Working from Home Securely

Baseline security requirements for your home environment

PG&E®

January 2021

Table of Contents

Why This Guide?

With our new normal, more of us are working from our homes than ever, and we must ensure that we take precautions to secure the information and technology assets in our homes from the risks of accidental exposure and damage.

The goal of this guide is offer requirements from SEC-1001S: User Responsibility Standard (and a few from IT-5302S: Information Classification and Protection Standard) that are especially salient to a home office environment. This guide also offers general security best practices.

You might consider using all of this information for your own home security!

NOTE: This guide includes baseline security requirements. It does not cover all security requirements for working remotely.

Securing Your Space

Physical & Logical Access Controls

My home has great security! What could go wrong?

Ideally, we feel more safe and secure in our homes than anywhere else. Regardless of how safe and secure you feel, it’s important to remember that every work environment comes with its own set of risks.

Evaluate the security risks within your environment and take appropriate measures to ensure the proper safeguarding of company technology assets and information. For example, if your partner runs a day care out of your home, take extra precautions to secure company assets, such as ensuring your office door is locked while not in use.

It doesn’t matter if you’re working in the office, at home, or on the road, all Security Standards still apply.

What home office? I work in my kitchen!

If a locked door isn’t an option, consider using locking drawers, such as in a desk or filing cabinet to securely store smaller devices or sensitive printed information.

NOTE: You must have a print from home exception to use a personal printer!

SEC-1001S Requirements

Access to PG&E Assets

1.1 You are responsible for keeping your authentication credentials secure (e.g., PG&E access badge, passwords, PIN codes).

1.2 You are responsible for any actions taken when using your company-assigned PG&E access badge and login credentials.

1.4 You are required to secure all sensitive information on your workspace at the end of the workday and when you expect to be away from your workspace for an extended period of time. This includes both electronic and physical hard copy information.

1.5 Computer workstations/laptops must be locked, logged out, or shut down when unattended and at the end of the workday.

Working remotely is riskier

Working from home is inherently riskier because your home network doesn't have the deep layers of security controls protecting it as PG&E networks. Keep this in mind when using PG&E devices and always use your VPN when you go online.

SEC-1001S Requirements

Remote Access of PG&E Networks

1.7 You are expected to comply with the requirements in SEC-3009S: Remote Access Standard.

1.8 You must only use approved methods when remotely accessing PG&E networks, such as a virtual private network (VPN) or Citrix.

NOTE: PG&E reserves the right to block any internet site or service. Content categories that are not specifically blocked are monitored closely and will be blocked as necessary.

Did you know – Virtual Private Networks

A VPN encrypts all of your internet traffic, so that it is unreadable to anyone who attempts to intercept it. This keeps your information safe from the prying eyes of cyber snoopers.

Do you use Wi-Fi?

The Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) and your PG&E Cybersecurity organization recommends that you secure your wireless network by changing your default password, encrypting the data on your network, and more. Review all their recommendations for securing your home network here.

What's Logical Access?

"Logical access" refers to the tools and protocols used for identification, authentication, authorization, and accountability in computer security. At PG&E, you gain logical access with your LAN ID and your password, aka, your login credentials.

Your login credentials are how the system identifies you. If someone else uses your login credentials, the system will think that it is you.

Password Do's and Don'ts

DO

- Keep passwords, PINs, and other security access codes secure.
- Use only your assigned login credentials (e.g., your LAN ID and password) to access technology assets.
- Use different passwords on every system and account internal and external to PG&E.
- Log out of active sessions (Ctrl + Alt + Delete, then select “Sign out”) before allowing another user access to your company-owned device.

DO NOT

- Share your password with anyone, unless requested for PG&E Security investigational or eDiscovery purposes.
- Write passwords down, unless you lock them out of sight.

Password Managers

Too many passwords to keep straight? Try a password manager! The ITStore offers KeePass, PG&E’s approved password manager.

With a password manager, you only need to remember one password - your password manager’s! The app can create long and strong passwords for you and store them along with your username for that account.

Securing Company Assets

Device Protection

Blurred Lines

While working out of the home, it’s natural to consider our company-issued laptops and smart devices as really “ours.”

Think twice, however, before distracting your child with your company mobile device or letting a house mate look something up online from your workstation! PG&E standards state that IT technology assets are for authorized users only.

While PG&E allows limited personal use of company devices, it’s best to keep work and personal activities on separate devices. Make compliance easy by only using company assets for company purposes.

SEC-1001S Requirements

Device Protection

2.1 You are responsible for protecting your company-issued technology assets from unauthorized access and theft.

2.2 Only authorized PG&E employees or non-employee workers may use company-owned technology assets.

2.3 You may allow other authorized users use of your assigned technology assets, so long as you log out and they log in using their own credentials.

