WATER AND WASTEWATER CYBERSECURITY PLAN TEMPLATE

i. VERSION HISTORY

Date	Version	Description
05/29/2018	0.1	Initial Draft
6/7/2018	0.2	Modifications – Connie Justice
6/11/2018	0.3	Modifications- Sondhi Solutions
6/11/2018	0.4	Modifications – Connie Justice
6/17/2018	0.5	Modifications- Sondhi Solutions
06/20/2018	1.0	Second Draft – Connie Justice
6/21/2018	1.1	Modifications – Connie Justice and John
6/29/2018	2.0	Lucas

7/10/2018	2.1	Third Draft – Connie Justice
7/20/2018	2.2	Modifications-Connie Justice
7/30/2018	2.3	Modifications-Connie Justice
8/15/2018	2.4	Modifications – Connie Justice
8/26/2018	3.0	Modifications – Connie Justice
9/6/2018	3.1	Fourth Draft – Connie Justice
		Modifications – Connie Justice, John Lucas, Steve Berube, Jamie Foreman, Jon Weirick
10/22/2018	4.0	Connie Justice
10/23/2018	4.1	Connie Justice
12/15/2018	4.2	Connie Justice
1/3/2019	4.3	Connie Justice

ii. CONTRIBUTORS AND ACKNOWLEDGEMENTS

This cyber security template was developed by the Water / Wastewater committee of the Indiana Executive Cyber Security Committee of the State of Indiana. This committee is a committee of business, government, and regulatory members from across the State of Indiana.

iii. IMPORTANT TERMS

Term	Definition

iv. TABLE OF CONTENTS

INTRODUCTION

This document is a checklist of recommendations for maintaining the overall Cybersecurity posture of a Water or Wastewater Treatment operation. To be effective, each entity must ensure the cooperation of its IT Department, the Water and Wastewater Operations, and a Cybersecurity partner (if additional expertise in this area is required). Having a plan is only the first step. At least twice a year, you should verify that people, systems and software continue to align with your cybersecurity plan. Create a ledger to ensure you've covered identified recommendations. The guide is based on NIST cyber security framework and the EPA Incident Action Checklist – Cybersecurity. This document has been established in order for Water utilities to become compliant with Indiana Senate bill 362.

HOW TO USE THIS GUIDE

The document should be followed in the creation of policies, processes, and programs and verified by a Cybersecurity lead and clearly documented as part of the regularly executed Cybersecurity maintenance routine. A secure document management repository should be used to maintain and publish all documentation revisions.

ACRONYM LIST

IT	Information Technology
EPA	Environmental Protection Agency
NIST	National Institute of Standards and Technology
CSF	Cybersecurity Framework
AWWA	American Water Works Association
US-CERT	US-Computer Emergency Readiness Team
FFIEC	Federal Financial Institutions Examination Council
IDS	Intrusion detection system
TCP/IP	Transmission Control Protocol/Internet Protocol,
ICS	Industrial controls system
NIST SP	NIST Special Publication
ERP	Emergency response plan
NCCIC	National Cybersecurity & Communications Integration Center
INWARN	
IDHS	Indiana Department of Homeland Security
ISAC	Water Information Sharing and Analysis Center (WaterISAC)
WATER-ISAC	Water Information Sharing and Analysis Center (WaterISAC)

AAR	After action report
IP	Improvement plan
SOX	Sarbanes Oxley
HR	Human resources
PII	Personally identifiable information
HIPAA	The Health Insurance Portability and Accountability Act
SCADA	Supervisory control and data acquisition
CSRC	Computer Security Resource Center (CSRC)
SANS	SANS Institute was established in 1989 as a cooperative research and education organization
DMZ	Demilitarized zone
NMS	Network monitoring system
IPSEC	Internet Protocol Security
AES	Advanced Encryption Standard
WPA2	Wi-Fi Protected Access II
DHS	Department of Homeland Security
POC	Point of Contact

CYBERSECURITY PLAN CHECKLIST INSTRUCTIONS

HOW TO USE

The Cybersecurity Plan Checklist (the checklist) is designed to check off the plan checklist items as you complete them or if you have them completed already you can check off the item.

Each link next to the check box will take you to the page with further explanation of the checklist item with links to example forms.

