CYBERSECURITY
BEST PRACTICES
FOR SMALL AND
MEDIUM
PENNSYLVANIA
UTILITIES
The information provided in this document is presented as a courtesy to be used for informational purposes only. This information is not intended to constitute legal advice or counsel nor is it a substitute for obtaining legal advice from your own private attorney.
1. ASK QUESTIONS

Cybersecurity is the responsibility of every employee; however, there are basic questions to which executives and employees should know the answers. For example:

- Who in my organization is responsible for cybersecurity?
- What are the rules that govern my use of company resources (computers, smartphones, tablets)? How can I be kept aware of updates to these rules?
- If I suspect I have a cybersecurity issue (malware, spyware), who should I contact within my organization?
- Does my organization have a policy on bringing personal devices into the workplace?
- What am I allowed to connect to my company’s system and could my device infect the system?

There are any number of questions a company may wish to add to this list. Additional ideas can be found by using the resources mentioned in or attached to these best practices.

2. FOCUS ON HUMAN CAPITAL

When thinking about cybersecurity, the instinct is to focus on computers and keyboards, networks and servers. However, one of the biggest immediate cyber risks to most utilities comes from employees and vendors. It has been reported that one in five employees will click on a “bad” link. Robust security systems can be compromised by an employee clicking a link in a phishing email or accidentally installing malicious pieces of software on a computer. Human error remains a point of vulnerability and one that companies should address.
• Train and test staff regularly and repeatedly so that they understand and fully appreciate their role in maintaining a cyber safe work environment.
• Institute strong security rules for vendor access to systems, facilities and equipment.
• Develop strong policies concerning employee access to sensitive information especially at separation of employment.

3. COVER SOME OF THE BASICS

There are some basic rules all companies should follow in practicing good cybersecurity.

• Every user should have their own account with particular rights and restrictions. These rights should be limited to what the employee needs to perform their job duties.
• Users should have strong passwords requirements and should be prompted to update those passwords at regular intervals.
• Employees’ cybersecurity responsibilities should be clearly identified in job descriptions, policy statements, or other company documents (like procedures manuals). Companies should update their employees’ and contractors’ security credentials as they move through the organization. Often, employees will still have access to systems despite moving to new areas that do not require such access or even upon leaving the company. Contractors may retain remote access to systems or sites even after their work is completed; companies should make concerted efforts to limit and prevent this remote access once outside vendors’ contracts are complete.
• Security patches on software should be updated regularly.
• Older versions of software should be removed.

The U.S. Department of Homeland Security (USDHS) provides additional detailed advice on maintaining safe computer networks and systems.
4. RISK MANAGEMENT

Approaching cybersecurity in an organization can be overwhelming. Look at all of your company’s systems and business processes, then start prioritizing.

- Which systems, IT or SCADA, and functions are most critical?
- Which data systems house your company’s most sensitive information?

Concentrate efforts and resources there first.

5. USE AN ASSESSMENT TOOL

If your company is not sure where to begin on a risk assessment, the USDHS has created a Cybersecurity Evaluation Tool to guide users through a step-by-step process to assess their cybersecurity readiness. Companies can download this free tool at https://ics-cert.us-cert.gov/Assessments.

6. MANAGING VENDORS AND CONTRACTORS

Often, companies must rely upon third parties to handle aspects of their information technology infrastructure, control systems and security. It is critical that companies understand the security services that contractors provide.

- If your company uses an Internet Service Provider, it should ask about the various levels of security they offer including protection from distributed denial of service (DDOS) attacks.
- If vendors are going to be able to access your company’s data, ensure that transfers of the data are properly protected and that the vendor has the necessary controls and procedures in place to maintain and protect confidential information.
- Be sure to draft requests for proposals (RFPs) that include requirements that support and consider your utility’s security policies. This should include restricting employee access based on their job descriptions and responsibilities, and preventing access to systems based on vulnerabilities in existing infrastructure.
7. SECURITY AS A STARTING POINT

Decades of familiarity with anti-virus programs have conditioned people to think of cybersecurity as a separate tool to be added on top of other products. Today’s software and control systems should be developed and designed from the outset with security in mind. Networks should be constructed to minimize possible intrusions and to allow a company to recognize when it is under attack.

