CYBER SECURITY PROGRAM

for Maine Water Systems & Utilities

CYBERSECURITY
LET'S ALL DO OUR PART

Brought to you by:

TOM'S Water Solutions

MWUA Maine Water Utilities Association Organized 1925

www.tomswatersolutions.com

www.mwua.org

Table of Contents

Brought to you by:

MWUA
Maine Water Utilities Association
Organized 1925

TOM'S
Water Solutions

This project was completed by Tom's Water Solutions LLC and Maine Water Utilities Association.

Acknowledgements:

The following organizations and individuals also contributed to the successful completion of these cybersecurity policies for the water industry in Maine. Without their support and input, this project would not have been possible.

- Maine Drinking Water Program
- University of Maine at Augusta, Maine Cyber Range
- Cybersecurity and Infrastructure Security Agency
- Susan Breau, Maine Drinking Water Program
- Dr. Henry Felch, University of Maine at Augusta
- Ryan Barnes, Cybersecurity and Infrastructure Security Agency
- Daisy Mueller, Cybersecurity and Infrastructure Security Agency
- Various water utilities and industry professionals across Maine

Must Read:

Prior to use and/or implementation of these policies, each policy should be thoroughly reviewed to ensure that they meet the utility's needs and unique considerations and environment. If changes, edits, or updates are required, they should be made before these policies are put into effect. Lastly, the policies should be frequently reviewed and updated to ensure that they remain accurate and effective for the utility.

Acceptable Use Policy

Overview and Purpose: This policy exists to define the acceptable and unacceptable uses of computer and other electronic equipment and resources (outlined under the Scope) at the [Utility Name].

Scope: The scope of this policy includes all, but is not limited to, computing, electronic, digital, informational, data-based, storage media, and process control/supervisory and control devices, software, and hardware. Also, the scope includes any other device or tool used in the execution and performance of work. These resources and devices fall under the purview of this policy whether owned, borrowed, or leased by the [Utility Name], the employee, or a third party. This policy further applies to all employees, management, board members, contractors, temporary staff, and other workers at the [Utility Name].

Policy: This policy is broken into the following sections: general guidelines and resource specific guidelines, which are further divided based on acceptable and unacceptable uses. While this policy and its guidelines are not exhaustive, it seeks to provide a structure for the use of the resources defined under the Scope.

General Guidelines: It is unacceptable to engage in illegal activities, whether local, state, federal, or international, while using the [Utility Name]'s resources. Private, sensitive, confidential, and/or proprietary information – such as Social Security numbers, medical records, and bank account details among others – must be handled with care. This information is owned by the [Utility Name] and may only be accessed, used, or shared when authorized and necessary to complete assigned job duties. If provided access to such information in error or by mistake, it is the employee's responsibility to notify management immediately. Further, lost or stolen information and data must also be reported as soon as possible.

Desktop, Laptop, and Other Computing Devices

✓ **Acceptable use(s):** Work-related activities may be carried out on work-owned desktops, laptops, and other computing devices as required by the task and/or approved by management. Approved activities are determined by an employee’s required job duties and may include, email and communications, administrative, financial, and regulatory reporting. The loss, theft, or unauthorized use of computing devices and resources must be reported to management as soon as possible. User identification, authentication, and authorization are further outlined in a separate policy.

🚫 **Unacceptable use(s):** Personal desktops, laptops, and other computing devices may not be used for work-related purposes. Work desktops, laptops, and other computing devices may not be used for personal purposes or other non-work-related activities. Tasks that do not require the use of computing devices should not be carried out on these devices.

Network Resources and Devices

✓ **Acceptable use(s):** Employees may make use of the [Utility Name]’s wired and wireless network technology for work-related purposes only as required by task, duty, and/or assignment. Passwords, firewalls, and other security measures must be enabled on all network resources and devices by trained staff members and/or contractors approved to do so. Such security processes must only be configured, altered, or terminated by appropriately designated individuals and approved by management.

🚫 **Unacceptable use(s):** All network resources and devices must be operated and maintained by trained staff members and/or contractors approved to do so. Employees without authorization must not make changes to these devices and resources unless directed to do so by management. These devices include, but are not limited to, routers, switches, wired connections, and wireless connections. Network security processes, credentials, and more must not be shared publicly or with any other non-work-related third parties unless approved by management or as required by law.

Cellphones and Other Mobile Devices

✓ **Acceptable use(s):** Work-related activities may be carried out on work-owned cellphones and other cellular devices as required by the task and/or approved by management. Passcodes and screen lock must be enabled on all devices used for work-related purposes. The loss, theft, or unauthorized use of such devices and resources must be reported to management as soon as possible.

🚫 **Unacceptable use(s):** Personal cellphones, personal cellular devices, and other non-work-owned cellular devices may not be used for work-related purposes. Work cellphones and work cellular devices may not be used for personal purposes or other non-work-related activities. Tasks that do not require the use of cellular devices should not be carried out on these devices.

Process Control and/or Supervisory, Control & Data Acquisition Systems

✓ **Acceptable use(s):** Process control systems (PCS) and/or supervisory control and data acquisition systems (SCADA) may be used by employees with proper authorization. Employees may monitor, operate, and manage the systems with the best interests of the [Utility Name] and its customers in mind, while following all training, laws, and standard operating procedures. PCS and SCADA systems must always be password protected, auto-logout and/or password protected screensaver enabled after 10 minutes of inactivity and have all unnecessary media ports disabled. In addition, the systems must be updated frequently and as soon as possible following the release of security patches, be segregated from all other non-PCS and/or non-SCADA networks and resources and be secured behind proper firewalls and virtual privacy networks (VPN) as appropriate. The systems' physical components must all be secured behind physically locked doors. When accessing the systems remotely (as applicable and if appropriate), only [Utility Name] owned devices and resources may be used to do so with two factor authentication and VPN(s) enabled. Only trusted networks and/or cellular connections may be utilized to access the systems remotely.

🚫 **Unacceptable use(s):** Only PCS and SCADA related tasks may be carried out on PCS and SCADA devices and resources. Personal or other non-PCS and/or non-SCADA work-related tasks may not be carried out on these devices and resources. This list of unacceptable activities includes, but is not limited to, email and communications, administrative, financial, social media, and gaming. Downloading or installing unapproved software and connecting unapproved hardware to the systems is prohibited. Only approved maintenance technicians and/or administrators may download, install, connect hardware, and otherwise alter the systems and their functionality and/or operation. Employees must have distinct logon credentials, including usernames and passwords, and must not share these with other colleagues or outside parties. Employee credentials must be terminated upon the employee's separation from the [Utility Name] immediately and not reused for any other employee or purpose. When accessing the systems remotely (as applicable and if appropriate), public and other non-trusted networks may not be utilized. Such un-trusted networks may be found at, but are not limited to, cafés, hotels, restaurants, sporting venues, and other non-password protected network locations.

Email and Communications

Please see the email and communications policy.

Social Media

✓ **Acceptable use(s):** Employees may use social media on the [Utility Name]'s resources for work purposes when directed by management or when carrying out work related duties as assigned. The use of social media must be in the best interests of the [Utility Name] and reflect organizational beliefs and/or opinions only. All laws must be followed when using social media and releasing any information publicly.

🚫 **Unacceptable use(s):** Employees may not use the [Utility Name]'s resources for personal social media or other non-work-related purposes. Further, employees shall not use personal devices and resources for work-related social media tasks and must refrain from personal social media activities during working hours and while on work premises. Confidential, private, and/or sensitive information about the [Utility Name] or its customers must never be released on social media. When using social media for work purposes, employees must never reflect personal beliefs and/or opinions.

Clean Desk Policy

Overview and Purpose: As confidential and sensitive information, documents, and resources can easily fall into the wrong hands either accidentally or intentionally, it is in the best interests of the [Utility Name] to secure it when not in use. This policy stipulates the procedures associated with removing and securing such content from unattended desks and digital workstations or computer desktops.

Scope: The scope of this policy includes all [Utility Name] employees, their workstations, and digital computer desktops and devices.

Policy: Employees must remove all information, documents, resources, and materials that are of a confidential, sensitive, and/or critical nature from their desks and publicly accessible workstations at the end of the workday or when absent for any extended period of time (time determined by management). If an employee is unsure about the status of the materials in question, prudence and caution should be followed. This includes any materials or resources that would otherwise be damaging to the [Utility Name] or its customers should they be lost or stolen.

An example list of such materials includes, but is not limited to, account information, financial data, usernames and passwords, employee data, customer data, and the [Utility Name]'s operations.

The following is a list of supplemental procedures to ensure a clean desk and workstation:

1. Materials and resources removed from desks and/or workstations should be secured in locked drawers, locked cabinets, and/or behind locked doors where unauthorized parties are unable to access.
2. Locked drawers, cabinets, and rooms (secured locations) must remain locked and secured when not in use.
3. Keys, passwords, and/or other tools used to access secured locations must not be left unattended and should also be stored securely.

4. Bulletin boards, whiteboards, and other notice boards should not contain information or materials of a sensitive, confidential, and/or otherwise damaging nature. This includes network information, such as Wi-Fi password and user account information.
5. Usernames, passwords, and other digital authentication information must not be kept on paper, sticky notes, or otherwise in visible locations. Passwords that are stored in a hard copy form must be secured at all times. Please note that hiding notes under other desktop items is not secure storage.
6. When printing and faxing, information and documents should be retrieved from the printer immediately and as soon as possible.
7. Documents of a sensitive and/or confidential nature should be shredded immediately or placed in official locked secure disposal bins when no longer needed.
8. All media devices including, but not limited to, CDROM, DVD, USB drives, hard drives, and backup devices, should be treated as confidential and sensitive materials and stored in secured locations when not in use. Hard copies, floppy disk, CD's, DVD's, USB drives and any other device or tool containing sensitive information must be removed from the desk and locked in a drawer when unattended and at the end of the workday.
9. As with physical desktops, digital desktops on computers must also be kept clean and secured. Confidential and sensitive information and/or data should not be stored on publicly accessible workstations, employees' computer desktops, or in otherwise easily seen and/or accessible locations.
10. Network information and data including, but not limited to, Wi-Fi passwords and account information, should be stored in secured locations when not in use. Such information and data should be treated with utmost care and not shared with outside parties.
11. Keys used for accessing restricted areas or sensitive information must not be left unattended.
12. File cabinets containing sensitive information must remain closed and locked when not in use.
13. Paper documents generated by printers and fax machines should be retrieved as soon as they are printed.
14. Whiteboards and blackboards must be erased after use.