EASE OF USE

The checklist is designed to be easy to use, however, if you have no background in cybersecurity it is recommended that you attend training sessions and attain help with the checklist.

CHECKLIST DOCUMENTS

The checklist and documents created are living documents and should be updated on a regular basis, when systems or people change, or on a periodic basis.

Cybersecurity Plan Checklist

Identify

□ Identify Organization Security Lead

Identify an organization security lead for you company

□ Classify data

Identify mission critical data assets and classify data assets in order of importance. Identify personnel responsible for data asset/s

□ Identify assets

Identify Mission Critical Technology Assets

□ Security policies

A document that states in writing how a company plans to protect the company's physical and information technology (IT) assets

□ Risk Assessment

Execute a cybersecurity risk assessment to identify vulnerabilities in business and industrial control mission critical systems

□ Risk Management Strategy

A security program established to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks

Protect

□ Employee Training and Awareness

Employees should be trained and be aware of cybersecurity issues and situations that can compromise the business and ruin the company's reputation

□ Access Controls

Granting access and privileges to systems, resources or information needed.

□ Securing Network and Cloud

Ensure secure communications and multifactor authentication are setup between the business and cloud providers

□ Authentication Policy

Multifactor-authentication should be used; a passphrase should be used; unique passwords for separate confidential accounts.

□ Data Security

Protect business data

□ Information Protection

Data should be protected by proper backups and testing. Proper destruction, incident response, disaster recovery, and business continuity plans in place.

□ Maintenance

Equipment maintenance/replacement program established

□ Protective Technology

Storage media management; centralized logging; Service level agreements with third party vendor; and system hardening based on criticality of systems

□ Physical Access

Physical access limited; procedures to access buildings and server rooms; and no physical plugging into network

Detect

□ Anomalies and Events

Device to identify malicious activity (intrusion detection system (IDS)) should be implemented. Logs should be used to notify of failed logins and malicious behavior.

□ Continuous Monitoring

Web filtering and patching should be used to monitor unauthorized activity.

□ Detection Processes

Register for cybersecurity alerts and advisories from water sector and government partners to be aware of new vulnerabilities and threats. Segment ICS network from business network. Restrict access of ICS network to internet unless needed.

Respond

□ Response Planning

A security and response program should be established to ensure staff is aware of security policies and incident response/notification procedures

□ Respond Communications

List of primary and backup contacts

□ Analysis

Investigate incidents, logs, and vulnerability systems; establish a digital forensics program

□ Mitigation

Contain incidents; mitigate incidents, or accept risks

□ Respond Improvements

Incorporate lessons learned; update response plans

Recover

□ Recovery Planning

Policies and procedures for system instantiation/deployment should be established to ensure business continuity

□ Recovery Improvements

Incorporate lessons learned from response plans and update response plans

□ Recovery Communications

Primary and backup contacts for personnel or vendors; points of contact for reporting a cyber incident and requesting assistance with response and recovery

1 IDENTIFY

When they happen, cybersecurity events are very stressful. This is not a time when you want to guess about who to call or where to find a serial number for an affected device. To help prepare for an event, it is important to create and maintain inventories of your assets. Knowing how those assets connect and work together is also very important. Having a list of contacts will ensure you have access to people and organizations in the event of an emergency. Building and maintaining an Information Technology Asset Inventory ensures you have critical information on your organization's technology items as they come in and out of their life cycle. Give each asset a unique code and label when entered into the inventory as they come into operation. Review the inventory at least annually and note items that are nearing "end of life" and plan to retire or replace them. Appendix A: IT Asset Inventory has a template to help you get started.

1.1 ORGANIZATION SECURITY LEAD

a. Identify an organization security lead
b. Identify emergency response team

1.2 ASSET MANAGEMENT

a. Identify mission critical data assets and classify data assets in order of importance. Identify personnel responsible for data asset/s.
b. See Exhibit 1 for data classification template
c. Identify mission critical assets
    a. Identify Mission Critical Technology Assets
        1. Applications (email applications, web browsers, productivity applications)
        2. Data (What storage devices data is stored on: hard drives, portable media, off site data backups)
        3. Servers (hardware devices that can host applications, or other virtual servers)
        4. Workstations/HMI/PLC (Systems that run SCADA software, Systems that run Business Software)
        5. Field devices (Laptops, Tablets, Cell Phones)
        6. Communications and network equipment (router, firewall, voice system)

Note: See Exhibit 2 for asset identification table template.