• When possible, speak with vendors about the security characteristics of their products and incorporate cybersecurity as a key component in any new specifications your company develops.

8. DON’T OVERLOOK THE PHYSICAL

Discussions of cybersecurity tend to focus upon firewalls, network infrastructure and control systems. It is important not to forget about protecting your company’s physical assets as well. For example, if your company has a computer on its network in a remote location, ensure that access is controlled and monitored. Employees or contractors who log in to your system remotely may inadvertently compromise your security by misplacing their devices.

• Understand the physical attack vectors that exist into your network and restrict access to those points.

9. TESTING

Training, assessment and system hardening are good, but they need to be tested regularly. In the same way utilities conduct exercises focused on physical security and disaster response, they should also focus upon cybersecurity scenarios. These exercises might range from sending a phishing email to employees to see if they click on the link to hiring a third party to attempt to penetrate your company’s cyber defenses. USDHS’s website offers some helpful tips for planning your own cybersecurity exercise.
10. LEARN FROM YOUR PEERS

Some of the best resources out there are your peers. Trade associations and other forums can provide a great outlet for sharing best practices and learning measures that other companies are undertaking. National and state organizations like the National Association of Water Companies and the Energy Association of Pennsylvania have actively engaged their members on issues of cybersecurity. These groups can be a great resource on everything from the latest threat information to sample questions for vendors within your industry.

II. SO YOU’VE BEEN HACKED...

In today’s world, it is not a question of whether your company has had a cybersecurity intrusion, it is whether your company knows about an intrusion or not. USDHS provides a useful checklist for companies who have been infiltrated by cyber attackers. Your company’s ability to detect the intrusion is critical, but do not forget to take steps to preserve forensic information after the attack. For example, running anti-virus software after the incident can change file names and dates, impeding the chances of discovering what caused the intrusion.
12. VIGILANCE

Your company’s cybersecurity defenses are only as good as they are timely. State of the art technology and techniques for both attackers and defenders changes constantly. Be sure your company is keeping up with and aware of the latest threats and issues. Government agencies, trade organizations and your company’s own vendors can be great resources in ensuring that your organization is on top of the latest cybersecurity developments.

13. REPORTING INCIDENTS

The best way to support your company’s and your industry’s cybersecurity defenses is to ensure that your company timely reports incidents through the appropriate channels. Utilities and others can report attempted or successful intrusions through the U.S. Department of Homeland Security. If your company has been the victim of a cyber-crime, notify the appropriate regional office for the Federal Bureau of Investigation. The FBI has also established InfraGard, a public-private partnership for members to report and receive threat information.

14. DEVELOPING AND MAINTAINING APPROPRIATE WRITTEN CYBERSECURITY, EMERGENCY RESPONSE AND BUSINESS CONTINUITY PLANS PURSUANT TO 52 PA. CODE §§ 101.1-101.7

According to state regulations, most utilities are required to develop and maintain written security, emergency response and business continuity plans. In addition, utilities are required to file an annual self-certification form with the Public Utility Commission that affirms their compliance with this requirement. Information about the self-certification as well as the form are available on the Commission’s website.
The Office of Cybersecurity and Communications (CS&C) works with state and local government as well as private sector partners to minimize the impact of cybersecurity incidents. Two of CS&C’s National Cybersecurity and Communications Integration Center components, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and United States Computer Emergency Readiness Team (US-CERT) work to mitigate cybersecurity incidents in close coordination with public and private sector partners.

ICS-CERT provides onsite support to owners and operators of critical infrastructure, including incident response, forensic analysis, and site assessments. ICS-CERT also provides tools and training designed to increase stakeholder awareness of the threats posed to industrial control systems.

The ICS-CERT website provides various resources for owners and operators of critical infrastructure and the industrial control systems that operate many of the key functions of their facilities, such as SCADA system. The website contains links to resources such as alerts, advisories, newsletters, training, recommended practices, as well as a large list of standards and references.

The ICS-CERT website can be found here: https://ics-cert.us-cert.gov/. ICS cyber incidents can be reported to: ics-cert@hq.dhs.gov.