Data Backup Policy

Overview and Purpose: Because the [Utility Name] maintains data critical for continued operations and business, this policy exists to ensure a backup copy of the data is available in the event of an accident or intentional incident resulting in loss or corruption. The importance of backups, a proper backup schedule, and backup procedure are of high importance. This policy covers what data should be backed up, the processes to follow, and how to keep it secure.

Scope: The scope of this policy includes all [Utility Name] employees and any device used for work-related purposes with storage media and/or storage capabilities. This includes, but is not limited to, computers, USB drives, hard drives, and other storage media.

Policy: The following sets a baseline backup policy and set of associated procedures; however, additional policies and/or procedures may be necessary depending on the situation and data to be backed up.

1. In general, all data used for business purposes should be backed up including data files, databases, programs, and software. It may be necessary to backup different types and categories of data separately. For example, sensitive and/or confidential information may be required to be backed up separately and following different procedures than those for data of a less critical nature. The list of data to backup may be categorized into the following, but is not limited to, operations and maintenance, monitoring, reporting, financials, administrative, management, customer, and human resources.
2. A minimum of two backup copies of data should be maintained: one for restoration purposes and another for redundancy. The two backups should be stored in two separate offsite (in case of structure fire, etc.) locations either physical or digital (cloud-based) as appropriate and determined by management.
3. Process control system (PCS) and supervisory control and data acquisition (SCADA) backups should be backed up and stored separately from all other backups. It is recommended to maintain a spare PCS and/or SCADA system complete and capable of fully restoring operations following loss events, especially when unable to operate and

monitor systems manually. Such spares should be securely stored away from all unauthorized parties, whether employee or otherwise, and behind locked door(s). The secured location should be temperature and humidity controlled as well as resilient to other natural and manmade hazards.

4. Backups should occur weekly or as determined by management and are created from a full copy of all data on the relevant host or set of hosts.
5. Backups should be performed by appropriately trained and management designated employees, software and/or systems, and/or other third parties.
6. Should any host – or set of hosts – to be backed up be compromised, or suspected of compromise, the backup should be postponed or halted as determined by management until such a time where the host(s) can be cleared of any and all compromise(s). This includes, but may not be limited to, malware, ransomware, spyware, and viruses.
7. Backup and restoration capabilities should be tested and exercised periodically, at least once every six months, to ensure that backups and their procedures remain viable. Testing should only be performed by an authorized individual with proper credentials, knowledge, and approved by management.

Email Communications Policy

Overview and Purpose: Email offers many benefits to the [Utility Name], including communication efficiency and customer contact among others. However, there are also cybersecurity threats that utilize email and a lack of awareness to exploit targets. In addition, the misuse of email by employees, staff, and others can lead to further issues and threats. Therefore, the [Utility Name] places an importance on employee email best practices and awareness training to ensure that email and communications are carried out appropriately and safety with the best interests of the [Utility Name] in mind.

Scope: The scope of this policy includes all [Utility Name] employees and any device used for work-related purposes. This also includes all [Utility Name] email accounts.

Policy: It is important to note that when using email, such an act connects the user to the outside world, third parties, and the Internet. Threats and hazards are not as easily controlled as within the [Utility Name]. Therefore, all employees, staff, and stakeholders acting on behalf of the [Utility Name] must understand that email offers benefits and risks. The following lists the set of policies applying to email communications:

1. Only employees, staff, stakeholders, and others authorized to use and access the [Utility Name]'s email may do so. Using email must be for work-related purposes only and always carried out with the best interests of the [Utility Name] and its customers in mind.
2. Using and accessing personal or otherwise email unrelated to work on devices connected to the [Utility Name]'s network, servers, and/or devices is prohibited without authorization.
3. The use of email must comply with all laws, regulations, rules, and the [Utility Name]'s applicable policies, procedures, and ethical code(s) of conduct.
4. Creating new email accounts must be carried out by trained and appropriately authorized parties. Only email systems and storage servers approved by management may be used to create new email accounts. Similarly, deleting and terminating email accounts must only be carried out by trained and appropriately authorized parties.

5. Email account addresses, usernames and passwords must follow the Password Policy.
6. It is prohibited to forward any work-related email to personal email accounts and/or systems or third parties not authorized to receive the email.
7. When receiving email, all users must be appropriately wary of the sender, the content, and any attachments. The user must first ensure the identity of the sender is accurate and as displayed, the content is appropriate and not misleading, and the attachments are safe before opening, downloading, forwarding, and/or using for other purposes.
    a. Identifying the sender can be carried out by, but is not limited to, checking to ensure the name and actual email address match the expected individual or entity. If there are concerns, the user should proceed no further with the email and refrain from forwarding or sending it and any content and attachments without first consulting with management and appropriately trained parties.
    b. When reviewing the content of the email after first checking the identity of the sender, users should scan for flags that the email has been compromised, check to ensure that the content matches what is expected from the sender, and review for any unexpected signs. Signs that should raise flags include, but are not limited to, spelling and/or grammar errors and inappropriate content among others.
    c. Finally, attachments should always be treated as potentially dangerous. Only attachments from properly identified senders should be opened, downloaded, forwarded, and/or used for other purposes. If able, all attachments should be scanned for threats prior to opening, downloading, and/or forwarding. Executable files must not be opened, downloaded, and/or forwarded expect by authorized and appropriately trained parties.

External & Removable Media Policy

Overview and Purpose: Although external and removable media, including but not limited to USB drives, SD cards, CDs, mobile phones, smart devices, and their relevant ports on assets and devices offer convenience for storage and transfer of data, they also present unique security concerns. As noted in the Physical Security Policy, the physical security of assets impacts their cybersecurity. This is never more apparent than with external and removable media.

More specifically, portable media are pieces of hardware that may contain, transfer, or expose assets to security risks. It is important to extend the same protections one would utilize in the real world when dealing with external and removable media. For example, most would not accept an unknown package from a stranger in public without knowledge of what is contained within, where it has been, and what it has been exposed to. The same concern and guard also applies to external and removeable media.

Scope: The scope of this policy includes all the [Utility Name]'s Information Technology (IT) assets, including but not limited to, computers, Supervisory, Control, and Data Acquisition (SCADA) systems, networking devices, and mobile devices as well as all external and removable media and their relevant ports on the [Utility Name]'s IT assets.

Policy: The following sets forth the External and Removable Media Policy:

1. External and removable media ports on devices that do not require their use should be disabled, especially on SCADA and Process Control System (PCS) assets as well as all devices that connect physically or logically to them. For those that require occasional use, the ports can be disabled and enabled on an as needed basis. It is also recommended that ports – when not in use – utilize safety/dust plugs to prevent unintended use.
2. For devices that require more frequent use of external and removable media, special consideration should be taken to ensure the device is not exposed to risk. Specifically, external and removable media from an unknown source or location should be treated

the same as media known to contain malware, viruses, or other security concerns. These external and removable media should never be connected to any device or asset at the [Utility Name].

3. External and removable media that is found – whether in public or at the [Utility Name] and regardless of labeling – should be turned over to the [Utility Name]’s IT department or responsible staff for proper disposal.
4. External and removable media owned by the [Utility Name] should be properly labeled and secured in a locked cabinet, drawer, or other similarly secured location when not in use. These media devices should also be encrypted, password protected, cleared of all critical and sensitive data when not in use, and properly disposed of by trained staff when no longer needed.
5. All assets and devices at the [Utility Name] should employ antivirus software and data blockers as well as disabling autorun, autoplay, and automatic downloads from removable and external media.
6. When possible, cloud transfer solutions approved and properly vetted by utility leadership should be employed instead of external and removable media.

Information Sharing & Collaboration Policy

Overview and Purpose: Sharing information and collaborating on cybersecurity is in the best interest of the [Utility Name]. Not only does collaboration offer the [Utility Name] advantages in mutual aid during cybersecurity events and emergencies, but it also promotes a culture of awareness at the utility. It should also be noted that many cybersecurity tools, such as antivirus, rely on information sharing to work effectively. For example, when new malware or viruses are found, antivirus software is updated across the world to include protections against it. Without a report from the first victim, others cannot be effectively secured against the threat. Beyond sharing information, receiving assistance and reports at the [Utility Name] also assists in protecting the [Utility Name]'s critical assets.

Scope: The scope of this policy applies to all utility staff.

Policy: The following sets forth the Information Sharing and Collaboration Policy:

1. The [Utility Name] should be a member of and active participant in the Maine Water and Wastewater Agency Response Network (WARN).
2. The [Utility Name] should develop mutual aid agreements with neighboring utilities and other partners that are able to offer assistance in the event of a cybersecurity incident or other emergency.
3. The [Utility Name] should gather and distribute details of relevant security incidents and events from utility partners and other relevant organizations to internal staff to promote awareness and cybersecurity at the utility. The internal reports should be provided on a regular basis determined by utility leadership and immediately following any critical event or report that may impact the [Utility Name]'s critical assets.
4. All cybersecurity incidents should be reported and shared with utility partners, such as WaterISAC, Cybersecurity Infrastructure Security Agency (CISA), Maine Information and Analysis Center (MIAC), Environmental Protection Agency, Drinking Water Program, federal and/or state authorities, and other mutual aid partners. Reporting should only be performed by staff designated by utility leadership.

5. All cybersecurity incidents should be reported as legally required. The [Utility Name]'s legal counsel should be consulted with questions and prior to any report.
6. Reports should only be shared by staff designated by utility leadership. Critical, sensitive, and confidential information should not be shared without consultation and approval from utility leadership and the [Utility Name]'s legal counsel.

Offboarding Policy

Overview and Purpose: IT assets no longer in use can pose substantial risk to the [Utility Name]. Thus, when assets are no longer required, they should be removed from service as soon as possible. Concurrently, employees separated from the [Utility Name] must be similarly treated in that the separated employee's access to systems should be terminated immediately and all assets returned to the [Utility Name] promptly. Properly off-boarding both IT assets and employees can reduce the [Utility Name]'s vulnerabilities and risk.

Scope: The scope of this policy includes all the [Utility Name]'s employees and any individual or entity with access to the [Utility Name]'s electronic and digital infrastructure and/or resources. The scope further includes all of the [Utility Name]'s devices, hardware, software, and any other digital or IT resources.