1.3 BUSINESS ENVIRONMENT AND GOVERNANCE

a. Governance framework is used to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.
b. Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.
c. Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.

d. Security Policies and Procedures Exhibit 3

1.4 Risk Assessment

1.4.1 Conduct a Risk Assessment

a. Execute a cybersecurity risk assessment to identify vulnerabilities in business and industrial control mission critical systems using the NIST CSF/AWWA tool (Link to Indiana Water/Wastewater Risk Model will be added).
b. Create action plan to mitigate significant vulnerabilities identified in risk assessment, and act on the mitigation plan.
   a. Create an action plan that prioritizes actions needed to mitigate risk.
   b. Prioritize the implementation of protective measures
   c. Low hanging fruit-Optimize your budget in relation to identified risks.

1.4.2 Risk Management Strategy

a. A security program established to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.
b. Risk management is the process of identifying what information requires what level of protection and then implementing the proper level of protection and subsequently monitoring the protection.
   The basic risk strategy is:
   a. Identify basic information stored and used in the business
   b. Determine the classification or value of the information
   c. Inventory the assets in the business
c. Understand what threats and vulnerabilities exists in the business

1.5 *Links for IDENTIFY Section*

a. US-CERT’s Protect Your Workplace Posters & Brochure: http://www.us-cert.gov/reading_room/distributable.html
b. Socializing Securely: Using Social Networking Services: http://www.us-cert.gov/reading_room/safe_social_networking.pdf
c. Governing for Enterprise Security: http://www.cert.org/governance/
d. FFIEC Handbook Definition of Reputation Risk: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/reputation-risk.aspx
e. What Businesses can do to help with cyber security: http://www.staysafeonline.org/sites/default/files/resource_documents/What%20Businesses%20Can%20Do%202011%20Final_0.pdf

RETURN TO CHECKLIST

2 PROTECT

The next step in your cybersecurity plan should be to determine what protections to put in place. This helps to limit exposure and limit damage in the event of an attack. Protections can include the following:

a. A way to control access to the IT assets you identified in Step 1.
b. A plan to provide cybersecurity awareness and training to your staff
c. A method to determine how to keep data, networks and systems secure
d. A plan to make sure systems are up-to-date with patches or if you can't patch systems then have appropriate controls to make sure systems are not modified (i.e. Scada systems with whitelisting).
e. A decision to use protective technologies to help prevent threats if appropriate

2.1 EMPLOYEE TRAINING AND AWARENESS

Employees should be trained and be aware of cybersecurity issues and situations that can compromise the business and ruin the company's reputation. See Exhibit 5 for training and awareness guidelines.

2.2 ACCESS CONTROL

2.2.1 SECURING NETWORK AND CLOUD

The network infrastructure is the backbone for defenses against internal and external malicious programs and nefarious persons. Layered protection and various devices are the key to protecting internal networks from these bad actors. Cloud services are becoming common place to conduct business. Ensure secure communications and multifactor authentication are setup between the business and cloud providers. See Exhibit 6 for example template of securing network and cloud.

2.2.2 IMPLEMENT A RIGOROUS USER AUTHENTICATION POLICY

a. Multifactor-authentication should be used wherever possible.
b. Use a passphrase instead of a password. A passphrase is a phrase constructed of multiple words. An example would be: "sunwalkraindrive". A passphrase constructed of 4 words (sun + walk + rain + drive) is easy to remember but hard to guess. It is not recommended that users change their passwords because of the general predictability in which users change specific characters.
c. Use unique passphrases for separate confidential accounts.

2.2.3 DATA SECURITY

In addition to understanding data classification, it is important to protect business data. Sensitive business data should be encrypted on storage medium and data should be encrypted in transit from end to end communications. The key elements to secure data are:

a. Data at rest is encrypted
b. Data in transit is encrypted

c. Logging in place to protect against data leaks
d. Systems in place to ensure integrity of data

2.3 Information Protection Processes and Procedures

Data should also be protected by proper backups and testing. Additionally, proper destruction of data is very important, as well as having an incident response, disaster recovery, and business continuity plan in place.

a. Backup and restore of data are tested
b. Data destruction process is in place
c. Incident response, disaster recovery, and business continuity plans are in place and managed.

