COLORADO
Governor's Office of
Information Technology

TECH KIT: GUIDELINES & RESOURCES FOR REMOTE WORKERS

Last updated: 4.1.20

This Tech Kit provides guidelines, resources, and best practices for remote workers. The information below can help answer many of your tech-related questions. Please read through this document before you begin working remotely, and prior to contacting the OIT Service Desk.

This Tech Kit does not supersede any specific policies or procedures in place for your agency. The guidance below will be updated as needed by the Governor's Office of Information Technology.

Getting Started

Before you begin working remotely, consider this guidance:

- Plan to use your state-provided computer if possible. If you need to work remotely without warning, your personal computer may be used to work in your state Google account. Note: In the midst of the COVID-19 situation, consider getting in the practice of taking your state-issued laptop home.
- Ensure you have access to the internet and are able to connect your state laptop to your home Wi-Fi. If you need assistance, contact the OIT Service Desk (see Assistance section at the end of this document). You can find tips in the Wi-Fi Security section.
- Plan to have a mobile phone or landline available, but **do not use call forwarding** to transfer incoming calls from your desk phone. Instead, update your voicemail personal greeting and if necessary, provide a phone number at which people can reach you while teleworking.
- OIT recommends **using a surge protector** when powering your devices.
- **Password Self-Service** allows you to reset or unlock your network password (the password used to log in to your state computer) without contacting the OIT Service Desk. The Password Self-Service User Guide will help you get set up. *Note: Password Self-Service is NOT yet available for DOR, HCPF, DOC, DMVA and CDPS employees.*
- Click here for a special edition of OIT Connections dedicated to best practices for working remotely and cybersecurity.

ACCEPTABLE USE POLICY & USE OF PERSONAL DEVICES

Acceptable Use of State IT Resources

The statewide Acceptable Use of State Data & IT Resources Policy (also known as the Acceptable Use Policy or AUP) provides state employees and other authorized users (e.g., contractors, interns, etc.) guidance on the proper use of and access to state technology resources. Here are a few key points, however, please review the AUP to make sure you are familiar with all guidance before you telework.

- The policy applies to the use of a state computer in both the office and a remote location.
- State business should be conducted in most cases on a state-provided computer. VPN access is only permissible from a state-provided computer.
- Even when working remotely, personal business should not be conducted on a state computer.
- State-provided computers come with software to protect you from viruses, etc. Do not disable or remove any software from your state computer. Additionally, do not download any software or apps unless authorized by your supervisor to do so.
- Removable storage devices such as flash drives, external drives, etc. are not permitted since they can introduce malware onto the system. These storage devices should not be used to store state data either.

Use of Personal Devices

When using a personal device to conduct state business, you must comply with the guidelines found in the AUP. It is incumbent upon you to read the AUP in its entirety to ensure you understand your responsibilities.

Before using a personal device make sure:

- All of your software is up to date. This includes the operating system, antivirus and security software, etc.
- It is free from malware infection and running anti-malware protective software.
- It is protected by strong authentication, such as a password or PIN.
- It is set to automatically receive security and operating system updates.

Do not save any work-related documents to your personal device.

In accordance with the AUP, the use of personal computers is not allowed when using a remote access tool such as eVPN.

Personal Phones

- You may use your personal phone to participate in meetings or to conduct state business in general.
- You may also download Google apps onto your personal smartphone and log in using your state credentials to access Gmail, Docs, and your Calendar. You can download each of the apps from the Apple App Store or the Google Play Store.
- Do not download or save work-related documents to your personal smartphone.

REMOTE ACCESS TOOLS

Remote Access Tools / VPN (e.g., Cisco AnyConnect, Citrix, CheckPoint, GlobalProtect, NetMotion)

Some state systems require a user to be on the state network or to utilize a remote access solution such as Cisco AnyConnect Secure Mobility Client (eVPN), CheckPoint, NetMotion, or Citrix. Most staff who access these state systems are already using a remote access solution that is installed on their computer. However, if you would like to request access, please submit an OIT Service Desk ticket.