Policy: The following sets forth the Off-Boarding Policy:

1. **Assets**
   a. It is a best practice to maintain an asset management program to ensure all assets are tracked. The program allows the [Utility Name] to remain informed about assets that may require maintenance, updates, patches, removal from service, and more. IT infrastructure and other digital assets should be included in the asset management program.
   b. An audit procedure – carried out at management-set intervals during the year – of the asset management program should be employed to ensure assets are not lost, misplaced, or forgotten. The audit procedure should also review employee access.
   c. When assets are no longer needed, they should be promptly removed from service. These assets include, but are not limited to, computers, printers, software, backups, other electronic devices, and IT infrastructure. It is of crucial importance that all devices with storage capabilities are included. Removal from service may include, but is not limited to:
      i. Backup of needed information and data,

        ii. Disconnection from the [Utility Name]’s IT infrastructure, networks, servers, and other related processes,
        iii. Deletion and/or wiping of stored media,
        iv. Resetting to factory conditions,
        v. Removal and/or destruction of storage media,
        vi. Proper disposal and/or destruction of the asset. Proper disposal and/or destruction methods may depend on the asset and management guidelines.
    d. Only individuals with authorization and proper expertise should carry out the steps to remove assets from service. All steps taken and carried out should be noted in the [Utility Name]’s asset management program.

2. **Employees** (and others with access to the [Utility Name]’s assets)
    a. The above-mentioned asset management program should include and track details about access and assignment of assets to employees and other third parties to allow the [Utility Name] to ensure only individuals with authorization maintain possession of and access to such assets.
    b. Employees separated from the [Utility Name], whether voluntarily or involuntarily, should have their physical and logical access to the [Utility Name]’s assets terminated immediately.
        i. Termination of physical access may include, but is not limited to:
            1. Returning or confiscation of assigned assets,
            2. Returning or confiscation of ID badges, keys, and other physical access controls,
            3. Returning of utility branded clothing, business cards, and other branded materials such as letterhead and cardstock,
            4. Removal from the premises as required,
            5. Notification of separated status to other employees and parties with the need to know.
        ii. Termination of logical access may include, but it not limited to:
            1. Termination of access, authorization, accounts, and authentication, such as accounts, usernames, passwords, and other related credentials to all internal and external devices, systems, software and programs, and more,
            2. Modification or termination of any shared access or credentials. It is important to note that sharing access controls and credentials is not recommended.

c. Only individuals with authorization and proper expertise should carry out the steps to terminate access. All steps taken and carried out should be noted in the [Utility Name]’s asset management program.

Password Policy

Overview and Purpose: Passwords are important for protecting the [Utility Name]’s assets, IT resources, and data against unauthorized access, attack, and/or damage. Simple and weak passwords open the [Utility Name] to additional risks and threats. Therefore, strong passwords are key as well as following password best-practices.

Scope: The scope of this policy includes all the [Utility Name]’s employees and any individual or entity with access to the [Utility Name]’s electronic and digital infrastructure and/or resources. The scope further includes all of the [Utility Name]’s devices, hardware, software, and any other resource that can be password protected.

Policy: The following sets forth the Password Policy:

1. All devices and resources with the ability to be password protected must be password protected. Devices without the ability to be password protected should be avoided.
2. All default passwords should be changed immediately, including employee passwords or manufactory passwords.
3. Passwords must not be shared internally or externally at the [Utility Name], and all staff must maintain unique passwords separate from any other staff member.
4. Staff with access to critical systems, including but not limited to Process Control Systems (PCS), Supervisory, Control, and Data Acquisition (SCADA) systems, and Business Critical Systems (BCS), must not share or reuse passwords. Each staff member with access to these systems must maintain unique and distinct passwords and other authentication details from any other staff member. When accessing critical systems, all staff must utilize their own unique credentials and passwords to do so and must not utilize any other credentials. Furthermore, multi-factor authentication must be enabled – in addition to passwords – for all critical systems as determined by management.
5. Passwords must be strong:
    a. Default passwords must be changed as soon as possible.
    b. Passwords should be at least 16 characters in length. It is recommended to set passwords longer than 16 characters when possible.

c. Passwords should be as random as possible. Randomizing a password includes mixing a string of upper-case, lower-case, numbers, and symbols together. **<u>Password123!</u>** is an example of a poor password, while **<u>EG^JH#@cP^o3IVM1</u>** is an example of a strong password.

d. Passwords should not contain any identifiable information, including but not limited to, usernames, family names, dates of birth, and more.

e. Passwords should not contain any easily guessable details, including but not limited to, song lyrics, famous quotes, popular travel destinations, and more.

f. Each account should have a different password.

6. Because strong passwords may be difficult to remember, it is recommended that the [Utility Name] make use of password managers. This will allow the use of strong passwords, unique passwords for all accounts and for all users, and the ability to easily recall passwords when needed. Password manager best-practices should always be followed.
7. Passwords must be adequately encrypted by properly trained individuals as determined by management. Passwords must also not be stored in clear text and reversible formats.
8. Passwords should only be changed or altered if the user has reasonable suspicion of password compromise.
9. Accounts should be monitored for suspicious activity, and if suspicious activity is suspected or proven, the password(s) must be changed immediately.
10. Passwords and other authentication data must be terminated immediately upon a staff member's separation from employment or other parties' separation from affiliation with the [Utility Name].
11. Staff should be periodically trained (every 6 months) on password hygiene and best-practices.

Patches and Updates Policy

Overview and Purpose: Patches and updates, including security updates, for devices, hardware, and software offer defenses against known vulnerabilities and threats. Typically, when a vulnerability is found, either through testing or experience, a patch and/or update is developed and released to mitigate and/or eliminate the vulnerability. It is important to note that this typically only applies to known vulnerabilities. Therefore, patching and updating devices, hardware, and software used for the [Utility Name]'s work-related purposes or those connected to the [Utility Name]'s network, systems, devices, hardware, and/or software are of critical importance. Unpatched and outdated devices, hardware, and software can create holes in the security of any system.

Scope: The scope of this policy includes all of the [Utility Name]'s employees, devices, hardware, software, and any other resource that can be patched and/or updated. Patches and updates apply to many resources, and they are not limited to smartphones, mobile phones, tablets, laptop computers, desktop computers, other computing devices, and the software on such resources. In addition, network hardware and software, process control systems (PCS) and/or supervisory control and data acquisition (SCADA) systems and their hardware and software, and printers among other resources are also included.

Policy: The following list sets forth the Patches and Updates Policy:

1. Patching and updating systems, devices, hardware, and/or software should only be carried out by properly trained and authorized parties approved by management.
2. Patches and updates, especially urgent security patches and updates, should be implemented as soon as possible following release even if it falls outside of the normal patch and update cycle. It is best practice to implement them immediately, but under no circumstances should a security patch or update be delayed more than one week.
3. As determined by management and trained information technology (IT) staff and/or authorized contractors, security patches and updates should be set to be performed automatically on all systems, devices, hardware, and software. It is recommended that

non-security patches and updates also be set to automatic, but they should never be delayed more than one week unless approved by management as appropriate.

4. It is best practice to track all resources outlined in the scope above through asset management to maintain records when patches and updates are performed and when they should be implemented. Such a practice may also be used to identify outdated and/or vulnerable resources that should be removed from service.
5. Patching and updating PCS and SCADA systems may require additional considerations, and properly trained and authorized parties should always be consulted when performing maintenance on such systems. Depending on the skills and authorization of staff, it may be required to have outside and/or third-party contractors and/or vendors perform patches and updates on PCS and SCADA systems. Such external parties should always be vetted, trusted, and approved by management.

Physical Security Policy

Overview and Purpose: The physical security of a utility is important in its own right but also for the role it plays in ensuring the cybersecurity of the utility. More specifically, physical security and cybersecurity go hand in hand and the neglect of one or the other may lead to the breakdown of both. Although cybersecurity often exists in the “digital” realm, most assets exist – at least in part – physically and, as a result, require physical security considerations.

Scope: The scope of this policy includes all of the [Utility Name]’s physical premises and assets, as well as all staff and individuals with access to these locations and assets.

Policy: The following sets forth the Physical Security Policy:

1. As noted in other policies, the principle of least privilege (if one does not need access, they should not have access) should also be applied to physical security. If an individual – whether staff, contractor, or other third party – does not need physical access to the premises, a specific location, or an asset critical to the cybersecurity of the [Utility Name], they should not be given access.
2. In addition, to secure physical locations and assets through the principle of least privilege, all buildings and structures containing assets critical to the [Utility Name]’s cybersecurity should be physically protected by non-technical barriers, including but not limited to, fences, gates, barricades, locked doors, photo identification and ID cards, and metal bars as needed and deemed necessary by utility leadership.
3. Furthermore, it is a best practice that all critical, physical locations and structures be protected and monitored by security cameras, intrusion detection systems, motion detectors, guards, and fire and smoke alarm systems. A culture of physical security should also be promoted among staff so that staff remain on guard against physical intrusion and suspicious individuals, situations, or events are noticed and reported to utility leadership as soon as possible.
4. Within the [Utility Name]’s premises and structures, assets critical to the cybersecurity of the utility should be protected behind locked doors and/or cabinets. As noted before, if an individual does not need access, they should not be provided access and this

extends to all locations and assets within physical structures as well. Networking devices and cables should not be neglected and should also be protected by locked doors and/or cabinets. Lastly, the keys, passwords, and any other means of authentication should be similarly protected by the principle of least privilege, must not be left unattended, and should be stored securely.

5. Please see the External and Removable Media and the Clean Desk Policies for further details on the physical security of assets and premises.

Preparedness, Response & Recovery Policy

Overview and Purpose: As outlined by the United States Environmental Protection Agency, utilities should follow the “prepare, respond, and recover” process in relation to emergencies that include both natural and man-made threats. The “all-hazards” approach to categorizes hazards into three categories: natural, man-made, and cyber threats. Natural hazards include fire, floods, storms, and more, while man-made threats include, but are not limited to, vandalism, theft, and terrorism. Further refining the man-made threats results in the third and final category. Properly preparing for, responding to, and recovering from cyber threats allows utilities to increase their cyber resilience.

Scope: The scope of this policy includes all the plans, procedures, and processes at the [Utility Name] in relation to preparing for, responding to, and recovering from cyber hazards.