2.4 Maintenance

Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity. See Exhibit 7 for the asset management process.

2.5 Protective Technology

a. Storage media management and disposal program established to ensure that any sensitive data/software is used appropriately and is removed prior to media disposal (including approved policies and procedures).
b. Centralized logging system including policies and procedures to collect, analyze and report to management.
c. SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.
d. Program for hardening servers, workstations, routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).

2.6 Physical Access

a. Physical access to facilities and areas where operational equipment is running should be limited to staff who require the access to perform their job. A more liberal policy on access control is not best practice and would inevitably provide access to individuals who accidently or purposefully create problems with the environment.
b. Physical Security should be implemented to ensure access is given to areas with operational or IT systems only to those personnel who need access to these areas to perform their job duties.
c. No access to the internet should be permitted to industrial control systems unless absolutely required. If required, a web content filter should be used to limit the access to the system based on a policy.

Return to Checklist

3 Detect

Organizations must implement the appropriate measures to quickly identify cybersecurity events. The adoption of continuous monitoring solutions that detect anomalous activity and other threats to operational continuity is required to comply with this function. Organizations should have network visibility in order to anticipate a cyber incident; which should be included in your current cybersecurity plan.

3.1 Anomalies and Events

a. An intrusion detection system (IDS) should be implemented to identify malicious activity. IDS systems are designed to watch for signatures of malicious traffic, or to recognize anomalies in the underlying TCPIP communications. If anything falls outside of the normal patterns for how these protocols work, the IDS will send an alert to the administrator for the system who can then act upon the alert by implementing a firewall rule to block the offensive traffic.
b. Security Continuous Monitoring. A basic logging server should be deployed to aggregate log data from different devices to correlate alerts and notify the administrator when certain thresholds have been met (e.g. 3 or more failed logins for an account).

3.2 Security Continuous Monitoring

a. Monitoring for unauthorized personnel, connections, devices, and software is performed
b. Active monitoring for adversarial system penetration
c. Intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter
d. If you use a web filtering system, employees should have clear knowledge of how and why their web activities will be monitored, and what types of sites are deemed unacceptable by your policy.
e. Identification of security deficiencies in existing hardware and software.

3.3 Detection Processes

a. Continuous monitoring is a very effective way to analyze and prevent cyber incidents in ICS networks. Use intrusion detection systems, intrusion prevention systems and file integrity checkers to spot intrusions and verify web content.
b. Register for cybersecurity alerts and advisories from water sector and government partners to be aware of new vulnerabilities and threats (two sources of cybersecurity alerts are WaterISAC, which has a basic membership that is free, and ICS-CERT (https://ics-cert.us-cert.gov/alerts)).
c. Ensure the ICS network is separated from the public network. Additionally, the business network should be segmented from the ICS network using industry best practices (NIST SP 800-82 section 5).
d. Restrict internet access to industrial control systems unless there is a critical need.
e. System acceptance standards including data validation (input/output), message authenticity, and data integrity established to detect information corruption during processing.

Return to Checklist

4 Respond

a. Should a cyber incident occur, organizations must have the ability to contain the impact. To comply, your organization should utilize your response plan which should include processes such as:
   i. define communication lines among the appropriate parties
   ii. collect and analyze information about the event
   iii. perform required activities to eradicate the incident
   iv. incorporate lessons learned into revised response strategies.

b. The Emergency Response Plan (ERP) should be referenced and adhered to in the event of a Cybersecurity incident. The Emergency Response Team should be comprised of essential personnel that should be contacted, followed by the contacts listed in the Emergency Response Plan including all other utility personnel and media outlets as necessary. NCCIC can also assist with critical system response and recovery (888-282-0870 or NCCIC@hq.dhs.gov)

4.1 Response Planning

A security and response program should be established to ensure staff is aware of security policies and incident response/notification procedures. See Exhibit 8 for ERP steps.

