TECHNOLOGY GUIDE FOR STATE EMPLOYEES WORKING FROM HOME

1) Office Productivity Tools

a) To run Microsoft Office applications (Outlook email, Word, Excel, etc.): https://portal.office.com

b) Office 365 is a subscription service that allows users to install on five different work or personal computers (Windows/Mac), five phones, and five tablets. https://www.microsoft.com/en-us/home-use-program

c) Training resources for Microsoft Office applications: https://support.office.com/en-us/office-training-center?ms.officeurl=training

2) Caution on Coronavirus Phishing and Scams

a) Scammers are targeting consumers using phishing sites, phony websites, and even telephone based scams. Be cautious and always validate the credibility of any phone call, website, and email to make sure it is legitimate. Report any suspicious activity to your Information Security Office.

a) For more information see: http://www.oesnews.com/california-cyber-security-integration-center-offers-guidance-for-teleworkers/

3) Internet Access

a) AT&T, Century Link, Charter, Comcast, Cox, Frontier, Sprint, T-Mobile, US Cellular, Verizon and many other companies are providing the following services for 60 days:
   - i) Not terminate service to any residential or small business customers
   - ii) Waive any late fees for residential or small business customers
   - iii) Open its Wi-Fi hotspots to any American who needs them

b) When accessing public Wi-Fi, please see the Physical and Data Protection Best Practices section for security safeguards.

4) Personal Computer Protection (Using Non-State Issued Equipment)

a) System and Software Updates
   - i) Ensure the automatic system update feature for your specific Operating System is turned on. For Windows users, go to the Start button, then Settings->Update & Security-> Windows Update, and select "Automatic Updates"
   - ii) Enable other application software, such as browsers and Office software to automatically update
   - iii) For Windows users, only use Windows 10 or other supported Operating Systems (Windows 7 is end-of-life)

b) For Local Computer Passwords: Use complex passwords and PINs: At least 10 characters with upper and lower case letters, numbers, special characters
   - i) Avoid common dictionary words
   - ii) Change passwords periodically
   - iii) Don't use the same password for all of your accounts
     - (1) Using Password Managers helps store and manage multiple accounts securely, for example: https://www.lastpass.com/password-manager

c) Anti-Malware
   - i) Validate you are running anti-malware/anti-virus.
     - (1) Microsoft Defender Anti-malware is available on Windows 10 computers and tablets.
     - (2) MAC/OSX: Useful tips to validate anti-malware (XProtect) protection and other built-in security features are turned on: https://mashtips.com/built-in-mac-security-software/
   - ii) Free Options for anti-malware / anti-phishing / and network security solutions (for 6 months):

(1) Trend Micro Maximum Security: https://resources.trendmicro.com/Work-From-Home-Assistance-Program.html. Sign up using your State email account and optionally install it on your personal computer, smartphone, or tablet.

(2) McAfee LiveSafe: https://www.mcafee.com/stateofcalifornia. To sign up use company code STA3303B35 and a State email account and optionally install it on your personal computer, smartphone, or tablet.

(3) Most Internet Service Providers (ISP) provide free anti-malware/anti-virus products Contact your ISP to check for availability.

d) Optionally, for increased privacy of personal sensitive information use full disk encryption

i) Always encrypt your device to protect your personal data stored

(1) How to turn-on BitLocker on Windows 10 : https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption

(2) How to enable FileVault encryption on a Mac: https://support.apple.com/en-us/HT204837

(3) How to enabled encryption on an Android device: https://it.ucsf.edu/how_do/enable-encryption-android-devices

(4) iOS: Personal data on Apple phones is encrypted by default

5) Personal Phone Protection

a) Mobile Security McAfee LiveSafe: https://www.mcafee.com/stateofcalifornia. To sign up use company code STA3303B35 and a State email account.

b) Other Tools - Free tools to protect your iOS and Mobile devices https://www.trendmicro.com/en_us/forHome/products/free-tools.html

c) Regularly Clean up Privacy Settings on Mobile Devices

i) For iOS: https://apps.apple.com/us/app/mypermissions-privacy-cleaner/id535720736

ii) For Android: https://play.google.com/store/apps/details?id=com.mypermissions.mypermissions&hl=en_US

6) Physical and Data Protection Best Practices

a) Never work at public places such as a coffee shop, etc.

