# Working Remotely

## A Guide for the Public Sector

BY ROB ROQUE AND ELIZABETH FU

While some state and local governments have allowed employees to work remotely for years, many are now being thrust into a remote work environment as a result of COVID-19 response. Employees who are used to easy access to physical resources are now faced with make-shift operations at home. These rapid transitions to remote work are proving their own challenges to public sector operations and technology requirements.

The following are key considerations for governments when supporting remote workers. Items were selected based on general public sector requirements. Consider your organization's unique situations to establish a complete list of your own.

# Operating Policies and Procedures

The following are elements of remote work operating policies and procedures:

## Communications

Without face-to-face meetings, relaying information to employees can be challenging. Some governments have adopted procedures to have standing calls with employees to keep everyone up to date on the current situation as well as check on colleagues during uncertain times. Other governments provide answers to general operating questions on a public-facing website. For example, Montgomery County, Maryland, shares common timekeeping questions while working remotely and in light of COVID-19.[1] The City of Seattle, Washington, publishes messages to employees as well as general questions amid COVID-19.[2] Communication cannot be overemphasized during emergency events when the situation is constantly evolving and employees need to adjust operations.

## Identify Who is Eligible

In normal times, governments should identify which positions or classifications are eligible for remote work. However, as part of the COVID-19 pandemic, organizations need to use a different standard and consider who is essential and not just preferred. There are some job functions (e.g., public safety) where remote work is impossible given the nature of the work. Identifying who is eligible streamlines declared emergencies so employees and supervisors can easily identify which positions can transition to remote work. For example, the City and County of San Francisco, California, establishes position eligibility as well as employee eligibility criteria (suited for normal times) in its telecommuting program policy.

## Review HR/Payroll Rules

Governments should review how employees' work schedules impact HR/payroll rules while working remotely, including implications per bargaining agreements. For example, when an employee with a 4/10 schedule takes one day of leave, is he or she taking eight or 10 hours off? Governments should be clear about how their overtime rules apply and also communicate the application of the Fair Labor Standards Act (FLSA) rules to employees working remotely.

## Risk Management

While working remotely, an employee's home may be considered an extension of a government's workspace. As such, governments should provide employees with appropriate safety requirements (e.g., tripping hazards) and have employees acknowledge these protocols.

## Use of Personal Assets for Business Activities

Governments should consider what is necessary for employees to carry out their tasks at home and be prepared to provide the necessary equipment or supplies. Implementing remote processes may require policies that recognize the use of personal devices for official work and provide for reimbursement of costs. Policies should also address access to sensitive data.

## Monitoring & Evaluation

In both normal and emergency times, governments should evaluate the effectiveness of remote work and make appropriate adjustments. For example, the City of San Jose, California, conducts an annual survey of its flexible workplace program and reviews for changes in employee retention and absenteeism, required parking spaces, and reports of employee productivity.

# Technology Policies and Procedures

To prepare for similar events in the future, organizations should strive to have the following technology policies in place:

## Controlled Asset Policy

Such a policy consists of an inventory of assets permanently or temporarily assigned to an employee. Examples of controlled assets include laptop computers, smartphones, and other equipment (it does not need to meet a government's capital asset threshold).

## Authorized Use of Office Technology

Establish policies that only allow employees to use office technology that is assigned to them. It may be enticing or convenient for other household members to use assigned devices, but nonemployee use presents its own risk; therefore, nonemployee use of equipment should be prohibited.

## Authorized/Approved Access to Organizational Data

Prohibit employees from accessing systems or data through unauthorized means. For example, some home devices, such as gaming devices, streaming devices, and smart televisions, have the ability to access the Internet. These devices are typically unprotected and should not be used to access business systems.

## Secured Data Safekeeping

Data stored in enterprise systems typically follow security standards. Remind employees that enterprise data is sensitive and should be maintained within these systems. In short, data should not be offloaded to other storage devices, such as personal thumb drives.

## Safe Storage of Data

If data needs to be stored on thumb drives, consider using encrypted drives. If ever lost, data cannot be retrieved from the device without an encryption key.

## Password Policy

Consider developing a password policy that requires employees to use strong passwords (passwords requiring letters, numbers, and symbols) and to change them periodically. Ideally, passwords require two-factor authentication; meaning an authenticating device (e.g., Google Authenticator) is used to provide a random sync key to be entered along with the password.

# Issuing Devices

When it comes to issuing devices, consider the following:

## Consistency

Ideally, all issued devices should be similar or follow consistent standards. Some information technology departments will create a base image of a laptop to achieve this. If a device is destroyed, it can be rebuilt using the image. Standard technologies make systems efficient to maintain. For risk mitigation, some organizations will support multiple standards, such as Windows, Apple, and Chromebook.

## License Check

Make sure the organization has adequate software licenses. Licenses related to an unused desktop remain with the desktop. The laptop represents a new license. This may come as a surprise for organizations using applications that require a desktop client.

## Operating Systems

Make sure that the operating systems on issued devices at remote locations and the physical facility are upgraded and patched. Any system not upgraded and patched is vulnerable. Updates should be set to automatic.

