastewater system.*			
Question	**Answer**	**Comment**	**Risk Assess/Action Taken**
29. Is computer access "password protected"?	Yes ❑ No ❑	All computer access should be password protected. Passwords should be changed every 90 days and (as needed) following employee turnover. When possible, each individual should have a unique password that they do not share with others.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
30. Is virus protection installed and software upgraded regularly?	Yes ❑ No ❑	Consider contacting a virus protection company and subscribing to a virus update program to protect your records. Update virus protection on a regular basis (daily, weekly, and in some circumstances monthly).	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
31. Do you have a plan to back up your computer?	Yes ❑ No ❑	Backing up computers regularly will help prevent the loss of data in the event that your computer is damaged or breaks. Backup copies of computer data should be made routinely and stored at a secure off-site location.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
32. Do you have Internet firewall software installed on your computer?	Yes ❑ No ❑	If you have Internet access, a firewall protection program should be installed on your side of the computer and reviewed and updated periodically. If you have a SCADA system, consider operating it on systems without internet access. (NOTE: Firewall protection software usually does not protect modem connections. If a modem must be used, use software that will disable the local network connection when the modem is not in use.)	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
33. If you have a SCADA system, has it been evaluated for weaknesses and hardened?	Yes ❑ No ❑	SCADA can be vulnerable to potential intruders. The most direct approach to evaluate vulnerabilities is penetration testing. Penetration testing can detect vulnerability and security breaches that could be used to attack and penetrate the entire SCADA system. Hardening is the process of making the system less vulnerable through equipment upgrades, redundancy of components, etc.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:
34. Can employees' by-pass SCADA and run system manually?	Yes ❑ No ❑	It is important to be able to completely override your SCADA and manually operate your system. Employees should be trained how to by-pass or shut down the SCADA and the procedures to manually operate the system in the event of an emergency.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion:

Question	Answer	Comment	Risk Assess/Action
35. Is there information on the Web that can be used to disrupt your system or contaminate your wastewater?	Yes ❑ No ❑	Posting detailed information about your wastewater system on a website may make the system more vulnerable to attack. Websites should be examined to determine whether they contain critical information that should be removed. You should do a Web search (using a search engine such as Google, Yahoo!, or Lycos) using key words related to your wastewater supply to find any published data on the Web that is easily accessible by someone who may want to damage your wastewater supply.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion
36. Are maps, records, and other information stored in a secure location?	Yes ❑ No ❑	Records, maps, and other information should be stored in a secure location when not in use. Access should be limited to authorized personnel only. You should make back-up copies of all data and sensitive documents. These should be stored in a secure off-site location on a regular basis.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion

Public Relations

You should educate your customer about your system. You should encourage them to be alert and to report any suspicious activity to law enforcement authorities.

Question	Answer	Comment	Risk Assess/Action
37. Do you have a program to educate and encourage the public to be vigilant and report suspicious activity to assist in the security protection of your wastewater system and neighborhood watch program?	Yes ❑ No ❑	Advise your customers and the public that your system has increased preventive security measures to protect the wastewater supply from vandalism. Ask for their help. Provide customers with your telephone number and the telephone number of the local law enforcement authority so that they can report suspicious activities. The telephone number can be made available through direct mail, billing inserts, notices on community bulletin boards, flyers, and consumer confidence reports.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion
38. Does your wastewater system have a procedure to deal with public information requests and to restrict distribution of sensitive information?	Yes ❑ No ❑	You should have a procedure for personnel to follow when you receive an inquiry about the wastewater system or its operation from the press, customers, or the general public. Your personnel should be advised not to speak to the media on behalf of the wastewater system. Only that person should respond to media inquiries. You should establish a process for responding to inquiries from your customers and the general public.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion
39. Do you have a procedure in place to receive notification of a suspected outbreak of a disease immediately after discovery by local health agencies?	Yes ❑ No ❑	It is critical to be able to receive information about suspected problems with the wastewater at any time and respond to them quickly. Written procedures should be developed in advance with your state wastewater primacy agency, local health agencies, and your local emergency planning committee and reviewed periodically.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion

Question	Answer	Comment	Risk Assess/Action
40. Do you have a procedure in place to receive notification of a suspected outbreak of a disease immediately after discovery?	Yes ❑ No ❑	As soon as possible after a disease outbreak (possibly from recreational swimming or consumption from a contaminated water body), you should notify testing personnel and your laboratory of the incident. In outbreaks caused by microbial contaminants, it is critical to discover the type of contaminant and its method of transport (wastewater, food, etc.). Active testing of your wastewater supply will enable your laboratory, working in conjunction with public health officials, to determine if there are any unique (and possibly lethal) disease organisms in your wastewater. It is critical to be able to get the word out to your or others using the source wastewater that your plant is discharging effluent to as soon as possible after discovering a health hazard in your water supply. Drinking water systems or other food/beverage manufactures using the same source of water downstream from your wastewater system should be contacted immediately. Some simple methods include announcements via radio or television, door-to-door notification, a phone tree, and posting notices in public.	High ❑ Medium ❑ Low ❑ Action Needed: Scheduled Completion

Now that you have completed the "Security Vulnerability Self-Assessment Guide for Small Wastewater Systems, " review your needed actions and then prioritize them based on the most likely threats. A Table to assist you in prioritizing actions is provided in Attachment 1.

Attachment 1: Prioritization of Needed Actions

Once you have completed the "Security Vulnerability Self-Assessment Guide for Small Drinking Wastewater Systems," review the actions you need to take to improve your system's security. Note the questions to which you answered "no" on this worksheet. You can use it to summarize the areas where your system has vulnerability concerns. It can also help you prioritize the actions you should take to protect your system from vulnerabilities. You can rank your priorities in numerical order or based on the categories of high, medium, and low.

Use the following information and the information you have generated by completing this assessment to prioritize and rank the most important security vulnerabilities to your system.

1. Any information from local law enforcement office about the likelihood of a terrorist attack or other threats.
2. The primary mission of your system (i.e., protection of public health, protection of the environment, etc.).
3. Single points of failure (i.e., disabling pump) that severely limit your capability to conduct your primary mission.
4. Critical customers- such as hospitals, manufactures, power plants, and schools that rely on your service for sanitation.
5. The vulnerabilities identified by completing this assessment.

Question	Needed Action	Scheduled Completion	Priority/Ranking
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐
			High ☐ Med ☐ Low ☐

VULNERABILITY ASSESSMENT & EMERGENCY RESPONSE PLAN CERTIFICATION

Please fill in the following information so that a record can be maintained of wastewater systems that have completed a vulnerability assessment and emergency response plan.

NPDES Permit Number: _____

System Name: _____

Address: _____

City: _____ **State:** _____

Phone: _____ **Fax:** _____

Email: _____

Authorized Person to Sign this Certification on behalf of the System (Printed):

_____

Title: _____

Address: _____

City: _____ **State/Zip:** _____

Phone: _____ **Fax:** _____ **Cell:** _____

Email: _____

24 Hour Emergency Contact Information for Your System:

Contact Person: _____

Daytime Phone: _____ **Night Phone:** _____

Emergency Phone: _____ **Email:** _____

Cell Phone: _____

I certify to that the information in this vulnerability assessment has been completed to the best of my knowledge and that the appropriate parties have been notified of the assessment and recommended steps to be taken to enhance the security of the wastewater system. Furthermore, a copy of the completed assessment will be retained at the public wastewater system, in a secure location, for state review as requested.

Signed: _____ **Date:** _____

Threat Identification Checklists

Wastewater System Telephone Threat Identification Checklist

In the event your wastewater system receives a threatening phone call, remain calm and try to keep the caller on the line. Use the following checklist to collect as much detail as possible about the nature of the threat and the description of the caller.