Policy: The following sets forth the Preparedness, Response, and Recovery Policy:

1. Preparation: Preparing for cyber emergencies includes, but is not limited to, assessing risk, developing an emergency response plan (ERP), training staff and stakeholders, and implementing other preventative and mitigation measures.
    a. Assessing risk: To properly assess cyber risk to the [Utility Name], a Risk Resiliency Assessment (RRA) following relevant standards should be completed considering all hazards. Prior to the development of the RRA, the [Utility Name]’s tolerance for risk should be determined and utilized in the development of the RRA. Determination of applicable hazards and vulnerabilities is also crucial as well as identifying critical assets utilized in completing the [Utility Name]’s mission critical goal. The basic steps to develop an RRA include:
        i. Threat-asset pairing: Pair threats with critical assets.
        ii. Risk calculation: Calculate risk by considering the consequences and likelihood of the threat, as well as the vulnerability of the relevant asset.
        iii. Risk categorization and prioritization: Categorize and prioritize risks based on their final risk values to utilize in future preparation steps.

   b. Developing an ERP: Utilizing the output of the RRA, an ERP should be developed. An ERP is a comprehensive plan that provides information, guidance, and assists in incident response and recovery. As such, an ERP should layout basic information about the [Utility Name], internal and external contact information, system and process details, a collection of procedures to follow in the event of common hazards, and relevant resources.
   c. Training: See the Cyber Awareness Training Policy.

2. Response: Responding to cyber emergencies begins with the development of a cyber incident response plan (IRP). It is a best practice that an IRP be developed as a standalone document and supplemental to an ERP. Although an ERP includes content and response procedures related to common cyber incidents, an IRP supplements the ERP by laying out more specific response procedures and processes for cyber incidents. The IRP opens with identification of the incident response team and other stakeholders, which may include internal and external parties, before laying out steps following the National Institute of Standards and Technology's incident response lifecycle: preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.
3. Recovery: Recovering from cyber emergencies begins with the development of a cyber disaster recovery plan (DRP), which may be a standalone document or contained as a section within an ERP. Similar to the IRP, a DRP supplements an ERP by further refining recovery steps for cyber incidents. The goals of the DRP include, but are not limited to, mitigating losses, ensuring services and business can continue uninterrupted, and eventually returning all devices and systems to normal.
4. All plans, procedures, and processes should be reviewed frequently – at least once per year – and kept up to date. The documents should be included in relevant training programs and provided to staff and external parties in an as-needed manner considering the sensitive and confidential nature of the information. Drills, tabletop exercises, and full-scale exercises are examples of ways to train on and maintain the plans, procedures, and processes.

Remote Access Policy

Overview and Purpose: Remote access to the [Utility Name]’s systems and resources offers a number of benefits to productivity and efficiency, but also poses potential security vulnerabilities. Therefore, this policy sets out to define the proper processes and procedures for accessing the [Utility Name]’s systems and/or resources when offsite and/or remotely.

Scope: The scope of this policy includes all the [Utility Name]’s employees and any individual or entity with remote access authorization to any of the [Utility Name]’s systems and/or resources. Such resources may include, but are not limited to, servers, computers, process control systems (PCS) and/or supervisory control and data acquisition (SCADA) systems, and printers among others.

Policy: Only employees and vendors or contractors authorized by management may access systems and/or resources remotely. If remote access is not needed to complete a task, remote access should not be used. When needed as described previously, remote access should always be in the best interests of the [Utility Name] and its customers. Because remote access can open holes and vulnerabilities into the [Utility Name]’s systems and resources, access to such systems and resources must be given the same security consideration, if not higher as appropriate, as on-site connection(s).

1. Only employees, vendors, and contractors approved by management and properly trained may access the [Utility Name]’s systems and/or resources remotely.
2. Remote access may only be utilized through a known, trusted, and secure connection that is under the complete control of the authorized party or another authorized party or entity. Public networks, especially those without passwords, must never be used to access systems and resources remotely. It is a best practice for management to provide authorized employees with a list of trusted networks and/or connections. Only the connections and/or networks on the list may be utilized.
3. Remote access must make use of encryption as determined by management and properly trained and authorized information technology (IT) staff and/or contractors.

4. Remote access must make use of strong usernames and passwords as outlined by policy, procedure, and management. Authentication information, including usernames and passwords, must be protected from other parties, including, but not limited to, colleagues, friends, family members, and strangers. Login credentials co-worked, friends, family, or other unauthorized parties.
5. Multi-factor authentication should always be implemented for all remote access. It is also a best practice to make use of an approved virtual privacy network (VPN) to access systems and/or resources remotely.
6. Only [Utility Name] owned resources may be used to remotely access systems and resources. Personal or other non-[Utility Name] owned resources may not be used for remote access. It is a best practice for management to provide a list of approved resources for remote access, and only resources on this list may be utilized for this purpose.
7. All resources used for remote access must have the latest updates and security patches implemented, as well as anti-virus software as appropriate and determined by management.
8. When accessing systems and/or resources remotely, authorized individuals must always be wary of their surroundings and all onlookers. Remote access may only be utilized in private and physically secured locations where third parties are unable to oversee.
9. When accessing systems and/or resources remotely, authorized individuals must always ensure that they have disconnected from all unknown, untrusted, and insecure connections and/or networks.
10. All resources used for remote access must have auto-screensaver enabled after 10 minutes of inactivity. It is also a best practice to implement auto-factory reset on such resources after incorrectly entering a password, pin, and/or passcode incorrectly 10 times in a row as appropriate. In addition, for mobile devices, strong passcodes are required, and all devices must not be left unattended.
11. When finished accessing systems and/or resources remotely, authorized individuals must disconnect and/or logout from remote access immediately.

Security Awareness Training Policy

Overview and Purpose: Although the implementation of technical security measures is important in all cybersecurity programs, most incidents target people. Even those that are complex and technical in nature also often stem from people. Therefore, it is important to pair technical processes and procedures with cybersecurity awareness training. This policy sets out the scope, timing, and content of such training.

Scope: The scope of this policy includes all the [Utility Name]'s employees and any individual or entity with access to the [Utility Name]'s electronic and digital infrastructure and/or resources.

Policy: The following sets forth the Security Awareness Training Policy:

1. All new employees, and other parties with access to the [Utility Name]'s electronic and digital infrastructure and/or resources, must be trained by a program approved by management within 60 days. The first program must be at least 2 hours in length and focus on threats, vulnerabilities, and best practices to ensure security at the [Utility Name] and for its customers.
2. A list of training programs approved by management should be created and distributed to all employees, and other parties with access to the [Utility Name]'s electronic and digital infrastructure and/or resources. The list should be updated and reviewed frequently by management.
3. All employees, and other parties with access to the [Utility Name]'s electronic and digital infrastructure and/or resources, must participate in ongoing training throughout their duration with the [Utility Name]. Following the first training, the above-mentioned individuals must take another training every 6 months. These training programs must be at least 1 hour in length, but it's recommended that they be longer. Different training programs should be prioritized each 6-month period, and individuals may only retake programs when approved by management.

4. Every two years, all employees, and other parties with access to the [Utility Name]’s electronic and digital infrastructure and/or resources, must retake the original 2-hour training previously taken.
5. Following any cybersecurity incident or breach, all employees, and other parties with access to the [Utility Name]’s electronic and digital infrastructure and/or resources, must participate in a 2-hour security awareness training program focusing on the incident(s) that occurred. If one or multiple employees are to blame for the incident, they should not be singled out and forced to take the training alone. These individuals’ names and identities should be kept confidential, and all employees should be trained.
6. Employees and other parties with access to the [Utility Name]’s electronic and digital infrastructure and/or resources should be encouraged to maintain their cybersecurity awareness through training apart from mandatory training as well. Incentives and other benefits can be offered to promote additional training.

Subcontractor, Supply Chain & Vendor Policy

Overview and Purpose: The statement that “a chain is only as strong as the weakest link” has become one of the most frequently used sayings in the world of cybersecurity. If the [Utility Name] secures itself against all threats without consideration for those stemming from the supply chain, the weakest link in the cybersecurity chain will be exposed and break the entire program. Therefore, the [Utility Name] should implement security controls to protect against supply chain threats, including but not limited to, software vulnerabilities, data breaches, implanted backdoors, and more.

Scope: The scope of this policy includes all the [Utility Name]’s contractors, subcontractors, vendors, and other third parties with physical or logical access to utility premises and assets as well as all newly purchased or acquired Information Technology (IT) assets and the companies from which they stem.

Policy: The following sets forth the Subcontractor, Supply Chain, and Vendor Policy:

1. All new contractors, subcontractors, and vendors should be properly vetted prior to being given access to the utility’s premises and critical assets. Vetting should also be carried out on vendors prior to purchase and connection of new IT assets and devices to the utility’s systems and infrastructure. In addition, vetting should include background checks that follow the utility’s background check policy.
2. Please see the Physical Security Policy.
3. Physical and logical access to the utility should follow the principle of least privilege.
4. All requests for proposals, quotes, and contracts should include security considerations and terms for the management of contractor, subcontractor, vendor, and supply chain security. These third parties should be required to adhere to minimum cybersecurity as determined by leadership and legal counsel.
5. All contractors, subcontractors, and vendors should be properly identified prior to being given access to the physical premises and assets. Further, these third parties should always be accompanied by utility staff when physically onsite.

6. Utility staff should be trained to recognize and report unauthorized changes, alterations, and inconsistencies to the utility’s physical and logical assets.
7. When a contractor, subcontractor, vendor, or other third party no longer requires access to physical or logical premises and assets, their access should be terminated immediately. This includes the return of all identification, IDs, and keys.
8. Existing contractors, subcontractors, and vendors should be periodically vetted to ensure that they continue to remain secure against threats to the utility. In addition, new and existing contracts and agreements should be reviewed to ensure that cyber events or incidents caused or triggered by contractors, subcontractors, and/or vendors are addressed properly.

Appendix

Must Read:

Prior to use and/or implementation of these policies, each policy should be thoroughly reviewed to ensure that they meet the utility's needs and unique considerations and environment. If changes, edits, or updates are required, they should be made before these policies are put into effect. Lastly, the policies should be frequently reviewed and updated to ensure that they remain accurate and effective for the utility.

References:

The documents, reports, and templates below served as reference material in the development of these cybersecurity policies.

- WaterISAC's 12 Cybersecurity Fundamentals for Water and Wastewater Utilities
- WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- NIST's Cybersecurity Framework: Policy Template Guide
- CISA's Cross-Sector Cybersecurity Performance Goals Report
- SANS' Security Policies Templates

CYBER SECURITY POLICIES

for Maine Water Systems & Utilities

CYBERSECURITY

LET'S ALL DO OUR PART

Brought to you by:

TOM'S Water Solutions

MWUA Maine Water Utilities Association Organized 1925

www.tomswatersolutions.com

www.mwua.org

Table of Contents

Brought to you by:

MWUA
Maine Water Utilities Association
Organized 1925

TOM'S
Water Solutions

This project was completed by Tom's Water Solutions LLC and Maine Water Utilities Association.

