Monitoring COVID-19

The School of Government continues to monitor COVID-19. Updates on courses can be found here.

Teleworking Guidance: Best Practices, Sample Policies, and Cybersecurity

Shannon H. Tufts

Type: Handout
March, 2020

This resource page includes the materials designed to help local governemnts navigate teleworking, including sample policies, procedures, best practices, and cybersecurity. Additional items will be added regularly to assist our clients. If you have questions about the technical aspects of teleworking, feel free to contact Shannon Tufts (tufts@sog.unc.edu; 919.962.5438).

Top Tech Tips for Working Remotely and Securely

Public Records Reminder: Recognize that if you are communicating about public business over non-enterprise tools, then you are likely creating a public record and you (as the sender/receiver of the record) need to determine how you will keep the record according to the North Carolina Local Government Records Retention requirements.

1. Check with your IT department prior to starting teleworking. They should have protocols in place to assist you with securing your environment and data access/transfer/storage.

2. If you are working from home on your home network (on work or personal devices), ensure that your home router is properly secured.
    1. First, make sure you change the factory-preset password. Many people do not do this, and it leaves their home networks vulnerable.
    2. Ensure firmware updates are installed to patch any security vulnerabilities.
    3. Set your router's encryption to WPA2 or WPA3. WEP is not sufficient.
    4. Use this guide for more advanced practices, like restricting inbound and outbound traffic: https://www.comparitech.com/blog/information-security/securing-your-wireless-router-and-your-wifi-network/

3. Avoid public WiFi if possible as these are unsecured. If you are working remotely but from public locations, use personal hotspots (like your smart phone or a MiFi device). If you are using a public WiFi network, make sure to use VPN for accessing work applications and data.

5. Do not use personally owned computers for work purposes if at all possible. It is unlikely that your personal computer has sufficient antivirus software, customized firewalls, and automatic backup tools running, compared to devices deployed by your employer.
    1. If your organization uses a portal or remote access environment like Office 365, this will help alleviate some of the concerns related to use of personally owned computers, but ensure that you only work online and do not download or store any items to your machine locally.

6. Ensure firewalls are set up. Your device's operating system should have a built-in firewall, but there are other options to add more protection on your personal devices if needed. Your IT department will have handled firewalls for work devices.

7. Use antivirus software on your personal devices. In the case of work-provided devices, this software will already be installed and running.

8. Ensure that your updates are being installed regularly. Patches for security vulnerabilities are essential for both work and personal devices. It is easiest to set these updates to run automatically during non-waking hours.

9. Always use strong passwords for all accounts. If your IT department allows it, use a password manager to ensure that you can leverage strong passwords without worrying about forgetting them.

10. Use two-factor authentication whenever possible.

11. Always back up your data.

12. Watch out for phishing emails, voicemails, text messages, and even Facebook Corona virus maps. As people transition to teleworking, we are seeing a huge spike in these attempts. If you receive a message that purports to be from a known associate, doublecheck the email address, never open attachments or click on links until you have confirmed that the sender is legitimate. Personally, I use the telephone or software like Microsoft Teams or another messaging service to verify with the purported sender before I open or click anything that I was not expecting to receive.

13. Use encrypted communications for all sensitive information. Your organization may have this communication channel established already through Office 365 or some other enterprise solution. You can also use mainstream applications like Signal or Telegram, which leverage end-to-end encryption.

Download (City of Concord Emergency Telework Policy, 122.36 KB)

Download (City of Monroe Teleworking Policy, 38.24 KB)

Download (Town of Apex Sample Flexwork/Telework Policy, 29.82 KB)

Download (Town of Apex Sample Flex/Telework Agreement Template, 60.93 KB)

Download (Coronavirus Anti-Phishing Awareness Content from ECU, 342.10 KB)

Download (Security Alert re: Coronavirus Map from the FBI, 292.30 KB)

Download (Microsoft Surface Sanitization, 252.10 KB)

Download (Cleaning Your Devices by Chris Niver, Conover NC, 15.77 KB)

Download (Additional Teleworking Guidance from NC DIT, 25.49 KB)

Web link:

NC Department of Information Technology Telework Guidance

Public Officials - Local and State Government Roles

City and County Clerks
City and County Managers
Elected Officials
Health and Human Services Professionals
HR Professionals
IT Professionals
Managers and Supervisors

Topics - Local and State Government

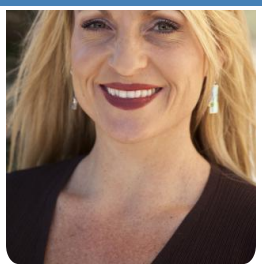
Human Resources
Information Technology
Leadership and Management

FACULTY COORDINATOR

Shannon H. Tufts

Associate Professor of Public Law and Government and Director, Center for Public Technology

tufts@unc.edu



UNC SCHOOL OF GOVERNMENT

Knapp-Sanders Building
Campus Box 3330, UNC Chapel Hill
Chapel Hill, NC 27599-3330
T: 919 966 5381 | F: 919 962 0654