9 Security Guidelines for Working Remotely

Review and implement the following guidelines to ensure your personal information is properly protected while you work remotely. These guidelines should be implemented on any device (Yale-owned or personal) being used to access university data or resources.
We know that working from home can be new to some of you, perhaps overwhelming as you adjust to your new environment. One of our goals is to enable you to work as securely as possible from home. Below are nine steps to working securely. These steps not only help secure your work, but they will make you and your family more safe as you create a cybersecure home.

1. **YOU are the best defense.**

Technology alone cannot fully protect you – Be vigilant and aware.

Attackers have learned that the easiest way to get what they want is to target you, rather than your computer or other devices. If they want your password, work data or control of your computer, they’ll attempt to trick you into giving it to them, often by creating a sense of urgency. For example, they can call you pretending to be Microsoft technical support and claim that your computer is infected. Or perhaps they send you an email warning that a package could not be delivered, fooling you into clicking on a malicious link that downloads malware to your computer, allowing your information to be accessed (i.e. phishing).

Common indicators of these types of cyber attacks include:

- Someone creating a tremendous sense of urgency, often through fear, intimidation, a crisis or an important deadline.
- Pressure to bypass or ignore security policies or procedures, or an offer too good to be true (no, you did not win the lottery!).
- A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them.

For more tips and tricks on how to recognize phishing, copy and paste the following into your browser: [cybersecurity.yale.edu/covid19phishing](cybersecurity.yale.edu/covid19phishing).

Yale Information Security
Secure your home network.

Almost every home network starts with a wireless (often called Wi-Fi) network. This is what enables all of your devices to connect to the Internet. This means securing your wireless network is a key part of protecting your home.

We recommend the following steps to secure it:

- **Change the default administrator password:** The administrator account is what allows you to configure the settings for your wireless network. An attacker can easily discover the default password that the manufacturer has provided.

- **Allow only people that you trust:** Do this by enabling strong security so that only people you trust can connect to your wireless network. Strong security will require a password for anyone to connect to your wireless network. It will encrypt their activity once they are connected.

- **Make passwords strong.** The passwords people use to connect to your wireless network must be strong (at least 12 characters long with a mix of upper and lower letters and characters). Remember, you only need to enter the password once for each of your devices, as they store and remember the password.

Not sure how to do these steps? Ask your Internet Service Provider, check their website, check the documentation that came with your wireless access point, or refer to the vendor’s website.

*Note: The ITS Help Desk won’t be able to assist you with securing your home network.*
Utilize Yale's VPN when necessary.

A Virtual Private Network (VPN) takes your Internet connection and makes it more secure. While most telework can be done without using Yale’s VPN, it should be utilized whenever:

- You are working from an unsecured Internet connection (e.g. at a hotel or coffee shop on free Wi-Fi) on your laptop, tablet, or mobile device.
- Yale services or applications require VPN (e.g., TMS).

Yale’s VPN is a shared resource, and usage will be higher than usual when campus is closed or under any state of emergency. Avoid using the Yale VPN unless absolutely required in order to preserve capacity for all.

For more information on Yale’s VPN, visit: [Off Campus Access VPN: Connecting to VPN](#).
Ensure each of your computers, mobile devices, programs, and apps are up to date with the latest software.

Cyber attackers are always looking for new vulnerabilities in the operating system and software your devices use. These vulnerabilities in software are like unlocked doors to your device. The hackers use these open doors to gain unauthorized access to your data and devices. Updates address identified security vulnerabilities.

Please note: A Yale-managed device is the default option and must be used where feasible.

Please review University HIPAA Policy 5100.15 for requirements on personal computers and remote access within the covered entity.

You will need to:

- Ensure your computer is running a supported operating system
  - For Windows: Windows 10
  - For Macs: macOS 10.14 (Mojave)

- Install available updates to your applications, browsers, and browser extensions.

- Enable automatic updates (security patches) whenever possible on all devices. This includes your work device(s) as well as personal devices – phones and tablets, internet-connected TVs, security cameras, and gaming consoles.
Cyber Viruses, and other types of malware, can wreak havoc on a computer.

They can slow down the computer, damage or delete files, cause computer crashes and data loss, and more. Anti-virus solutions are used to protect against viruses and other cyber threats. Anti-virus is required for all devices accessing Yale data or the Yale network.

How can I get Anti-Virus?

If your device is not running an updated Anti-virus solution, you can install Trend Micro through Yale’s Software Library. Open software.yale.edu and search for “personal antivirus“.

What should I do if I believe my device was infected?

If you have any reason to believe your device was infected based on the symptoms above, immediately stop using the device and contact the ITS Help Desk at 203-432-9000.
Encryption protects the data on your device from unauthorized access by scrambling it into an unreadable code, in the event the device is lost or stolen.

If the disk is not encrypted, a bad actor could easily extract and utilize the unencrypted data either through a USB storage device or by mounting the hard drive to another machine to examine the data.

**How can I encrypt my device?**

Windows and Macs can view the [Desktop Encryption Guide](#) for directions on how to encrypt the device.
Avoid saving data on personal devices or printing Yale data on a personal printer.

To best protect Yale data, do not save Yale data on your device. Instead, save information in secure locations such as:

- Yale Secure Box or One Drive (required for Yale high risk data or potentially sensitive information).
- Box at Yale or Eli Apps (easy file sharing and collaboration for moderate and low risk data).

For a complete list of services available to the Yale community for high, moderate, or low risk data, visit Yale’s Protect Your Data website. This site provides a list of applications by data classification that you can use to access, store, and share Yale data securely.

How do I know if I am working with high or moderate risk data?

High and moderate risk data are classifications for Yale’s sensitive or confidential information. Visit Yale’s Protect Your Data website or review Yale’s Data Classification Policy to determine if you are working with high or moderate risk data and to determine what services you can use to appropriately access, store, or transmit this data.

Personal Printers

As a reminder, printing Yale confidential or sensitive data (high or moderate risk data) is not permitted.
Ensure each of your computers, mobile devices, programs, and apps are up to date with the latest software.

If Yale data is stored on your personal device while working remotely, that data should be deleted immediately once it is no longer needed. If the data is needed until you are back on campus, the data should be securely transferred to your Yale device and completely deleted from your personal device.

As a reminder, encrypted USBs must be used for transferring sensitive or confidential (i.e., high or moderate risk) data. Non-encrypted USBs are not permitted. If you are unsure if the USB is encrypted, you should assume it’s not.

What are other ways to securely transfer my data?

- Use secure cloud services. (See #7)
- Use encrypted USBs.
- Use encrypted email.

How can I securely delete my data?

You can securely delete the data by erasing the data from both:

- Where it is stored on the device.
- The recycle bin.
Limit secondary use of devices.

Something you most likely don’t have to worry about at the office is children, guests or other family members using your work laptop or other work devices.

Make sure family and friends understand they cannot use your work devices. This is because they can accidentally:

- **Erase or delete data:** family members may close or delete important information before you have the chance to save and store it securely.
- **Modify important information:** Family members, specifically kids, may touch and change important documents, compromising the integrity of your work.
- **Infect the device:** Family members may want to download applications and games. Doing so puts the device at risk if they accidentally download malware – software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. It is best practice to only download applications or software – whether work related or not – from a known, trusted source.

**Tips for ensuring friends/family do not access the device:**

- Lock the device when you walk away.
- Ensure your device is protected with a **strong password**.
- If appropriate, consider locking the door where your computer is set up to avoid unwanted access to the device.