Acknowledgements:

The following organizations and individuals also contributed to the successful completion of these cybersecurity policies for the water industry in Maine. Without their support and input, this project would not have been possible.

- Maine Drinking Water Program
- University of Maine at Augusta, Maine Cyber Range
- Cybersecurity and Infrastructure Security Agency
- Susan Breau, Maine Drinking Water Program
- Dr. Henry Felch, University of Maine at Augusta
- Ryan Barnes, Cybersecurity and Infrastructure Security Agency
- Daisy Mueller, Cybersecurity and Infrastructure Security Agency
- Various water utilities and industry professionals across Maine

Must Read:

Prior to use and/or implementation of these policies, each policy should be thoroughly reviewed to ensure that they meet the utility's needs and unique considerations and environment. If changes, edits, or updates are required, they should be made before these policies are put into effect. Lastly, the policies should be frequently reviewed and updated to ensure that they remain accurate and effective for the utility.

Acceptable Use Policy

Overview and Purpose: This policy exists to define the acceptable and unacceptable uses of computer and other electronic equipment and resources (outlined under the Scope) at the [Utility Name].

Scope: The scope of this policy includes all, but is not limited to, computing, electronic, digital, informational, data-based, storage media, and process control/supervisory and control devices, software, and hardware. Also, the scope includes any other device or tool used in the execution and performance of work. These resources and devices fall under the purview of this policy whether owned, borrowed, or leased by the [Utility Name], the employee, or a third party. This policy further applies to all employees, management, board members, contractors, temporary staff, and other workers at the [Utility Name].

Policy: This policy is broken into the following sections: general guidelines and resource specific guidelines, which are further divided based on acceptable and unacceptable uses. While this policy and its guidelines are not exhaustive, it seeks to provide a structure for the use of the resources defined under the Scope.

General Guidelines: It is unacceptable to engage in illegal activities, whether local, state, federal, or international, while using the [Utility Name]'s resources. Private, sensitive, confidential, and/or proprietary information – such as Social Security numbers, medical records, and bank account details among others – must be handled with care. This information is owned by the [Utility Name] and may only be accessed, used, or shared when authorized and necessary to complete assigned job duties. If provided access to such information in error or by mistake, it is the employee's responsibility to notify management immediately. Further, lost or stolen information and data must also be reported as soon as possible.

Desktop, Laptop, and Other Computing Devices

✓ **Acceptable use(s):** Work-related activities may be carried out on work-owned desktops, laptops, and other computing devices as required by the task and/or approved by management. Approved activities are determined by an employee's required job duties and may include, email and communications, administrative, financial, and regulatory reporting. The loss, theft, or unauthorized use of computing devices and resources must be reported to management as soon as possible. User identification, authentication, and authorization are further outlined in a separate policy.

🚫 **Unacceptable use(s):** Personal desktops, laptops, and other computing devices may not be used for work-related purposes. Work desktops, laptops, and other computing devices may not be used for personal purposes or other non-work-related activities. Tasks that do not require the use of computing devices should not be carried out on these devices.

Network Resources and Devices

✓ **Acceptable use(s):** Employees may make use of the [Utility Name]'s wired and wireless network technology for work-related purposes only as required by task, duty, and/or assignment. Passwords, firewalls, and other security measures must be enabled on all network resources and devices by trained staff members and/or contractors approved to do so. Such security processes must only be configured, altered, or terminated by appropriately designated individuals and approved by management.

🚫 **Unacceptable use(s):** All network resources and devices must be operated and maintained by trained staff members and/or contractors approved to do so. Employees without authorization must not make changes to these devices and resources unless directed to do so by management. These devices include, but are not limited to, routers, switches, wired connections, and wireless connections. Network security processes, credentials, and more must not be shared publicly or with any other non-work-related third parties unless approved by management or as required by law.

Cellphones and Other Mobile Devices

✓ **Acceptable use(s):** Work-related activities may be carried out on work-owned cellphones and other cellular devices as required by the task and/or approved by management. Passcodes and screen lock must be enabled on all devices used for work-related purposes. The loss, theft, or unauthorized use of such devices and resources must be reported to management as soon as possible.

Unacceptable use(s): Personal cellphones, personal cellular devices, and other non-work-owned cellular devices may not be used for work-related purposes. Work cellphones and work cellular devices may not be used for personal purposes or other non-work-related activities. Tasks that do not require the use of cellular devices should not be carried out on these devices.

Process Control and/or Supervisory, Control & Data Acquisition Systems

Acceptable use(s): Process control systems (PCS) and/or supervisory control and data acquisition systems (SCADA) may be used by employees with proper authorization. Employees may monitor, operate, and manage the systems with the best interests of the [Utility Name] and its customers in mind, while following all training, laws, and standard operating procedures. PCS and SCADA systems must always be password protected, auto-logout and/or password protected screensaver enabled after 10 minutes of inactivity and have all unnecessary media ports disabled. In addition, the systems must be updated frequently and as soon as possible following the release of security patches, be segregated from all other non-PCS and/or non-SCADA networks and resources and be secured behind proper firewalls and virtual privacy networks (VPN) as appropriate. The systems' physical components must all be secured behind physically locked doors. When accessing the systems remotely (as applicable and if appropriate), only [Utility Name] owned devices and resources may be used to do so with multi factor authentication and VPN(s) enabled. Only trusted networks and/or cellular connections may be utilized to access the systems remotely.

Unacceptable use(s): Only PCS and SCADA related tasks may be carried out on PCS and SCADA devices and resources. Personal or other non-PCS and/or non-SCADA work-related tasks may not be carried out on these devices and resources. This list of unacceptable activities includes, but is not limited to, email and communications, administrative, financial, social media, and gaming. Downloading or installing unapproved software and connecting unapproved hardware to the systems is prohibited. Only approved maintenance technicians and/or administrators may download, install, connect hardware, and otherwise alter the systems and their functionality and/or operation. Employees must have distinct logon credentials, including usernames and passwords, and must not share these with other colleagues or outside parties. Employee credentials must be terminated upon the employee's separation from the [Utility Name] immediately and not reused for any other employee or purpose. When accessing the systems remotely (as applicable and if appropriate), public and other non-trusted networks may not be utilized. Such un-trusted networks may be found at, but are not limited to, cafés, hotels, restaurants, sporting venues, and other non-password protected network locations.

Email and Communications

Please see the email and communications policy.

Social Media

✓ **Acceptable use(s):** Employees may use social media on the [Utility Name]'s resources for work purposes when directed by management or when carrying out work related duties as assigned. The use of social media must be in the best interests of the [Utility Name] and reflect organizational beliefs and/or opinions only. All laws must be followed when using social media and releasing any information publicly.

🚫 **Unacceptable use(s):** Employees may not use the [Utility Name]'s resources for personal social media or other non-work-related purposes. Further, employees shall not use personal devices and resources for work-related social media tasks and must refrain from personal social media activities during working hours and while on work premises. Confidential, private, and/or sensitive information about the [Utility Name] or its customers must never be released on social media. When using social media for work purposes, employees must never reflect personal beliefs and/or opinions.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.
Signature ____

Clean Desk Policy

Overview and Purpose: As confidential and sensitive information, documents, and resources can easily fall into the wrong hands either accidentally or intentionally, it is in the best interests of the [Utility Name] to secure it when not in use. This policy stipulates the procedures associated with removing and securing such content from unattended desks and digital workstations or computer desktops.

Scope: The scope of this policy includes all [Utility Name] employees, their workstations, and digital computer desktops and devices.

Policy: Employees must remove all information, documents, resources, and materials that are of a confidential, sensitive, and/or critical nature from their desks and publicly accessible workstations at the end of the workday or when absent for any extended period of time (time determined by management). If an employee is unsure about the status of the materials in question, prudence and caution should be followed. This includes any materials or resources that would otherwise be damaging to the [Utility Name] or its customers should they be lost or stolen.

An example list of such materials includes, but is not limited to, account information, financial data, usernames and passwords, employee data, customer data, and the [Utility Name]'s operations.

The following is a list of supplemental procedures to ensure a clean desk and workstation:

1. Materials and resources removed from desks and/or workstations should be secured in locked drawers, locked cabinets, and/or behind locked doors where unauthorized parties are unable to access.
2. Locked drawers, cabinets, and rooms (secured locations) must remain locked and secured when not in use.
3. Keys, passwords, and/or other tools used to access secured locations must not be left unattended and should also be stored securely.

4. Bulletin boards, whiteboards, and other notice boards should not contain information or materials of a sensitive, confidential, and/or otherwise damaging nature. This includes network information, such as Wi-Fi password and user account information.
5. Usernames, passwords, and other digital authentication information must not be kept on paper, sticky notes, or otherwise in visible locations. Passwords that are stored in a hard copy form must be secured at all times. Please note that hiding notes under other desktop items is not secure storage.
6. When printing and faxing, information and documents should be retrieved from the printer immediately and as soon as possible.
7. Documents of a sensitive and/or confidential nature should be shredded immediately or placed in official locked secure disposal bins when no longer needed.
8. All media devices including, but not limited to, CDROM, DVD, USB drives, hard drives, and backup devices, should be treated as confidential and sensitive materials and stored in secured locations when not in use. Hard copies, floppy disk, CD's, DVD's, USB drives and any other device or tool containing sensitive information must be removed from the desk and locked in a drawer when unattended and at the end of the workday.
9. As with physical desktops, digital desktops on computers must also be kept clean and secured. Confidential and sensitive information and/or data should not be stored on publicly accessible workstations, employees' computer desktops, or in otherwise easily seen and/or accessible locations.
10. Network information and data including, but not limited to, Wi-Fi passwords and account information, should be stored in secured locations when not in use. Such information and data should be treated with utmost care and not shared with outside parties.
11. Keys used for accessing restricted areas or sensitive information must not be left unattended.
12. File cabinets containing sensitive information must remain closed and locked when not in use.
13. Paper documents generated by printers and fax machines should be retrieved as soon as they are printed.
14. Whiteboards and blackboards must be erased after use.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ______________________________________

Data Backup Policy

Overview and Purpose: Because the [Utility Name] maintains data critical for continued operations and business, this policy exists to ensure a backup copy of the data is available in the event of an accident or intentional incident resulting in loss or corruption. The importance of backups, a proper backup schedule, and backup procedure are of high importance. This policy covers what data should be backed up, the processes to follow, and how to keep it secure.