Device Protection Do's and Don'ts

DO

- Physically secure mobile devices with a lock or compensating control at all times.
- Keep hardware tokens physically separate from mobile computing devices when stored for travel.
- Be aware of your surroundings at all times, practicing situational awareness, especially when using mobile devices in public.
- Use approved remote access methods when connecting to public wireless networks (Wi-Fi), such as a virtual private network (VPN).
- Secure smaller technology assets when not in use (e.g., in a locked drawer).
- Lock your screen (Windows Key + the letter "L") when leaving your workstation.
- Check the MyITServices intranet page before installing smart device operating system (OS) updates, to ensure IT approval.

DO NOT

- Leave technology assets unattended in public places or open company areas, such as break rooms, conference rooms or outside of restrooms.
- Leave technology assets unattended in vehicles, unless compensating controls are used.
- "Jailbreak" or "root" company-owned or Bring Your Own Device-enrolled (BYOD) smart phones or tablets.
- Store personal data (e.g., music, photos, tax returns) on technology assets.
- Store company information on personal technology assets unless it is enrolled Bring Your Own Device (BYOD) program.

Securing Information

Information Protection

Did you know – Pre-Classified Data Elements

Customer Care and Human Resources have lists of pre-classified data elements. Everyone is encouraged to use these handy guides when classifying information.

Information Classification & Protection Requirements

IT-5302S Information Classification

4.1 Personnel who use PG&E information are responsible for explicitly or implicitly classifying information, regardless of media type, into one of four categories:

4.1.1 **Public:** Information available to anyone inside or outside PG&E without restriction. ‘Public’ information can be disclosed or disseminated without any restrictions on content, audience, or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules.

4.1.2 **Internal:** Information intended primarily for use within PG&E. ‘Internal’ information can be disclosed or disseminated by its owner to third parties for authorized business purposes only. Information is to be used for PG&E business purposes only, without any restrictions on content or time of publication.

Information Classification & Protection Requirements

IT-5302S Information Protection

4.1.3 **Confidential:** Information intended for use within PG&E on a “business-need-to-know basis.” Confidential information, if unintentionally disclosed or disseminated, may incur negative publicity, and is likely to cause financial or reputational damage to PG&E.

4.1.4 **Restricted:** Information that is the most sensitive due to its significant value to the company and requires the maximum level of handling and protection from unauthorized collection, access, use or disclosure. Restricted information, if unintentionally disclosed.

4.6.1 Confidential and Restricted information contained in a physical document must always be attended or physically secured; when not in use the information must be physically secured (e.g., in a locked drawer, cabinet, or safe).

4.6.5 Restricted, Confidential, Internal, and Public information must be stored in an authorized location.

NOTE: Ensure that you’ follow Enterprise Records and Information Management (ERIM) requirements while working remotely!

Information Classification Guides

The Information Classification and Protection Standard has attachments offering more guidance and requirements.

- Appendix A: **Approved Electronic Data Storage**
  Details the approved storage options for PG&E Public, internal, Confidential, and Restricted Information
- Appendix B: **Information Classiication and Handling Guide**
  Offers considerations and examples to assist with classifying information.
- Appendix C: **Questionnaire**
  A series of yes and no questions to help you verify that information should be classified Confidential or higher.

SEC-1001S Requirements

Information Protection Don'ts

DO NOT

- Store company information on personal technology assets unless it is enrolled Bring Your Own Device (BYOD) program.
- Send or transfer company information to personal accounts or systems for work or personal purposes.
- Use unapproved cloud services, such as DropBox to store or transfer company information. Learn more about approved methods of securely transferring files here.
  NOTE: you may receive information from external parties via well-known file transfer services, but only for business purposes.

SEC-1001S Requirements

Electronic Communications Do's and Don'ts

DO

- Use email security best practices, such as not clicking embedded links or downloading unexpected attachments.
- Double-check the email address field to ensure the email is going to the intended recipient.
- Use company-authorized options for accessing PG&E email while working remotely.

DO NOT

- Send confidential or restricted company information external to PG&E without the appropriate approvals and controls, such as encryption or Third Party Vendor Risk Assessment.

Keep Company Information on Company Assets

PG&E's information is one of its most valuable assets. It's important that the company knows where its information is and has strict guidelines for its protection. That's why it's against company standards to send or transfer company information to personal accounts or systems for work or personal purposes.

Phishing & Other Scams

What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

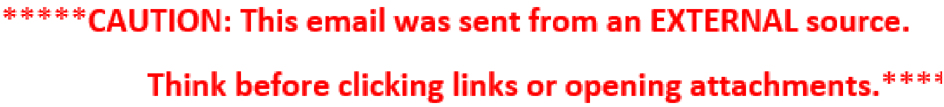
Phishing is one of the most popular cyber scams out there, and from individuals to massive enterprises, nobody is safe from being targeted.