1. Types of Tampering/Threat:

❑ Contamination ❑ Threat to tamper

❑ Biological ❑ Bombs, explosives, etc.

❑ Chemical ❑ Other (explain)

2. Wastewater System Identification

Name:

Address:

Telephone:

PWS Owner or Manager's Name:

3. Alternate Wastewater Source Available: Yes / No If yes, give name and location:

4. Location of Tampering:

❑ Raw Wastewater Source ❑ Bio-solids Storage ❑ Wastewater Collection System

❑ Treatment Chemicals ❑ Other (explain):

5. Contaminant Source and Quantity:

6. Date and Time of Tampering/Threat:

7. Caller's Name/Alias, Address, and Telephone Number:

8. Is the caller (check all that apply):

❑ Male ❑ Female ❑ Foul ❑ Illiterate ❑ Well Spoken ❑ Irrational ❑ Incoherent

9. Is the caller's voice (check all that apply):

❑ Soft ❑ Calm ❑ Angry ❑ Slow ❑ Rapid ❑ Slurred ❑ Loud

❑ Laughing ❑ Crying ❑ Normal ❑ Deep ❑ Nasal ❑ Clear ❑ Lisping

❑ Stuttering ❑ Old ❑ High ❑ Cracking ❑ Excited ❑ Young

❑ Familiar (who did it sound like?)

❑ Accented (which nationality or region?)

10. Is the connection clear? (Could it have been a wireless or cell phone?)

11. Are there background noises?

❑ Street noises (what kind?)	
❑ Machinery (what type?)	
❑ Voices (describe)	
❑ Children (describe)	
❑ Animals (what kind?)	
❑ Computer Keyboard, Office	
❑ Motors (describe)	
❑ Music (what kind?)	
❑ Other	

12. Call received by (name, address, and telephone number):

Date received: Time Received:

13. Call Reported to: Date/Time:

14. Action(s) taken following receipt of the call:

Wastewater System Report of Suspicious Activity

In the event personnel from your wastewater system (or neighbors of your wastewater system) observe suspicious activity, use the following checklist to collect as much detail about the nature of the activity.

1. Types of suspicious activity:

- ❑ Breach of security systems (e.g., lock cut, door forced open).
- ❑ Unauthorized personnel on wastewater system property.
- ❑ Presence of personnel at the wastewater system at unusual hours.
- ❑ Changes in wastewater quality noticed by customers (e.g., change in color, odor) that were not planned or anticipated by the wastewater system
- ❑ Other (explain)

2. Wastewater System Identification:

Name:

Address:

Telephone:

NPDES Owner or Manager's Name:

3. Alternate wastewater source available : Yes / No If yes, give name and location:

4. Location of Suspicious Activity:

- ❑ Raw Wastewater Source ❑ Bio-solids Storage Facilities ❑ Treatment Plant ❑ Wastewater Collection System
- ❑ Treatment Chemical
- ❑ Other (Explain):

5. If breach of security, what was the nature of the breach?

- ❑ Lock was cut or broken, permitting unauthorized entry. (Specify location)
- ❑ Lock was tampered with, but not sufficiently to allow unauthorized entry. (Specify location)
- ❑ Door, gate, window, or any other point of entry (vent, hatch, etc.) was open and unsecured. (Specify location)
- ❑ Other (Specify nature and location

6. Unauthorized personnel on site:

Where were these people? (Specify location)

What made them suspicious?

- ❑ Not wearing wastewater system uniforms
- ❑ Something else? (Specify)

What were they doing?

7. Please describe these personnel features (height, weight, hair color, clothes, facial hair, any distinguishing marks):

8. Call received by (name, address and telephone number):

Date Received:

Time of call:

9. Call reported to: Date / Time:

10. Action(s) taken following receipt of call:

Attachment 3:

Accidental Chlorine Release Emergency Notifications

By Jon Groethe, Minnesota Department of Health

A critical piece of pre-planning for any water system emergency is having a complete list of emergency contact notifications readily available to you. Certain emergency notifications must be made immediately, being governed by strength of statute or historic legislative policy. Notifications that are required at the onset of an accidental chlorine release fall within that category.