Scope: The scope of this policy includes all [Utility Name] employees and any device used for work-related purposes with storage media and/or storage capabilities. This includes, but is not limited to, computers, USB drives, hard drives, and other storage media.

Policy: The following sets a baseline backup policy and set of associated procedures; however, additional policies and/or procedures may be necessary depending on the situation and data to be backed up.

1. In general, all data used for business purposes should be backed up including data files, databases, programs, and software. It may be necessary to backup different types and categories of data separately. For example, sensitive and/or confidential information may be required to be backed up separately and following different procedures than those for data of a less critical nature. The list of data to backup may be categorized into the following, but is not limited to, operations and maintenance, monitoring, reporting, financials, administrative, management, customer, and human resources.
2. A minimum of two backup copies of data should be maintained: one for restoration purposes and another for redundancy. The two backups should be stored in two separate offsite (in case of structure fire, etc.) locations either physical or digital (cloud-based) as appropriate and determined by management.
3. Process control system (PCS) and supervisory control and data acquisition (SCADA) backups should be backed up and stored separately from all other backups. It is recommended to maintain a spare PCS and/or SCADA system complete and capable of fully restoring operations following loss events, especially when unable to operate and

monitor systems manually. Such spares should be securely stored away from all unauthorized parties, whether employee or otherwise, and behind locked door(s). The secured location should be temperature and humidity controlled as well as resilient to other natural and manmade hazards.

4. Backups should occur weekly or as determined by management and are created from a full copy of all data on the relevant host or set of hosts.
5. Backups should be performed by appropriately trained and management designated employees, software and/or systems, and/or other third parties.
6. Should any host – or set of hosts – to be backed up be compromised, or suspected of compromise, the backup should be postponed or halted as determined by management until such a time where the host(s) can be cleared of any and all compromise(s). This includes, but may not be limited to, malware, ransomware, spyware, and viruses.
7. Backup and restoration capabilities should be tested and exercised periodically, at least once every six months, to ensure that backups and their procedures remain viable. Testing should only be performed by an authorized individual with proper credentials, knowledge, and approved by management.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ___________________________________

Email Communications Policy

Overview and Purpose: Email offers many benefits to the [Utility Name], including communication efficiency and customer contact among others. However, there are also cybersecurity threats that utilize email and a lack of awareness to exploit targets. In addition, the misuse of email by employees, staff, and others can lead to further issues and threats. Therefore, the [Utility Name] places an importance on employee email best practices and awareness training to ensure that email and communications are carried out appropriately and safety with the best interests of the [Utility Name] in mind.

Scope: The scope of this policy includes all [Utility Name] employees and any device used for work-related purposes. This also includes all [Utility Name] email accounts.

Policy: It is important to note that when using email, such an act connects the user to the outside world, third parties, and the Internet. Threats and hazards are not as easily controlled as within the [Utility Name]. Therefore, all employees, staff, and stakeholders acting on behalf of the [Utility Name] must understand that email offers benefits and risks. The following lists the set of policies applying to email communications:

1. Only employees, staff, stakeholders, and others authorized to use and access the [Utility Name]'s email may do so. Using email must be for work-related purposes only and always carried out with the best interests of the [Utility Name] and its customers in mind.
2. Using and accessing personal or otherwise email unrelated to work on devices connected to the [Utility Name]'s network, servers, and/or devices is prohibited without authorization.
3. The use of email must comply with all laws, regulations, rules, and the [Utility Name]'s applicable policies, procedures, and ethical code(s) of conduct.
4. Creating new email accounts must be carried out by trained and appropriately authorized parties. Only email systems and storage servers approved by management may be used to create new email accounts. Similarly, deleting and terminating email accounts must only be carried out by trained and appropriately authorized parties.

5. Email account addresses, usernames and passwords must follow the Password Policy.
6. It is prohibited to forward any work-related email to personal email accounts and/or systems or third parties not authorized to receive the email.
7. When receiving email, all users must be appropriately wary of the sender, the content, and any attachments. The user must first ensure the identity of the sender is accurate and as displayed, the content is appropriate and not misleading, and the attachments are safe before opening, downloading, forwarding, and/or using for other purposes.
    a. Identifying the sender can be carried out by, but is not limited to, checking to ensure the name and actual email address match the expected individual or entity. If there are concerns, the user should proceed no further with the email and refrain from forwarding or sending it and any content and attachments without first consulting with management and appropriately trained parties.
    b. When reviewing the content of the email after first checking the identity of the sender, users should scan for flags that the email has been compromised, check to ensure that the content matches what is expected from the sender, and review for any unexpected signs. Signs that should raise flags include, but are not limited to, spelling and/or grammar errors and inappropriate content among others.
    c. Finally, attachments should always be treated as potentially dangerous. Only attachments from properly identified senders should be opened, downloaded, forwarded, and/or used for other purposes. If able, all attachments should be scanned for threats prior to opening, downloading, and/or forwarding. Executable files must not be opened, downloaded, and/or forwarded expect by authorized and appropriately trained parties.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

External & Removable Media Policy

Overview and Purpose: Although external and removable media, including but not limited to USB drives, SD cards, CDs, mobile phones, smart devices, and their relevant ports on assets and devices offer convenience for storage and transfer of data, they also present unique security concerns. As noted in the Physical Security Policy, the physical security of assets impacts their cybersecurity. This is never more apparent than with external and removable media.

More specifically, portable media are pieces of hardware that may contain, transfer, or expose assets to security risks. It is important to extend the same protections one would utilize in the real world when dealing with external and removable media. For example, most would not accept an unknown package from a stranger in public without knowledge of what is contained within, where it has been, and what it has been exposed to. The same concern and guard also applies to external and removeable media.

Scope: The scope of this policy includes all the [Utility Name]'s Information Technology (IT) assets, including but not limited to, computers, Supervisory, Control, and Data Acquisition (SCADA) systems, networking devices, and mobile devices as well as all external and removable media and their relevant ports on the [Utility Name]'s IT assets.

Policy: The following sets forth the External and Removable Media Policy:

1. External and removable media ports on devices that do not require their use should be disabled, especially on SCADA and Process Control System (PCS) assets as well as all devices that connect physically or logically to them. For those that require occasional use, the ports can be disabled and enabled on an as needed basis. It is also recommended that ports – when not in use – utilize safety/dust plugs to prevent unintended use.
2. For devices that require more frequent use of external and removable media, special consideration should be taken to ensure the device is not exposed to risk. Specifically, external and removable media from an unknown source or location should be treated

the same as media known to contain malware, viruses, or other security concerns. These external and removable media should never be connected to any device or asset at the [Utility Name].

3. External and removable media that is found – whether in public or at the [Utility Name] and regardless of labeling – should be turned over to the [Utility Name]'s IT department or responsible staff for proper disposal.
4. External and removable media owned by the [Utility Name] should be properly labeled and secured in a locked cabinet, drawer, or other similarly secured location when not in use. These media devices should also be encrypted, password protected, cleared of all critical and sensitive data when not in use, and properly disposed of by trained staff when no longer needed.
5. All assets and devices at the [Utility Name] should employ antivirus software and data blockers as well as disabling autorun, autoplay, and automatic downloads from removable and external media.
6. When possible, cloud transfer solutions approved and properly vetted by utility leadership should be employed instead of external and removable media.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

Information Sharing & Collaboration Policy

Overview and Purpose: Sharing information and collaborating on cybersecurity is in the best interest of the [Utility Name]. Not only does collaboration offer the [Utility Name] advantages in mutual aid during cybersecurity events and emergencies, but it also promotes a culture of awareness at the utility. It should also be noted that many cybersecurity tools, such as antivirus, rely on information sharing to work effectively. For example, when new malware or viruses are found, antivirus software is updated across the world to include protections against it. Without a report from the first victim, others cannot be effectively secured against the threat. Beyond sharing information, receiving assistance and reports at the [Utility Name] also assists in protecting the [Utility Name]'s critical assets.

Scope: The scope of this policy applies to all utility staff.

Policy: The following sets forth the Information Sharing and Collaboration Policy:

1. The [Utility Name] should be a member of and active participant in the Maine Water and Wastewater Agency Response Network (WARN).
2. The [Utility Name] should develop mutual aid agreements with neighboring utilities and other partners that are able to offer assistance in the event of a cybersecurity incident or other emergency.
3. The [Utility Name] should gather and distribute details of relevant security incidents and events from utility partners and other relevant organizations to internal staff to promote awareness and cybersecurity at the utility. The internal reports should be provided on a regular basis determined by utility leadership and immediately following any critical event or report that may impact the [Utility Name]'s critical assets.
4. All cybersecurity incidents should be reported and shared with utility partners, such as WaterISAC, Cybersecurity Infrastructure Security Agency (CISA), Maine Information and Analysis Center (MIAC), Environmental Protection Agency, Drinking Water Program, federal and/or state authorities, and other mutual aid partners. Reporting should only be performed by staff designated by utility leadership.

5. All cybersecurity incidents should be reported as legally required. The [Utility Name]'s legal counsel should be consulted with questions and prior to any report.
6. Reports should only be shared by staff designated by utility leadership. Critical, sensitive, and confidential information should not be shared without consultation and approval from utility leadership and the [Utility Name]'s legal counsel.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

Offboarding Policy

Overview and Purpose: Information Technology (IT) assets no longer in use can pose substantial risk to the [Utility Name]. Thus, when assets are no longer required, they should be removed from service as soon as possible. Concurrently, employees separated from the [Utility Name] must be similarly treated in that the separated employee's access to systems should be terminated immediately and all assets returned to the [Utility Name] promptly. Properly off-boarding both IT assets and employees can reduce the [Utility Name]'s vulnerabilities and risk.

Scope: The scope of this policy includes all the [Utility Name]'s employees and any individual or entity with access to the [Utility Name]'s electronic and digital infrastructure and/or resources. The scope further includes all of the [Utility Name]'s devices, hardware, software, and any other digital or IT resources.