The Federal Bureau of Investigation (FBI) has two field offices in Pennsylvania, one in Pittsburgh and the other in Philadelphia. The FBI may be able to assist critical infrastructure owner/operators when there is a cyber-attack or suspected cyber incident. The
FBI encourages reporting of suspected cyber-attacks by critical infrastructure owners.

The Pittsburgh Office number is 412-432-4000 and the Philadelphia Office number is 215-418-4000.

**NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER (NCCIC)**

The NCCIC, within the Office of Cybersecurity and Communications, serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The center’s activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

Cyber incidents can be reported to the NCCIC watch desk at: NCCIC_WatchandWarning@hq.dhs.gov.

**INFRAGARD**

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI’s investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide
range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes. Membership is free and open to all critical infrastructure owners and operators.

More information, including information on membership, can be found here: [https://www.infragard.org/](https://www.infragard.org/).

**iGUARDIAN**

The FBI recently release the iGuardian portal as a pilot program designed to give companies a designated location to report cyber threats they’ve encountered. Initially, the program will be open only to members of the InfraGuard Network (see above). The iGuardian portal offers a one-stop-shop for cyber incident reporting. Reports received by iGuardian will go to the local FBI office and the FBI may follow up with the reporting entity. More information on becoming an InfraGard member can be found here: [https://www.infraguard.org/](https://www.infraguard.org/).
The Department of Homeland Security (DHS) Protective Security Advisor (PSA) program offers critical infrastructure owner/operators a conduit to many free services such as security training, site assessments, and assistance with local exercise coordination. PSAs are locally based within three regions in Pennsylvania.

There is also a regionally based Cyber Security Advisor (CSA) that functions in the same capacity for cybersecurity-specific issues.

More information on the PSA program may be found here: [http://www.dhs.gov/protective-security-advisors](http://www.dhs.gov/protective-security-advisors).

The PSAs in Pennsylvania are:

- **Central and Eastern Pennsylvania** – Stephen P. White, Stephen.P.White@dhs.gov
- **Greater Philadelphia Region** – William J. Ryan, William.J.Ryan@dhs.gov
- **Western Pennsylvania** – Robert Winters, Bob.Winters@dhs.gov

The regional CSA is:
- **Bradford J. Willke**, Bradford.Willke@dhs.gov
The PaCIC was formed in 2003 by the Pennsylvania State Police with the goal of proactively addressing the threats posed to our citizens from criminal and terrorist acts by sharing state police intelligence resources with criminal justice agencies in Pennsylvania and nationwide. The PaCIC’s mission has expanded to include providing information bulletins to critical infrastructure partners as well as providing a means to report suspicious activities or emerging threats.

For more information on PaCIC, including applying to receive informational bulletins, please email or call: SP-ProtectPA@pa.gov, 855-772-7768.

The Pennsylvania Office of Administration (OA) is responsible for ensuring the cybersecurity of the Commonwealth network systems. OA has a website with information and resources related to cybersecurity that is available to the public.

The website can be accessed here: www.cybersecurity.state.pa.us.

Utilities are responsible for managing cybersecurity as part of their overall security planning and readiness. Jurisdictional utilities are required to self-certify that they have developed and maintained their security plans on an annual basis. Utilities cybersecurity plans are subject to audit by the Commission.
For more information on the Commission’s self-certification forms, visit:
www.puc.pa.gov/general/onlineforms/pdf/FAQ_PUSPR_Self_Certification.pdf (PDF)
or
www.puc.pa.gov/general/onlineforms/doc/FAQ_PUSPR_Self_Certification.doc (Word)

To download a Commission self-certification form, visit
www.puc.pa.gov/general/onlineforms/pdf/Physical_Cyber_Security_Form.pdf (PDF)

PENNSYLVANIA GOVERNOR’S OFFICE OF HOMELAND SECURITY

The Office of Homeland Security (OHS) coordinates homeland security functions among federal agencies, state government, regional task forces, local government, and the private sector. OHS is a source for general information about cybersecurity in the state.

More information is available at www.homelandsecurity.state.pa.us.