b) It is highly recommended to not connect to public or untrusted/insecure WiFi connections However, if you need to use public WiFi use extreme caution because of malicious and spoofed WiFi hotspots. Here are a few tips:

i) Only visit websites that are encrypted for business and sensitive personal use. This can be identified by looking at the browser address bar to see if the website address starts with HTTPS://

ii) Never ignore browser SSL/TLS certification warning when you access a website.

c) Never disclose confidential or sensitive data to any unauthorized personnel including friends and family.

d) Always lock your computer when leaving it unattended.

e) Do not store State sensitive or confidential information on your personal computer.

f) Store any sensitive or confidential information on encrypted media provided by your department.

g) Ensure confidential paper documents are properly disposed of, i.e. shredding

h) Report security incidents or security concerns to you supervisor immediately.

i) Refrain from using personal email for business use.

j) Always comply with your organizations policies and procedures to protect specific high risk data elements regulated by HIPAA, IRS, PCI, etc.

TECHNOLOGY GUIDE FOR STATE IT ORGANIZATIONS

1) Hardening End User Devices

a) Anti-Malware Resources (at no cost for 6 months):

i) Crowdstrike: https://go.crowdstrike.com/WF-Request-Info-Remote-Workers.html

ii) Trend Micro Maximum Security: https://resources.trendmicro.com/Work-From-Home-Assistance-Program.html

iii) McAfee LiveSafe: https://www.mcafee.com/stateofcalifornia - To sign up use company code STA3303B35

iv) Microsoft Defender Anti-malware is available as part of Windows 10 computers and tablets.

b) Other Security Protection

i) Manage Bitlocker encryption on all computers, tablets, and laptops within your enterprise: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-management-for-enterprises

(1) Note: All devices outside of a State building must be encrypted

c) Microsoft Office 365 Resources

i) Office 365 is a subscription service that allows users to install on five different work or personal computers (Windows/Mac), five phones and five tablets.

ii) For additional information on the following products and more, contact your Microsoft representative.

(1) Enterprise Mobility & Security

(2) Azure Active Directory Premium: Identity Management

(3) Intune Device Management

(4) Azure Information Protection – Data Protection

2) Teleconferencing and Digital Engagement Tools

The list below represents a sample of what is available across the state and includes options to access meetings online, and by phone.

a) WebEx

i) Where to Access: CALNET

ii) For hosts: There are four plans available including a free version, which is not recommended due to the limits on participation and meeting length. Priced plans offer larger participation limits and longer (or unlimited) meeting duration times. More information can be found here.

iii) For participants: Participants can join in a variety of ways -- through an email invite, or by clicking on a meeting link through their desktop or mobile application. Participants do not need an account to access a meeting.

iv) Accessibility: WebEx offers keyboard navigation, low vision support, and screen reader support. WebEx also offers the ability to create automatic transcripts.

v) Capturing Comments & Questions: Meetings set through WebEx come with an automatic chat function (though hosts will need to set user privileges) to take comments and questions.

vi) Also available through CALNET as an option: AT&T Conferencing and NWN.

b) Zoom

i) Where to Access: DGS Software Licensing Program

ii) For hosts: There are four plans available including a free version, which is not recommended due to the limits on participation and meeting length. Priced plans offer larger participation limits and longer (or unlimited) meeting duration times. More information can be found here.

iii) For participants: Participants do not need to have a Zoom account to attend a Zoom meeting. A first time user will be prompted to download the software, and can do so by clicking on a meeting link, or by heading to the Download Center.

iv) Accessibility: Zoom has four key accessibility features: closed captioning, keyboard accessibility, automatic transcripts, and screen reader support. More information can be found here. Each meeting room also comes with a dial-in number, which can be provided to those without reliable internet access.

v) Capturing Comments & Questions: There is a chat function at the bottom of the screen that allows any participant to comment or ask questions. You can save in meeting chat content by following these instructions.

a) Skype Meeting Broadcast

i) Where to Access: Through the Microsoft Office 365 bundle; may have to ask your system administrator to push it out.

ii) For hosts: Enables you to schedule, produce and broadcast meetings or events to online audiences of up to 10,000 attendees. Scheduling instructions are linked here.

iii) For participants: Participants do not need a Skype for Business account to attend a meeting, however members of the public will need to download the software plug-in to participate. Instructions for those steps are linked here.