Policy: The following sets forth the Off-Boarding Policy:

1. **Assets**
   a. It is a best practice to maintain an asset management program to ensure all assets are tracked. The program allows the [Utility Name] to remain informed about assets that may require maintenance, updates, patches, removal from service, and more. IT infrastructure and other digital assets should be included in the asset management program.
   b. An audit procedure – carried out at management-set intervals during the year – of the asset management program should be employed to ensure assets are not lost, misplaced, or forgotten. The audit procedure should also review employee access.
   c. When assets are no longer needed, they should be promptly removed from service. These assets include, but are not limited to, computers, printers, software, backups, other electronic devices, and IT infrastructure. It is of crucial importance that all devices with storage capabilities are included. Removal from service may include, but is not limited to:

      i. Backup of needed information and data,
      ii. Disconnection from the [Utility Name]’s IT infrastructure, networks, servers, and other related processes,
      iii. Deletion and/or wiping of stored media,
      iv. Resetting to factory conditions,
      v. Removal and/or destruction of storage media,
      vi. Proper disposal and/or destruction of the asset. Proper disposal and/or destruction methods may depend on the asset and management guidelines.
   d. Only individuals with authorization and proper expertise should carry out the steps to remove assets from service. All steps taken and carried out should be noted in the [Utility Name]’s asset management program.

2. **Employees** (and others with access to the [Utility Name]’s assets)
   a. The above-mentioned asset management program should include and track details about access and assignment of assets to employees and other third parties to allow the [Utility Name] to ensure only individuals with authorization maintain possession of and access to such assets.
   b. Employees separated from the [Utility Name], whether voluntarily or involuntarily, should have their physical and logical access to the [Utility Name]’s assets terminated immediately.
      i. Termination of physical access may include, but is not limited to:
         1. Returning or confiscation of assigned assets,
         2. Returning or confiscation of ID badges, keys, and other physical access controls,
         3. Returning of utility branded clothing, business cards, and other branded materials such as letterhead and cardstock,
         4. Removal from the premises as required,
         5. Notification of separated status to other employees and parties with the need to know.
      ii. Termination of logical access may include, but it not limited to:
         1. Termination of access, authorization, accounts, and authentication, such as accounts, usernames, passwords, and other related credentials to all internal and external devices, systems, software and programs, and more,
         2. Modification or termination of any shared access or credentials. It is important to note that sharing access controls and credentials is not recommended.

c. Only individuals with authorization and proper expertise should carry out the steps to terminate access. All steps taken and carried out should be noted in the [Utility Name]'s asset management program.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ___________________________________

Password Policy

Overview and Purpose: Passwords are important for protecting the [Utility Name]'s assets, IT resources, and data against unauthorized access, attack, and/or damage. Simple and weak passwords open the [Utility Name] to additional risks and threats. Therefore, strong passwords are key as well as following password best-practices.

Scope: The scope of this policy includes all the [Utility Name]'s employees and any individual or entity with access to the [Utility Name]'s electronic and digital infrastructure and/or resources. The scope further includes all of the [Utility Name]'s devices, hardware, software, and any other resource that can be password protected.

Policy: The following sets forth the Password Policy:

1. All devices and resources with the ability to be password protected must be password protected. Devices without the ability to be password protected should be avoided.
2. All default passwords should be changed immediately, including employee passwords or manufactory passwords.
3. Passwords must not be shared internally or externally at the [Utility Name], and all staff must maintain unique passwords separate from any other staff member.
4. Staff with access to critical systems, including but not limited to Process Control Systems (PCS), Supervisory, Control, and Data Acquisition (SCADA) systems, and Business Critical Systems (BCS), must not share or reuse passwords. Each staff member with access to these systems must maintain unique and distinct passwords and other authentication details from any other staff member. When accessing critical systems, all staff must utilize their own unique credentials and passwords to do so and must not utilize any other credentials. Furthermore, multi-factor authentication must be enabled – in addition to passwords – for all critical systems as determined by management.
5. Passwords must be strong:
    a. Default passwords must be changed as soon as possible.
    b. Passwords should be at least 16 characters in length. It is recommended to set passwords longer than 16 characters when possible.

c. Passwords should be as random as possible. Randomizing a password includes mixing a string of upper-case, lower-case, numbers, and symbols together. **Password123!** is an example of a poor password, while **EG^JH#@cP^o3IVM1** is an example of a strong password.
d. Passwords should not contain any identifiable information, including but not limited to, usernames, family names, dates of birth, and more.
e. Passwords should not contain any easily guessable details, including but not limited to, song lyrics, famous quotes, popular travel destinations, and more.
f. Each account should have a different password.

6. Because strong passwords may be difficult to remember, it is recommended that the [Utility Name] make use of password managers. This will allow the use of strong passwords, unique passwords for all accounts and for all users, and the ability to easily recall passwords when needed. Password manager best-practices should always be followed.
7. Passwords must be adequately encrypted by properly trained individuals as determined by management. Passwords must also not be stored in clear text and reversible formats.
8. Passwords should only be changed or altered if the user has reasonable suspicion of password compromise.
9. Accounts should be monitored for suspicious activity, and if suspicious activity is suspected or proven, the password(s) must be changed immediately.
10. Passwords and other authentication data must be terminated immediately upon a staff member's separation from employment or other parties' separation from affiliation with the [Utility Name].
11. Staff should be periodically trained (every 6 months) on password hygiene and best-practices.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

Patches and Updates Policy

Overview and Purpose: Patches and updates, including security updates, for devices, hardware, and software offer defenses against known vulnerabilities and threats. Typically, when a vulnerability is found, either through testing or experience, a patch and/or update is developed and released to mitigate and/or eliminate the vulnerability. It is important to note that this typically only applies to known vulnerabilities. Therefore, patching and updating devices, hardware, and software used for the [Utility Name]'s work-related purposes or those connected to the [Utility Name]'s network, systems, devices, hardware, and/or software are of critical importance. Unpatched and outdated devices, hardware, and software can create holes in the security of any system.

Scope: The scope of this policy includes all of the [Utility Name]'s employees, devices, hardware, software, and any other resource that can be patched and/or updated. Patches and updates apply to many resources, and they are not limited to smartphones, mobile phones, tablets, laptop computers, desktop computers, other computing devices, and the software on such resources. In addition, network hardware and software, process control systems (PCS) and/or supervisory control and data acquisition (SCADA) systems and their hardware and software, and printers among other resources are also included.

Policy: The following list sets forth the Patches and Updates Policy:

1. Patching and updating systems, devices, hardware, and/or software should only be carried out by properly trained and authorized parties approved by management.
2. Patches and updates, especially urgent security patches and updates, should be implemented as soon as possible following release even if it falls outside of the normal patch and update cycle. It is best practice to implement them immediately, but under no circumstances should a security patch or update be delayed more than one week.
3. As determined by management and trained information technology (IT) staff and/or authorized contractors, security patches and updates should be set to be performed automatically on all systems, devices, hardware, and software. It is recommended that

non-security patches and updates also be set to automatic, but they should never be delayed more than one week unless approved by management as appropriate.

4. It is best practice to track all resources outlined in the scope above through asset management to maintain records when patches and updates are performed and when they should be implemented. Such a practice may also be used to identify outdated and/or vulnerable resources that should be removed from service.
5. Patching and updating PCS and SCADA systems may require additional considerations, and properly trained and authorized parties should always be consulted when performing maintenance on such systems. Depending on the skills and authorization of staff, it may be required to have outside and/or third-party contractors and/or vendors perform patches and updates on PCS and SCADA systems. Such external parties should always be vetted, trusted, and approved by management.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

Physical Security Policy

Overview and Purpose: The physical security of a utility is important in its own right but also for the role it plays in ensuring the cybersecurity of the utility. More specifically, physical security and cybersecurity go hand in hand and the neglect of one or the other may lead to the breakdown of both. Although cybersecurity often exists in the "digital" realm, most assets exist – at least in part – physically and, as a result, require physical security considerations.

Scope: The scope of this policy includes all of the [Utility Name]'s physical premises and assets, as well as all staff and individuals with access to these locations and assets.

Policy: The following sets forth the Physical Security Policy:

1. As noted in other policies, the principle of least privilege (if one does not need access, they should not have access) should also be applied to physical security. If an individual – whether staff, contractor, or other third party – does not need physical access to the premises, a specific location, or an asset critical to the cybersecurity of the [Utility Name], they should not be given access.
2. In addition, to secure physical locations and assets through the principle of least privilege, all buildings and structures containing assets critical to the [Utility Name]'s cybersecurity should be physically protected by non-technical barriers, including but not limited to, fences, gates, barricades, locked doors, photo identification and ID cards, and metal bars as needed and deemed necessary by utility leadership.
3. Furthermore, it is a best practice that all critical, physical locations and structures be protected and monitored by security cameras, intrusion detection systems, motion detectors, guards, and fire and smoke alarm systems. A culture of physical security should also be promoted among staff so that staff remain on guard against physical intrusion and suspicious individuals, situations, or events are noticed and reported to utility leadership as soon as possible.
4. Within the [Utility Name]'s premises and structures, assets critical to the cybersecurity of the utility should be protected behind locked doors and/or cabinets. As noted before, if an individual does not need access, they should not be provided access and this

extends to all locations and assets within physical structures as well. Networking devices and cables should not be neglected and should also be protected by locked doors and/or cabinets. Lastly, the keys, passwords, and any other means of authentication should be similarly protected by the principle of least privilege, must not be left unattended, and should be stored securely.

5. Please see the External and Removable Media and the Clean Desk Policies for further details on the physical security of assets and premises.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

Preparedness, Response & Recovery Policy

Overview and Purpose: As outlined by the United States Environmental Protection Agency, utilities should follow the “prepare, respond, and recover” process in relation to emergencies that include both natural and man-made threats. The “all-hazards” approach to categorizes hazards into three categories: natural, man-made, and cyber threats. Natural hazards include fire, floods, storms, and more, while man-made threats include, but are not limited to, vandalism, theft, and terrorism. Further refining the man-made threats results in the third and final category. Properly preparing for, responding to, and recovering from cyber threats allows utilities to increase their cyber resilience.

Scope: The scope of this policy includes all the plans, procedures, and processes at the [Utility Name] in relation to preparing for, responding to, and recovering from cyber hazards.