4.2 Communications

Contacts

a. Have ready access to a list of primary and backup contacts for personnel or entities (vendors, government agencies, etc.) responsible for the operation and maintenance of each critical system.

b. Next, identify priority points of contact for reporting a cyber incident and requesting assistance with response and recovery. Include any state resources that may be available such as Indiana State Police, Indiana National Guard Cyber Division or mutual aid programs (INWARN), as well as the Indiana Department of Homeland Security to assist with an attack and any other contact information needed. Exhibit 9: Emergency Contacts has a template to help organize necessary contacts.

4.3 Analysis

a. Investigate notifications from detection systems
b. Understand incidents
c. Incidents are categorized appropriately per response plans
d. A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.

4.4 Mitigation

a. Contain incidents
b. Mitigate incidents
c. Newly identified vulnerabilities are mitigated or documented as accepted risks

4.5 Improvements

a. Incorporate lessons learned from response plans

b. Update response plans

4.6 Contacts

4.6.1 *Assess the damage to utility systems and any disruption to operations.*

A checklist should be created for use in the Emergency Response Plan to verify functionality for critical business services and their supporting infrastructure. Any affected services should be documented and relayed to the administrator of the Emergency Response Plan. The administrator of the Emergency Response Plan should also document any reports of suspicious communications before or during the incident. The documentation should include date and time that information was reported.

4.6.2 *Forensics Image*

a. A forensic image should be taken of the impacted systems and transferred to other secure media that is not connected to a network. If possible, the original systems that were affected should be disconnected from the network and not powered down or rebooted.
b. After containment and a forensic image has been captured and the original system has been taken off the network and preserved for evidence, restore the system function to a new system from the last known good backup before the infection occurred.
c. Never work on the original evidence when responding to a Cybersecurity incident. This will ensure the integrity of the original evidence.

4.6.3 *Lessons Learned*

a. A Lessons Learned session should be conducted after an incident has been resolved. Each problem, it's perceived cause, and what should have been done differently should be discussed.
a. Positive feedback should also be discussed to show what went right during the response.
b. Submit the incident to WaterISAC and Indiana AWWA. The online WaterISAC incident report form can be found at https://www.waterisac.org/report-incident or a call can be placed at 866-H2O-ISAC. Additionally, report incident to Indiana AWWA.

Return to Checklist

5 Recover

5.1 Recovery Planning

Policies and procedures for system instantiation/deployment should be established to ensure business continuity.

5.2 Improvements

Develop a lessons learned document and/or an after action report (AAR) to document utility response activities, successes, and areas for improvement. Create an improvement plan (IP) based on your AAR and use the IP to update your vulnerability assessment, ERP and contingency plans. See Exhibit 10 for an example AAR report.

5.3 Communications

a. Organizations must develop and implement effective activities to restore any capabilities or services that were impaired due to a cybersecurity event. Organizations must have a recovery plan in place, be able to coordinate restoration activities with external parties and incorporate lessons learned into updated recovery strategy. Defining a prioritized list of action points which can be used to undertake recovery activity is critical for a timely recovery.
b. The organizations recovery plan should address damage to reputation from data breaches, criminal organizations, inappropriate employee actions.
c. Mission critical processes should be documented in the Emergency Response Plan, and the appropriate sequence should be determined and communicated by the Emergency Response Plan administrator based on the systems that have been affected.
d. If required, the public and media outlets should be notified of the incident.

Return to Checklist

EXHIBIT 1: DATA CLASSIFICATION TEMPLATE

Example Data Classification Template

Data	Classification	Justification	Data Owner	Data User
Executive Business Material	Restricted Confidential	Intellectual Property		Executives & Assistants
Bank Accounts - Information	Confidential	SOX		Financial Reporting
Financial Reporting Data	Confidential/Public - phases	SOX		Financial Reporting
Building Information	Confidential	SOX		Financial Reporting
Legal Case Information	Sensitive	Intellectual Property		Legal
Leasing Information	Confidential / Restricted Confidential phases	Intellectual Property		Leasing
Security video	Sensitive	Intellectual Property		Security
Custom Application Code	Sensitive	Intellectual Property		Information Services
Audit Information	Restricted Confidential	Data from all areas		Audit Services
Tax Filings	Sensitive			Corporate Tax
HR	Sensitive	PII, Laws		HR
Benefits	Confidential	HIPAA / do not submit		HR