Phishing Red Flags

The best way to protect yourself and PG&E is to familiarize yourself with **phishing red flags** including:

- Red external email banner.
- Alarmist messages and threats of account closures.
- Promises of money for little or no effort.
- Deals that sound too good to be true.
- Any event in the news, such as requests to donate to a charitable organization after a disaster.

Learn more about phishing here.



*****CAUTION: This email was sent from an EXTERNAL source.

Think before clicking links or opening attachments.****

Phishing Goes Beyond Email...

Phone calls (a.k.a., voice phishing or “vishing”). A common vishing scam is from criminals claiming that your iCloud has been breached, the goal being for you to give your login credentials.

Another common scam are people alledging to be from PG&E warning customers that their power is going to be cut off unless they pay their bill immediately.

Text and instant messages (a.k.a., SMS phishing, or “smishing”). Smishing messages are designed to elicit personal and financial information from victims so fraudsters can gain access to their identity, bank accounts and credit cards. Typical smishing scams include messages claiming that you’ve won money, or that your banking information has been compromised.

Did you know — Phishing Vulnerabilities

The remote worker growth spurred by the pandemic has led to an exponential increase in phishing attacks. Our Monthly Phishing Campaigns show that PG&Ers are more susceptible to campaigns that have subject lines related to COVID 19 or operational messages.

Hardware & Software

Keeping IT Assets Clean

SEC-1001S Requirements

Software Requirements

5.5 You are prohibited from installing personal or commercial software, shareware, freeware, adware, or any other software onto PG&E computers.

DO

- Use the ITStore to acquire and install software.

Hardware Requirements

5.2 Using personal peripherals (e.g., monitors, keyboards, docking stations, and webcams) is acceptable when working from home.

5.3 Using personal printers is prohibited unless you have a valid Print from Home Exception.

5.4 You are prohibited from connecting personal storage peripherals to company-owned technology assets (e.g., USB drives, smart phones, digital cameras).

SEC-1001S Requirements

Hardware Do's and Don'ts

DO

- Use company-approved channels to acquire PG&E-owned IT Assets.

DO NOT

- Plug in removable storage media into personal docking stations when company computers are connected.
- Use USB ports on technology assets to charge or power devices, such as fans, personal smart phones or tablets (unless enrolled in the Bring Your Own Device program), or other items. Such items may contain malicious content.

Did you know – Docking Stations

When a laptop is connected to a docking station, the docking station acts as an extension of the laptop. That's why it's against company standards to use the docking station's USB ports for personal devices.

Telephones

Video & Teleconference Calls

SEC-1001S Requirements

Conference Calls

6.1 You are responsible for ensuring that your conversations cannot be overheard while discussing sensitive information.

6.2 When hosting video or teleconferencing calls, you must use company-approved tools, such as Microsoft Teams

Did you know – Conference Calls

The Information Classification and Protection Standard requirements apply to video and teleconference calls.

- Consider your surroundings when you're discussing sensitive information, are other people within earshot?
- Does everyone on the call have appropriate access rights to what's being discussed?
- Turn off Alexa and other digital home assistants that may record you
- Video chatting? Check out what's going to be on camera and move sensitive items prior to call
- Protect access numbers and personal identification numbers (PIN) as you would a password.
- If the host's videoconferencing tool isn't PG&E-approved, use the tool's web attendance option, when attending a videoconference. Learn more here.

Reporting

Knowing How to Respond

Cybersecurity Event

Suppose a message appears informing you that all of your computer files have been encrypted and you must pay to have them unencrypted, or you open an email attachment that takes you to an Internet site and then suddenly your computer starts acting strangely? Contact PG&E Security at 800-691-0410 right away to report the situation!

Loss, Theft, Vandalism, and Incident Report

If you know that a valuable PG&E asset was stolen, immediately contact PG&E Security at 800-691-0410. You must also file a police report in the county where the theft occurred, which can be done on the phone, or online. Once you've reported the theft, fill out a Loss/Theft/Vandalism/Incident form online. If the asset was lost, fill out a Loss/Theft/Vandalism/Incident form online.

Data Loss Event

Data Loss Events (a.k.a. data breach) can occur accidentally, such as emailing a file containing customer information to the wrong recipient, or as the result of an intentional, malicious act, such as stealing documents or system information. Call the TSC at 415-973-9000 as soon as possible.

More Information

Knowing Where to Look

Security Guidance Documents

Security Policies, Standards, and Procedures:

The PG&E Guidance Document Library — SEC category

- http://pgeweb.utility.pge.com/guidance/Pages/Security-SEC.aspx

The Security intranet site - Select “Standards and Procedures” from the Toolkit

- http://pgeweb.utility.pge.com/security/standards/Pages/default.aspx

The Technical Information LIbrary (TIL) perform a Title Search for “PG&E CIP”

Security Intranet Site

Type *security/* in your internet browser’s address bar.

NOTE: You must be connected to the PG&E network using a PG&E VPN connection.

Security Questions

Send your security-related questions, requests, and comments to SecurityCommunications@pge.com