Policy: The following sets forth the Preparedness, Response, and Recovery Policy:

1. Preparation: Preparing for cyber emergencies includes, but is not limited to, assessing risk, developing an emergency response plan (ERP), training staff and stakeholders, and implementing other preventative and mitigation measures.
   a. Assessing risk: To properly assess cyber risk to the [Utility Name], a Risk Resiliency Assessment (RRA) following relevant standards should be completed considering all hazards. Prior to the development of the RRA, the [Utility Name]’s tolerance for risk should be determined and utilized in the development of the RRA. Determination of applicable hazards and vulnerabilities is also crucial as well as identifying critical assets utilized in completing the [Utility Name]’s mission critical goal. The basic steps to develop an RRA include:
      i. Threat-asset pairing: Pair threats with critical assets.
      ii. Risk calculation: Calculate risk by considering the consequences and likelihood of the threat, as well as the vulnerability of the relevant asset.
      iii. Risk categorization and prioritization: Categorize and prioritize risks based on their final risk values to utilize in future preparation steps.

   b. Developing an ERP: Utilizing the output of the RRA, an ERP should be developed. An ERP is a comprehensive plan that provides information, guidance, and assists in incident response and recovery. As such, an ERP should layout basic information about the [Utility Name], internal and external contact information, system and process details, a collection of procedures to follow in the event of common hazards, and relevant resources.
   c. Training: See the Cyber Awareness Training Policy.
2. Response: Responding to cyber emergencies begins with the development of a cyber incident response plan (IRP). It is a best practice that an IRP be developed as a standalone document and supplemental to an ERP. Although an ERP includes content and response procedures related to common cyber incidents, an IRP supplements the ERP by laying out more specific response procedures and processes for cyber incidents. The IRP opens with identification of the incident response team and other stakeholders, which may include internal and external parties, before laying out steps following the National Institute of Standards and Technology's incident response lifecycle: preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.
3. Recovery: Recovering from cyber emergencies begins with the development of a cyber disaster recovery plan (DRP), which may be a standalone document or contained as a section within an ERP. Similar to the IRP, a DRP supplements an ERP by further refining recovery steps for cyber incidents. The goals of the DRP include, but are not limited to, mitigating losses, ensuring services and business can continue uninterrupted, and eventually returning all devices and systems to normal.
4. All plans, procedures, and processes should be reviewed frequently – at least once per year – and kept up to date. The documents should be included in relevant training programs and provided to staff and external parties in an as-needed manner considering the sensitive and confidential nature of the information. Drills, tabletop exercises, and full-scale exercises are examples of ways to train on and maintain the plans, procedures, and processes.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

Remote Access Policy

Overview and Purpose: Remote access to the [Utility Name]’s systems and resources offers a number of benefits to productivity and efficiency, but also poses potential security vulnerabilities. Therefore, this policy sets out to define the proper processes and procedures for accessing the [Utility Name]’s systems and/or resources when offsite and/or remotely.

Scope: The scope of this policy includes all the [Utility Name]’s employees and any individual or entity with remote access authorization to any of the [Utility Name]’s systems and/or resources. Such resources may include, but are not limited to, servers, computers, process control systems (PCS) and/or supervisory control and data acquisition (SCADA) systems, and printers among others.

Policy: Only employees and vendors or contractors authorized by management may access systems and/or resources remotely. If remote access is not needed to complete a task, remote access should not be used. When needed as described previously, remote access should always be in the best interests of the [Utility Name] and its customers. Because remote access can open holes and vulnerabilities into the [Utility Name]’s systems and resources, access to such systems and resources must be given the same security consideration, if not higher as appropriate, as on-site connection(s).

1. Only employees, vendors, and contractors approved by management and properly trained may access the [Utility Name]’s systems and/or resources remotely.
2. Remote access may only be utilized through a known, trusted, and secure connection that is under the complete control of the authorized party or another authorized party or entity. Public networks, especially those without passwords, must never be used to access systems and resources remotely. It is a best practice for management to provide authorized employees with a list of trusted networks and/or connections. Only the connections and/or networks on the list may be utilized.
3. Remote access must make use of encryption as determined by management and properly trained and authorized information technology (IT) staff and/or contractors.

4. Remote access must make use of strong usernames and passwords as outlined by policy, procedure, and management. Authentication information, including usernames and passwords, must be protected from other parties, including, but not limited to, colleagues, friends, family members, and strangers. Login credentials co-worked, friends, family, or other unauthorized parties.
5. Multi-factor authentication should always be implemented for all remote access. It is also a best practice to make use of an approved virtual privacy network (VPN) to access systems and/or resources remotely.
6. Only [Utility Name] owned resources may be used to remotely access systems and resources. Personal or other non-[Utility Name] owned resources may not be used for remote access. It is a best practice for management to provide a list of approved resources for remote access, and only resources on this list may be utilized for this purpose.
7. All resources used for remote access must have the latest updates and security patches implemented, as well as anti-virus software as appropriate and determined by management.
8. When accessing systems and/or resources remotely, authorized individuals must always be wary of their surroundings and all onlookers. Remote access may only be utilized in private and physically secured locations where third parties are unable to oversee.
9. When accessing systems and/or resources remotely, authorized individuals must always ensure that they have disconnected from all unknown, untrusted, and insecure connections and/or networks.
10. All resources used for remote access must have auto-screensaver enabled after 10 minutes of inactivity. It is also a best practice to implement auto-factory reset on such resources after incorrectly entering a password, pin, and/or passcode incorrectly 10 times in a row as appropriate. In addition, for mobile devices, strong passcodes are required, and all devices must not be left unattended.
11. When finished accessing systems and/or resources remotely, authorized individuals must disconnect and/or logout from remote access immediately.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

Security Awareness Training Policy

Overview and Purpose: Although the implementation of technical security measures is important in all cybersecurity programs, most incidents target people. Even those that are complex and technical in nature also often stem from people. Therefore, it is important to pair technical processes and procedures with cybersecurity awareness training. This policy sets out the scope, timing, and content of such training.

Scope: The scope of this policy includes all the [Utility Name]'s employees and any individual or entity with access to the [Utility Name]'s electronic and digital infrastructure and/or resources.

Policy: The following sets forth the Security Awareness Training Policy:

1. All new employees, and other parties with access to the [Utility Name]'s electronic and digital infrastructure and/or resources, must be trained by a program approved by management within 60 days. The first program must be at least 2 hours in length and focus on threats, vulnerabilities, and best practices to ensure security at the [Utility Name] and for its customers.
2. A list of training programs approved by management should be created and distributed to all employees, and other parties with access to the [Utility Name]'s electronic and digital infrastructure and/or resources. The list should be updated and reviewed frequently by management.
3. All employees, and other parties with access to the [Utility Name]'s electronic and digital infrastructure and/or resources, must participate in ongoing training throughout their duration with the [Utility Name]. Following the first training, the above-mentioned individuals must take another training every 6 months. These training programs must be at least 1 hour in length, but it's recommended that they be longer. Different training programs should be prioritized each 6-month period, and individuals may only retake programs when approved by management.

4. Every two years, all employees, and other parties with access to the [Utility Name]’s electronic and digital infrastructure and/or resources, must retake the original 2-hour training previously taken.
5. Following any cybersecurity incident or breach, all employees, and other parties with access to the [Utility Name]’s electronic and digital infrastructure and/or resources, must participate in a 2-hour security awareness training program focusing on the incident(s) that occurred. If one or multiple employees are to blame for the incident, they should not be singled out and forced to take the training alone. These individuals’ names and identities should be kept confidential, and all employees should be trained.
6. Employees and other parties with access to the [Utility Name]’s electronic and digital infrastructure and/or resources should be encouraged to maintain their cybersecurity awareness through training apart from mandatory training as well. Incentives and other benefits can be offered to promote additional training.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

Subcontractor, Supply Chain & Vendor Policy

Overview and Purpose: The statement that "a chain is only as strong as the weakest link" has become one of the most frequently used sayings in the world of cybersecurity. If the [Utility Name] secures itself against all threats without consideration for those stemming from the supply chain, the weakest link in the cybersecurity chain will be exposed and break the entire program. Therefore, the [Utility Name] should implement security controls to protect against supply chain threats, including but not limited to, software vulnerabilities, data breaches, implanted backdoors, and more.

Scope: The scope of this policy includes all the [Utility Name]'s contractors, subcontractors, vendors, and other third parties with physical or logical access to utility premises and assets as well as all newly purchased or acquired Information Technology (IT) assets and the companies from which they stem.

Policy: The following sets forth the Subcontractor, Supply Chain, and Vendor Policy:

1. All new contractors, subcontractors, and vendors should be properly vetted prior to being given access to the utility's premises and critical assets. Vetting should also be carried out on vendors prior to purchase and connection of new IT assets and devices to the utility's systems and infrastructure. In addition, vetting should include background checks that follow the utility's background check policy.
2. Please see the Physical Security Policy.
3. Physical and logical access to the utility should follow the principle of least privilege.
4. All requests for proposals, quotes, and contracts should include security considerations and terms for the management of contractor, subcontractor, vendor, and supply chain security. These third parties should be required to adhere to minimum cybersecurity as determined by leadership and legal counsel.
5. All contractors, subcontractors, and vendors should be properly identified prior to being given access to the physical premises and assets. Further, these third parties should always be accompanied by utility staff when physically onsite.

6. Utility staff should be trained to recognize and report unauthorized changes, alterations, and inconsistencies to the utility’s physical and logical assets.
7. When a contractor, subcontractor, vendor, or other third party no longer requires access to physical or logical premises and assets, their access should be terminated immediately. This includes the return of all identification, IDs, and keys.
8. Existing contractors, subcontractors, and vendors should be periodically vetted to ensure that they continue to remain secure against threats to the utility. In addition, new and existing contracts and agreements should be reviewed to ensure that cyber events or incidents caused or triggered by contractors, subcontractors, and/or vendors are addressed properly.

Statement of Understanding & Signature: I understand that it is my responsibility to read and know this policy – regardless of position or duties assigned to me – and will request clarification if needed. By signing below, I pledge that I have read and understood this policy and will conduct my activities accordingly and in the best interest of the [Utility Name] and its customers.

Signature ____________________________________

Appendix

Must Read:

Prior to use and/or implementation of these policies, each policy should be thoroughly reviewed to ensure that they meet the utility's needs and unique considerations and environment. If changes, edits, or updates are required, they should be made before these policies are put into effect. Lastly, the policies should be frequently reviewed and updated to ensure that they remain accurate and effective for the utility.

References:

The documents, reports, and templates below served as reference material in the development of these cybersecurity policies.

- WaterISAC's 12 Cybersecurity Fundamentals for Water and Wastewater Utilities
- WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- NIST's Cybersecurity Framework: Policy Template Guide
- CISA's Cross-Sector Cybersecurity Performance Goals Report
- SANS' Security Policies Templates