Definitive guide to data classification: https://infosecpartners.com/wp-content/uploads/2017/02/The-Definitive-Guide-to-Data-Classification.pdf

6 EXHIBIT 2: CRITICAL ASSET INVENTORY PER FACILITY

Facility Name: ______________________

AssetID	Item	Description	Serial #	Service Date	Retirement Date	Original Value	Current Value	Custodian	Department

7 Exhibit 3: Policy Examples

Policy Name	**Description**
Security Policy	A document designed for staff that should include the security program requirements and require signoff for employees.
Emergency Response Plan	Procedures to follow in the event of a Cybersecurity breach.
Password Policy	Outlines the specific password requirements for the organization.
Acceptable Use Policy	Defines how the internet and email should be used to promote a responsible culture around Cybersecurity.

- Guide to Industrial Control Systems (ICS) Security https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- Guide for Cybersecurity Event Recovery https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf
- 21 Steps to Improve Cyber Security of SCADA Networks https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf
- Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf
- 10 ways to develop cybersecurity policies and best practices https://www.zdnet.com/article/10-ways-to-develop-cybersecurity-policies-and-best-practices/
- SANS Information Security Policy Templates https://www.sans.org/security-resources/policies

8 Exhibit 4: Water Waste Water Risk Assessment (To Be Delivered)

9 Exhibit 5: Employee Training and Awareness

a. Implement a cybersecurity awareness program that includes:
   i. Social engineering
   ii. Sharing of personal information
   iii. Phishing
      1. Types of phishing attacks
      2. What can happen as a result of Phishing
   iv. Ransomware
      1. What to do in the event your system has been compromised by Ransomware
   v. Email Best Practices and what to watch for
   vi. Internet browsing acceptable use policy
   vii. Authentication (password policy, use of multi-factor authentication, and remote access where required).

b. Provide on-going cross training for critical systems and ICS staff that identifies current best practices and standards for ICS cybersecurity.

c. Provide basic network and radio communications training for ICS technicians.

d. Participate in water sector programs that facilitate cybersecurity knowledge transfer.

e. Identify appropriate certifications for internal and external staff. Include certification requirements in SLAs and contracts with external service providers.

f. Provide periodic security awareness training to employees that identifies risky behaviors and threats.

g. Promote information sharing within your organization.

10 Exhibit 6: Securing Network and Cloud

a. Network

   i. Network Separation

      1. Business systems such as email or other systems that require access to the internet should be managed on a separate physical network from the water/wastewater operation systems.
      2. A DMZ should be established for any traffic originating from outside of the internal network, although traffic of this origin should be eliminated where possible and ensure there is no connectivity to the Water/Wastewater systems network.

   ii. Network Hardware

      1. Have records of current hardware and software configurations.
      2. Maintain support contracts with critical software vendors, for example: endpoint protection (anti-virus, malware detection, log monitoring) and operating system patches in accordance with each vendor's recommended patch level if applicable
      3. It is important to maintain support contracts for software programs required to maintain the operation or protect/backup the systems.

         a. There could also be a delay in gaining access to critical software patches or system support if there is a lapse in support coverage.

         b. Software patches should be first tested on an offline system that doesn't have access to the Water/Wastewater Industrial Control System network.

         c. Once the patch is demonstrated to be safe, it can be scheduled on actual production systems.

   iii. Monitoring

      1. An NMS should be implemented to ensure alerts are sent to the network manager when a device is unavailable for a pre-determined period of time.
      2. System and Event Logs should be monitored for critical events that occur, and alerts sent to the network manager.

   iv. Cloud

      1. Interfacing with cloud environments
      2. IPSEC tunnels should be used between on premises networks and public cloud networks
      3. Firewalls should be used in cloud-based network for separation in the same manner recommended on internally hosted systems.
      4. Centralized authentication authority and multi-factor authentication should be used when accessing public cloud environments.

b. Server and Workstation Hardening:

   i. Disable services that are not required

      1. Use whitelisting software to only allow execution of required applications.
      2. Ensure system-based firewalls are not more permissive than they need to be – only allow what is absolutely necessary.
      3. Disable built-in, default accounts.
      4. Access Control should be employed and provide multi-factor authentication, pass phrases made up of 4 regular words, and unique passwords for different