iv) Accessibility: Skype offers screen reader support, closed captioning, and real time transcription and translation features. For those with less reliable internet access, follow instructions on how to add a dial in number.

v) Capturing Comments & Questions: To enable questions and comments, add a Q&A section that will display during the meeting.

vi) Microsoft is transitioning Skype users to Microsoft Teams, which also is part of Office 365, although departments are just learning about Teams' webcasting functionality.

b) Teleconferencing

i) Teleconferencing can be an important supplement to web conferencing. To add teleconferencing services, call the provider your organization has chosen from the CALNET options and purchase additional services using Form 20.

ii) One service that offers a broad range of features is AT&T Teleconferencing, which can be offered as audio through web browsers, and features scheduling, comment queueing, moderated question and answer session. It also allows voting and polling. Different service levels include translation, question queueing and transcripts.

c) Other Video Tools Available Through CALNET

The following services also are available through CALNET. These services typically are used for point-to-point virtual conferencing and may not provide all of the features necessary for conducting a public meeting.

i) Jive Multipoint Video Conferencing Bridge Service

Multipoint Video Conference Bridge for 6-80 participants. Allows 6-80 participants to join and communicate via both video and audio on the same conference call.

ii) Verizon Managed Video Conferencing Service

Managed Video Conferencing provides Video Conference session support with assistance of a live Conferencing Attendant.

iii) Verizon Open Video Communication Service

OVC is multi-party video conferencing with a variety of usage levels suitable for individual devices to multi-screen telepresence rooms with document sharing.

3) Professional and Advisory Services

The following vendors are offering emergency assistance (e.g., assessment, planning, strategy, guidance, etc.) on a pro-bono or reduced fee basis, depending on the exact needs of the State:

- a) Accenture – Contact is Teri Bennett at (916)202-6608 or teri.bennett@accenture.com. Here is the link to Accenture's information specific to COVID-19: "What to do Now, What to do Next" at https://www.accenture.com/us-en/about/company/coronavirus-solution-elastic-digital-workplace
- b) KPMG – Contact is Todd Jerue at (916)955-2204 or tjerue@KPMG.com. KPMG has a Pandemic Readiness Checklist and a Business Resilience and COVID-19 document available upon request.
- c) Gartner Research and Advisory Services is providing COVID-19 Resource Center assets to use as needed. Gartner analysts are producing content as quickly as possible in an effort to help achieve and maintain business continuity so check often for new content. No Gartner membership is required for the information contained on this page.

4) Remote Access Suggestions for Critical Business Services

- a) Inventory all IT critical services that need to be accessed remotely. Consider classification and sensitivity of data and appropriate safeguards are implemented.
- b) Identify the best way to access each of the critical services
  - i) Ensure multi-factor authentication is used for remotely accessing resources
  - ii) Intranet web applications – Securely expose intranet web applications externally, Virtual Desktop Infrastructure (VDI) or Virtual Private Network (VPN) access
  - iii) Fat client applications - VDI or VPN access
    - (1) Business applications
  - iv) Business services requiring public interaction
    - (1) Call Centers
    - (2) Field Offices (i.e,. DMV Services)
- c) Look at re-platforming or relocating critical services to cloud, if current environment is too limited. For example: Many departments have productivity files and home directories on premises. If access to file shares is a need for telework, consider use of Microsoft's OneDrive, SharePoint, or Teams for departments using Office 365.
  - i) Amazon Web Services
  - ii) Microsoft Azure
  - iii) IBM Softlayer
  - iv) VMware
  - v) Citrix
- d) Network considerations
  - i) Calculate Wide Area Network (WAN) bandwidth requirements
  - ii) Intrusion Prevention System (IPS) capacities
  - iii) Firewall rules
- e) VDI/DaaS Solutions: (Available on the State's FedRAMP Cloud Contracts):
  - i) Amazon WorkSpaces: Amazon WorkSpaces is a managed, secure Desktop-as-a-Service (DaaS) solution. Learn more at https://aws.amazon.com/workspaces/
  - ii) Microsoft Windows Virtual Desktop: Windows Virtual Desktop is a comprehensive desktop and app virtualization service running in the cloud. Learn more at https://azure.microsoft.com/en-us/services/virtual-desktop/