Teleworker Cybersecurity Checklist

Below is a simple checklist you can follow to ensure your teleworking is cyber secure.

Secure My Devices

- ❑ I keep devices (computers, tablets, smartphones) secure when not in use.
- ❑ I set devices to automatically lock, with a strong password/PIN, after 15 minutes or less of inactivity, the shorter the better.
- ❑ I use anti-virus software and only use authorized and licensed software/apps.
- ❑ I keep all the software I use updated and set up automatic updates whenever possible.
- ❑ If available, I will enable encryption on my mobile/portable devices.

Secure My Workspace

- ❑ I do not leave sensitive work papers or documents out for others to see, and I secure them from unauthorized view.
- ❑ I don't allow family members to use work-issued devices or access work files.
- ❑ If working with sensitive information around others (e.g. Personnel files), I make sure others cannot view my screen (e.g. use a privacy filter on your monitor).

Secure My Wi-Fi

- ❑ I changed the Wi-Fi router's default admin password to something strong.
- ❑ I use strong Wi-Fi encryption (WPA2-PSK AES or WPA3, or WPA2-PSK AES + WPA-PSK TKIP).
- ❑ I only install manufacturer updates.
- ❑ I have my Wi-Fi firewall enabled.
- ❑ I do not connect to open or guest Wi-Fi.

Secure My Passwords

- ❑ I use strong passwords per the City's Password Security Policy on InsideLA.
- ❑ I use unique passwords for each computer/device or online account.
- ❑ I use multi-factor authentication.
- ❑ I do not share my passwords with others.

Secure My Data

- ❑ I will not download work data to non-work-issued devices.
- ❑ I securely store, or dispose of, paper files, written notes, removable disks and drives.
- ❑ I can identify confidential and restricted information and secure them according to the City's Information Handling Guidelines.

Secure My Email

- ❑ I watch out for phishing email red flags.
- ❑ When I receive a suspicious email, I do not click links, I do not open attachments, and I report the email using PhishAlarm.
- ❑ I only access and share information from official and trusted sources.
- ❑ I do not forward work emails to personal email accounts.

Secure My Meetings (Video Conferences)

- ❑ I do not install unfamiliar or suspicious virtual meeting software.
- ❑ I do not record virtual meetings, unless it is necessary and I have permission.
- ❑ I do not allow remote users access to control my device.
- ❑ Before I share my screen, I make sure to not share sensitive information accidentally.
- ❑ I do not share my meeting links in public forums or social media.
- ❑ When highly sensitive information will be discussed, I contact my IT Help Desk first to find out if there are additional security steps I should take.

If you see suspicious activity on any device you're using to telework (computer, mobile device, or home network) ask for help—better safe than sorry. Contact your department's help desk or security operations center to report the activity.

August 2021