When using a remote access solution from home, please keep the following in mind:

- Your internet connection may be slower than your office location.
- There is a limit to the number of people who can use eVPN to connect to the state network. Please be considerate of others who may need to use this remote access tool and log out when you are done accessing state resources. Note: After three hours of inactivity, remote access will be automatically disconnected to free up network capacity.
- VPN connectivity is not permissible from a personal device.
- To help ensure adequate bandwidth for all state employees, OIT has restricted VPN and office access to all audio and video streaming services (e.g., Spotify) except those required for business purposes. Streaming services may be used through personal internet connections while not connected to VPN. *Note: State residential nursing facilities will retain access to Netflix.*

NOTE: To reduce the need for remote access to the state network, any files you have saved on a network drive should be copied to Google Drive. Click here for instructions on how to upload files to Drive.

Examples of commonly used software and systems:	
VPN not required: ● Google G Suite ● Microsoft Productivity Suite ● Adobe ● Contract Management System (CMS) ● CPPS - QWS3270 & TSS (“Green Screen”) ● Hyland Onbase ● Kronos v 8.0 (OIT, CDA, CDPS, CDLE, Governor’s Office, Dept of Law, and Dept. of State) ● Salesforce ● Perceptive Web Client (e.g., forms and approvals)	**VPN required:** ● CPPS Web Client (payroll system) ● CORE ● EDW ● Employee Self-Service (ESS) ● Financial Data Warehouse (FDW) ● HRDW ● Kronos v 5.2 (CDHS,DPA, DNR, CDPHE) ● Perceptive Deskside Client (e.g., back end accounting functions) ● PPMS

Helpful Resources:

- eVPN: Overview
- Installation Guide: Cisco AnyConnect
- Video Tutorial: Connecting to Cisco AnyConnect for eVPN
- User Guide: Setting Up Two-Factor Authentication (2FA) for eVPN
- User Guide: Global Protect
- Video Tutorial: Installing and Connecting to GlobalProtect
- User Guide: NetMotion
- User Guide: Connecting to Citrix

GOOGLE | G SUITE TOOLS

Gmail & 2-Step Verification

The main collaboration and productivity tools for state employees can be found within your state Google account. Your state Google account can be accessed directly through your home internet service. You may be prompted to enter a verification code. You will continue to receive your code as you normally do—on your smartphone, desk phone, etc. If that device will not be accessible to you from home you may need to change the way you receive your passcode. Information on how to receive 2-Step Verification codes, video tutorials, and more can be found here.

If you are unexpectedly required to work remotely, you can and are allowed to log in to your state Google account on a personal computer or by using any of the Google apps like Gmail, Calendar, or Docs on your personal smartphone. Your state Google account is protected with a higher level of security then your personal Gmail account so **there is no need to use a state network remote access solution when working in your state Google account.** If you are using a personal device, **do not download any files or folders related to state business onto your personal computer or device**.

Google Tips & Tricks for Working Remotely

If you do not regularly work remotely, there are some best practices that will help you get the most from your state Google tools. Here are some tips to help you get started and make the most of Google's collaboration suite while working remotely.

Google Virtual Office Hours

The OIT Google Team will offer virtual open office hours starting Monday, March 23, at 11 a.m. to answer any questions you may have about G Suite apps. Please use this link to add the event to your calendar or join with this Meeting Code. If you have any questions for the Google Team, you also can use this form.

STATE-ISSUED DEVICES: TELEPHONES & DESKTOP COMPUTERS

Telephones & Teleworking

Desk phones

- **Do not use call forwarding** to send calls from your desk phone to a cell phone or another landline. This takes up valuable network capacity. Instead, update your voicemail message to indicate that you are working remotely and include the number where you can be reached (cell or landline).
  - Depending on your role, you may want to update your voicemail message and point callers to covid19.colorado.gov if they have questions, and then offer an alternative way to reach you.
- Be sure to regularly check for voice messages (at least once per hour).
  - Cisco IP Phones: to access your voicemail remotely, call your phone number (including area code), press the * key. When prompted, re-enter your phone number and password, followed by the # key. (Information about other features of the Cisco IP Phones can be found in this Cisco IP Phone and Voice Mail Quick Reference Guide.)
  - Avaya: to access your voicemail remotely, dial your office telephone number. Press 8 to interrupt the voicemail greeting. Enter your access code to begin listening to your messages.