## Anti-Virus Software

Devices should have anti-virus technologies. Software should be updated and virus definition updates should be set to automatic.

## Office Software

Load all office software on issued devices. Ideally, the required software is based on a standard setup. Software should be set to update automatically, because out-of-date software is vulnerable to attacks. Consider processes for installing software on devices that are missing applications.

## Remote Access Software

Consider installing remote access software on government-issued laptops. This allows authorized persons to access an employee's machine to maintain or service it remotely. Conversely, an employee may need to access internal desktops using a remote laptop. (This is not recommended since the unattended machine being accessed is vulnerable during remote access. Consider leaving monitors off in the office so that remote transactions cannot be seen.)

## Password Utility Software

Consider distributing a password utility software. The software maintains passwords for employees to help manage access even when remote. Most utility software can also generate passwords (including strong passwords).

## Inventory

Maintain an inventory of government-owned devices issued to employees. Laptops, for example, should be tagged and indexed by employee. Cellular devices should be indexed by phone number with the employee.

## Videoconference Software

Identify a videoconference platform to facilitate remote meetings. Many laptops are equipped with cameras, audio, and microphones. Governments should consider choosing platforms that have support call-in numbers in case home network bandwidth is not strong enough to support video. Depending on additional needs, a government should consider whether the platform will allow the sharing of applications or files or chatting. Do not forget that employees may need earpieces with microphones. It is sometimes easier to understand the speaker when an earpiece and microphone are used with the videoconferencing software. Finally, consider using passwords for online meetings to prevent videoconference bombings. (In these rare instances, hackers display pornographic images or interrupt meetings with inappropriate comments.)

# Deployment

Once the employees and equipment are deployed to work remotely, there are other processes that should be maintained. The following list addresses some of the important ones.

### Mitigation Training

Cybercriminals will use any opportunity to claim a victim. The COVID-19 pandemic has created opportunities for phishing. Remind employees to never open attachments from suspicious email addresses and never give out usernames and passwords without authenticating the requesting source.

### Training Tools

Governments should develop a Governments should develop a remote training program for staff. Subjects can include remote access, office applications, and safe computing. Training can be delivered internally using videoconferencing software, or it can be outsourced. Organizations have used free resources such as YouTube and other online resources as additional educational guides. While under shelter-in-place, the City of San Rafael, California, provides tech support resources and training for the added number of employees working remotely.[3]

### Secured Networks

Most home networks are secured, meaning they require a password to access the Internet. If an employee suspects that the network is not secure or is accessing data through an open network not requiring a password, then the employee should use a Virtual Private Network (VPN) to access business data. A VPN establishes a secured tunnel between the remote device and the enterprise network.

### Safe Access

It may be tempting to use another network, particularly when a household member has access to the Internet through a separate network (e.g., using the smartphone provided by a household member's employer). Even though the other network may be secured, it is doubtful that the provider of the infrastructure (household member's employer) is willing to take on the liability of handling business data from another organization. Employees on the host network may also be able to access data being transacted on their network (the household member may be able to access activity on their network).

### Clean Devices

Finally, in these times, it is highly recommended to clean all surfaces of remote devices. If possible, send employees home with electronic cleaning supplies consisting of at least 60% alcohol. Establish a process to clean devices once everyone is allowed to return to in-person workspaces.

# Conclusion

We hope that the checklists in this document will help you manage operations and technology that may have been rapidly deployed for remote work due to COVID-19 precautions. The remote work experiences during the COVID-19 crisis can also inform future policies and procedures and provide lessons learned for future emergency preparedness for business continuity. If you needed to rapidly deploy your technologies and did not have a chance to gather your inventory, now is the time to ask employees to submit the information to a central person. Most importantly, continue to emphasize safe computing practices for staff while they work from home.

[1] See Montgomery County, Maryland, Office of Human Resources, "Telework," https://www.montgomerycountymd.gov/HR/Telework/TeleworkProgram.html.

[2] See City of Seattle, Washington, Human Resources, "Information for City Employees about Coronavirus 19," https://www.seattle.gov/hr/covid-19.

[3] See City of San Rafael, California, Digital Service & Open Government, "Working Remotely," https://employees.cityofsanrafael.org/working-remotely.

### Sources

A Byte of Prevention, https://www.gfoa.org/byte-prevention-best-practices-cybersecurity.

Checklist for Companies with Remote Employees Due To COVID-19 — Forbes (March 18, 2020), https://www.forbes.com/sites/waynerash/2020/03/18/checklist-for-companies-with-remote-employees-due-to-covid-19/#1b33b140184a.

University of Virginia IT Department Faculty/Staff Technology Checklist for Working Remotely, https://virginia.service-now.com/its?id=itsweb_kb_article&sys_id=d8614580dba788d4d6655595ce9619eb.

Society for Human Resource Management, "Are telecommuters covered under workers' compensation?" https://www.shrm.org/resourcesandtools/tools-and-samples/hr-qa/pages/wcandtelecommuting.aspx.

Dustin Haisler, Government Technology, "Updated: A Resource Guide to Coronavirus for Government Leaders," March 18, 2020, https://www.govtech.com/health/A-Resource-Guide-to-Coronavirus-for-Government-Leaders.html.