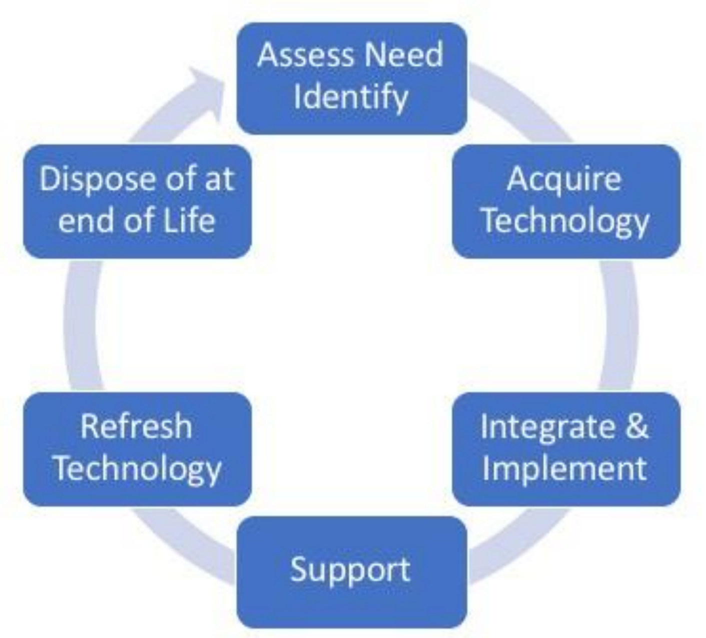
systems. Operational systems and Business systems should reside on two separate physical networks separated by firewall devices.

5. Service Level Agreements (SLAs) should be included in vendor contracts to ensure they are providing the amount of internet bandwidth and round-trip speeds agreed to in the contract, and that 3rd party personnel that work on utility systems are certified based on agreed upon industry standard certifications based on their job function.

c. Wireless and Wireless guest access secured by strong protocols, such as WPA2 with AES encryption.

11 Exhibit 7: Maintenance Life Cycle Process

Asset Lifecycle Management Process



12 Exhibit 8: Emergency Response Plan (ERP)

An emergency response plan (ERP) is important if a cybersecurity incident were to occur that requires notification outside of the primary business. The following is a guide for possible ERP action items:

1. Contact Law Enforcement-if required
2. Contact government authorities-if required
3. Notify customers
4. Record the data lost or exposed
5. Record measures taken to reduce future exposure
6. Technical and leadership work to limit damage
7. Containment
8. Reputation risk management
9. Request outside assistance if needed
10. Begin recovery
11. Eradicate malware
12. Hold lessons learned meeting
13. Discover knowledge gained during the incident
14. Document knowledge gained during the incident
15. Refine knowledge gained during the incident

13 EXHIBIT 9: CONTACT LIST

Contact Name	Organization Name	Phone	Email	Website
	Law Enforcement			
	IT Staff/Vendor			
	SCADA Staff/Vendor			
	DHS NCCIC	888-282-0870		
	Local Laboratory			
	State Primacy Agency			
	Local Emergency Management Agency			
	Local Health Department			
	INWARN Chair			
	State Emergency Management Agency			

14 EXHIBIT 10: AFTER ACTION REPORT

Incident Name	[Insert the formal name of exercise, which should match the name in the document header]
Incident Dates	[Indicate the start and end dates of the incident]
Description	This incident …
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor)]

[Incident]

The strengths and areas for improvement for each core capability aligned to this objective are described in this section.

[Incident Description]

Strengths

The [full or partial] incident can be attributed to the following:

1: [Observation statement]

2: [Observation statement]

3: [Observation statement]

Areas for Improvement

The following areas require improvement to achieve the full capability level:

Area for Improvement 1: [Observation statement. This should clearly state the problem or gap; it should not include a recommendation or corrective action, as those will be documented in the Improvement Plan.]

Reference: [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: [Provide a root cause analysis or summary of why the full capability level was not achieved.]

Area for Improvement 2: [Observation statement]

Reference**:** [List any relevant plans, policies, procedures, regulations, or laws.]

Analysis: [Provide a root cause analysis or summary of why the full capability level was not achieved.]