Desktop Computers & Teleworking

While **OIT strongly advises against taking state-issued desktops home to telework**, it is possible to do so. Permission from your agency leadership is required before proceeding in this direction.

- **Security.** If permitted to use your state-issued desktop to telework, please submit a Service Desk ticket to request that encryption be added to your computer. This is required to secure state systems.
- **Remote Access Tools.** Desktop computers are not configured with the remote access tools (e.g., eVPN, CheckPoint, Citrix, NetMotion) required to connect to the state network remotely. Submit a Service Desk ticket if you need remote access tools loaded on your desktop computer.
- **Hardware.**
  - Most desktop computers do not have the ability to connect directly to Wi-Fi and would require an additional device or adapter to be purchased and installed by the agency.
  - Desktops must be adjusted to work on your home network and there is no guarantee that they will actually connect with reliability.
  - You may need to take home a monitor, keyboard, mouse, and network cable.
- **Damage.** Be mindful that desktops are far more fragile than laptops; if the desktop is not moved correctly it can shake items loose like memory, video, and network cards.
- **Support.** OIT is unable to dispatch support staff to employees' homes to assist with setup issues. The OIT Service Desk can only provide general setup guidance (e.g., connecting a desktop to a monitor and Wi-Fi).

CONDUCTING BUSINESS WHILE TELEWORKING

Virtual Meetings & Conference Calls

- **Virtual Meetings.** There are various options for holding online meetings, all of which require the host to have internet access. Participants can join using a computer, smartphone or tablet.
    - Google Meet. Allows you to host up to 250 participants in a single meeting.
    - Google Livestream. Allows you to host up to 100,000 people with an @state.co.us email address in a single meeting.
    - Zoom - Allows you to host up to 100 participants in a single meeting.
    - WebEx. Allows you to host up to 100 participants (200 if you have a WebEx license) in a single meeting. Participants do not have to have an @state.co.us email address to participate. Users can join via browser or (depending) will be offered to download a temp application.
        - Cisco. Want to connect to a WebEx meeting through a Cisco DX80 or MX800/700 video unit? Read the quick start guides at the top of the Cisco Devices page on TechU.

- **Conference Calls.** There are three options for hosting a traditional conference call.
    - CenturyLink Conference Bridge. If you have a pre-assigned conference bridge, you can use that to host up to 300 audio-only participants.
    - Google Hangouts Meet. When you schedule a meeting in Google Calendar, a conference bridge is automatically created as soon as you add guests to your meeting invite. Hangouts Meet brings together participants who call into the meeting and those using the URL to join via video conference. There is no need to both dial in and join via the URL for Hangouts Meet unless your computer does not have a microphone.

COLORADO
Governor's Office of
Information Technology

TIPS FOR WORKING SAFELY & SECURELY ONLINE

Cyber threats and associated malicious acts through phishing, ransomware, malware, and hacking are geared toward tricking the unsuspecting user and acquiring access to their state system and/or personal information. Although OIT provides a robust system to protect computers, systems, and the state network from cyber attacks, state employees are truly on the front line when it comes to protecting state data. These tips will help you work securely and safely while online.

General Security

- Attackers are expected to try to take advantage of employees working from home, and will be attempting to trick them into taking actions, capitalizing on the fact that the employee can't immediately validate face-to-face with co-workers or managers. Validate any urgent requests, out of band, whether from a customer, manager, or executive, before providing information, clicking on a link, opening a document, transfering money, or downloading/installing something.
- As you do when you are at the office, make sure that the information on your screen is not visible by others in your home and lock your computer when you walk away from it.
- Similarly, ensure that work discussions cannot be easily heard by others in your home (i.e., shut the door). Use a headset, if available, rather than speaker phone.
- Do not allow others, including family members or roommates, to use your work computer.
- Avoid using public computers and/or public Wi-FI to access, process, store, or transmit data.
- You can find more guidance on working securely from home here.