The purpose of this article is to share with you three important and basic notifications that must be made when you are facing a chlorine release at your water plant, as well as the time frame in which they are expected to be completed. This article is not meant to address operations or all post-incident communications that take place.

For chlorine, the reportable quantity (RQ) is defined by two federal statutes (Comprehensive Environmental Response, Compensation, and Liability Act of 1980 and Emergency Planning and Community Right-to-Know Act) as being a release of 10 pounds or greater occurring in a 24-hour time window.

If you believe you have exceeded this amount but are unsure of the exact amount that has been released, it is better to go ahead and make the necessary notifications and establish a firm quantity later. There are no penalties associated with over-reporting.

Three immediate emergency notification calls must then be made. The first call is made at the local level of government (Emergency 911), which alerts local emergency responders. The second notification call occurs at the state level of government. This is the call you will make to the Minnesota State Duty Officer (800-422-0798). The duty officer will share information you have provided among state agencies having emergency response roles through both phone calls and email transmissions. On-call personnel at various state and local agencies will coordinate a field response based on regional resources. The third call occurs at the federal level.

This is the notification call you will make to the National Response Center (1-800-424-8802). This notification is equally critical because a hazardous chemical release may bear impacts with federal considerations (state and national borders, an immediate need for deployment of federal resources, etc.).

If you have had a chlorine leak and are absolutely certain that the amount released is less than the RQ, you are still required to make a single call to the Minnesota State Duty Officer to satisfy Minnesota Statute 115.061 (Duty to Notify). But if you're not sure of the amount released, you need to go ahead and make all three calls. Remember: if in doubt, report.

What is the allowable time-frame in which all three notification calls need to be made? Superfund legislative history states that ordinarily "delays in making the required notifications should not exceed 15 minutes after the person in charge has knowledge of the release. Immediate notice requires shorter delays whenever practicable." Therefore, the time frame that would be considered allowable and prompt is 15 minutes. All three notification calls should be completed consecutively, one following another. Although there may be competing priorities around you, making these notifications should be prioritized and accomplished.

An important note: The person in charge of the utility must always be the one directly making the emergency notification calls. This requirement is explicitly stated in the Federal Register, Part 302.69. Remember, as the person in charge, you cannot delegate notification calls to others. You must always personally notify, even when a notification call has previously been made by your local fire chief.

Within 30 days, an emergency release follow-up report must be submitted to Minnesota Department of Public Safety (DPS) Division of Homeland Security and Emergency Management. The Emergency Release Follow-up Report can be downloaded using a link located on the DPS website https://dps.mn.gov/divisions/hsem/epcra/Pages/regulated-facilities.aspx under Resources.

The completed report should be emailed directly to Steve Tomlyanovich (steve.tomlyanovich@state.mn.us) at the Minnesota Department of Public Safety.

To boil all of this down, there are three calls the person in charge must make during an accidental chlorine release, and they correspond to the three levels of government—local, state and federal. Once you have knowledge that a reportable release has occurred, you then have a 15-minute window to make all three calls. Completion of these actions will go a long ways toward keeping your utility on course relative to prevailing emergency notification requirements.

Disclaimer

This document contains information on how to plan for protection of the assets of your wastewastewater system. The work necessarily addresses problems in a general nature. You should review local, state, and federal laws and regulations to see how they apply to your specific situation.

Knowledgeable professionals prepared this document using current information. The authors make no representation, expressed or implied that this information is suitable for a specific situation. The authors have no obligation to update this work or to make notification of any changes in statutes, regulations, information, or programs described in this document. Publication of this document does not replace the duty of wastewastewater systems to warn and properly train their employees and others concerning health and safety risks and necessary precautions at their wastewastewater systems.

The National Rural Wastewater Association does not assume any liability resulting from the use or reliance upon any information, guidance, suggestion, conclusion, or opinions contained in the document.