KEY STEPS
for setting up technology for your agency personnel to work from home

INITIAL STEPS
First, talk to IT personnel (who may reside within your agency and/or jurisdiction), when available, to determine what requirements might already be in place to facilitate remote access for your office. These requirements include the following:

• EQUIPMENT
  – Determining what equipment employees will require. This may vary by job or individual (e.g., some may need special equipment under the Americans with Disabilities Act). This equipment may include:
    – Computer
    – Mouse and keyboard
    – Reliable internet access
    – Telephone
    – Printer or scanner
    – Web-cam
    – Digital signing capability
    – Email access
    – Video conferencing access
    – Secure remote access to intranet
  – Performing an inventory of existing equipment and employees to determine needs.

• SOFTWARE
  – Determining pre-existing contracts, vendor licenses, and required applications for work. Ensure that license requirements are being met, and that employees have access to necessary license keys.

• GATEWAYS
  – Ensuring that equipment includes required software or that employees have access to this software. Software can be either pushed-out or downloaded.

• POLICIES, PROCEDURES, AND PROTOCOLS
  – If purchasing new equipment, determine the following:
    – Budget and spending authority
    – Shipping location for equipment
    – Availability of required equipment and timing of delivery
    – Whether required software can be pre-loaded
  – Before final purchase, check with IT personnel to ensure that all purchases conform to agency and jurisdictional requirements.

• REQUIREMENTS FOR ANY NEW PURCHASES
  – If remote access is not available, determine:
    – Whether establishing it is possible in the near future. If not, determine if a cloud provider can provide access to essential files.
    – The level of security required. Some cloud providers can provide certified Criminal Justice Information System and/or military levels of security.

EQUIPMENT AND LICENSING

REMOTE ACCESS

01

02

03

CONSULT with your IT personnel to determine what is already available for remote access.

DETERMINE whether servers can be remotely accessed and whether doing so requires additional equipment.

CONFIRM that required email is available via the web.
**SECURITY CONSIDERATIONS**

- **USE** secure platforms for document sharing. Be aware of discovery requirements when sharing documents.
- **USE** strong passwords on all devices and applications.
- **BE AWARE** of phishing emails.
- **ENSURE** that software on all devices is updated with the most recent security updates.
- **BE AWARE** of file saving locations and policies (i.e., saving files on personal devices versus organizational network).
- **CHECK** with your IT personnel to determine if there are any pre-existing licenses for security software and/or recommendations for such software for each computer.

---

**VIDEO CONFERENCING AND REAL TIME CHAT OPTIONS**

- **DETERMINE** your video conferencing needs (e.g., internal meetings, victim and witness interviews, consultations with experts).
- **CHOOSE** a platform that suits your needs. There are multiple platforms available that have varying costs and features.
- **EXAMPLES** of video conference platforms include:
  - Zoom
  - FaceTime
  - Microsoft Teams
  - Skype
  - Cisco Webex
  - GoToMeeting
  - Google Hangouts
  - BlueJeans
- **EXAMPLES** of video conference platforms include:
  - Slack
  - Google Hangouts
  - Microsoft Teams
  - WhatsApp
  - Zoom Chat
  - Skype
- **CONSIDER** discovery requirements before using any of these platforms.
- **CHECK** with your IT personnel to determine if there are any restrictions or pre-existing licenses for the commercial versions of these platforms.

---

**ADDITIONAL CONCERNS**

- **DETERMINE** whether your agency or jurisdiction has existing policies for use of take-home equipment and remote access.
- **ENSURE** that this work-from-home policy includes clear guidance on how employees should engage in telephone communication, video-conferencing, and email, and how this relates to future discovery requirements.
- **COMMUNICATE** instructions, policies, requirements, and restrictions to users.
- **WORK** with IT and vendors to ensure proper user support to bring equipment online and to maintain equipment.
- **BE AWARE** of potential phishing scams related to IT security and from IT vendors.

---

**EXAMPLE TRAINING MODULES**

- **PROVIDE** basic “quick start” instructions to users to teach them how to begin using the equipment, assuming no technical knowledge.
  - Include instructions on how to access other training, in hard copy or online.
- **CONDUCT** webinars and/or conference calls to train the users in using their new technology.
- **IF YOUR OFFICE** does not have the ability to produce your own training, consider available training from other organizations, such as LinkedIn, who are producing good-quality training videos and modules to help transition to working from home.

---

FOR QUESTIONS, CONTACT US AT COVID19_COURTS@CNA.ORG.