Email Security

- Be even more vigilant and skeptical of unsolicited email and watch for phishing attacks.
- Do not keep your personal email open on the computer you are using for work; access personal email from a different computer.
- Be wary when opening emails and do not click on links from people you do not know.
- Do not provide state or personal information in response to an email, pop-up webpage, or other communication you did not initiate.
- Manually encrypt email messages containing sensitive information that may not contain the keywords that trigger Zix to auto-encrypt the message. To manually encrypt an outgoing email message, simply type the word "encrypt" in the subject line. Click here for additional information on how to use Zix, retrieve a Zix-encrypted email, and FAQs.
- Do not use your personal email to conduct state business.

Laptop Security

- When transporting your laptop from your work location to a remote location, do not leave it visible and accessible in your vehicle. Lock it in your trunk if you must make a stop between your office and your home.
- Do not take it with you into shopping centers, restaurants, or bars.
- Be sure to take your power cable with you, as well as any other necessary devices such as a webcam or microphone.

Mobile Device Security

- Keep your device in a secure spot and know its whereabouts at all times.
- Switch off your Wi-Fi and Bluetooth connections when not in use.
- Ensure your mobile device is protected by a strong PIN and configured to lock automatically when not in use.

Wi-Fi Security

- If you are having difficulty with your home Wi-Fi, contact your service provider. The OIT Service Desk will not be able to assist with this issue.
- The default username and password of home routers are freely available and known to attackers. Change the default password to a complex password or an easy-to-remember passphrase. OIT's password standards can be found here.
- Before you log into a site, and if your transaction contains sensitive information (e.g., password, credit card, etc.), confirm that connections are secure (HTTPS).
    - The "s" in "https" stands for "secure" and indicates that communication with the webpage is encrypted. Alternatively, look for the lock symbol (it's sometimes green) in the internet address bar.
    - If you do not see the "https" or lock, do not enter a password or any other sensitive data on the website.
- Note: There are different levels of protection on Wi-Fi networks. WPA2 and WPA3 provide the strongest protection, followed by WPA. WEP is the least secure and if possible, should not be used. Depending on your router, you may be able to turn on WPA2 encryption for your wireless networks. If you don't know which level you have, refer to your router manual, contact your internet service provider, and click here to learn more on TechU.

ADDITIONAL RESOURCES

Helpful Links

- **Center for Internet Security.** The CIS Stay Secure at Work and Home Poster provides 11 cyber defense best practices you can use at home or work.

- **Kronos**. On this webpage you will find links for employees and managers to access the Kronos timekeeping system and user guides.

- **TechU**. Provides State of Colorado employees with training, video tutorials, fact sheets, and FAQs on their available tech tools.

NEED ASSISTANCE?

Technical Support

- If you are using a **state-provided compute**r, please call 303.239.HELP (4357), submit a ticket through the Customer Service Portal, or email your OIT Service Desk.
  - Visit the Customer Service Portal page on TechU to find a video showing you how to login as well as a Customer Service Portal User Guide.

- If you are using a **personal computer** and are experiencing a problem with a state system or application, call the OIT Service Desk at 303.239.HELP or submit a ticket using the customer portal at www.colorado.gov/oitcustomerportal. Please note that if you are experiencing a problem with the computer itself, the OIT Service Desk will not be able to assist you.

- If you experience issues with your internet (e.g., bandwidth, router, etc.), please contact your internet provider.

- If you need to reset your network password and your agency has Password Self-Service enabled, follow the Password Self-Service User Guide to set up and manage your account without having to call the OIT Service Desk. You will need to provide answers to security questions and choose secret words, which will be used by the Service Desk to unlock your account if you forget your answers.