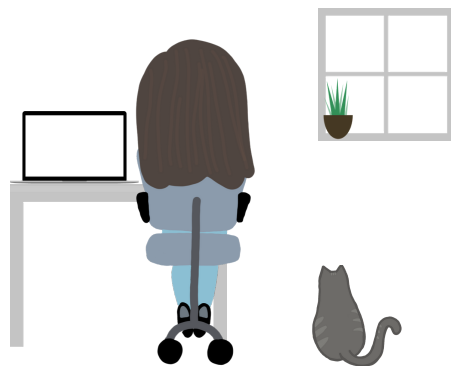THINGS TO KNOW ABOUT

WORKING REMOTELY

What can you do to secure your personal and UW data working from home and other off-campus locations?

SECURE DATA

Protect your accounts and devices with **strong passwords** and passphrases. **Back up your data** in several forms and keep your backups in a secure place. **Know the type of data** you are working with (public, restricted, or confidential) and secure it accordingly.

SECURE DEVICES

Keep your devices in a **secure location.** Laptops stolen from vehicles is a common way that data is lost at universities. Always **keep all software updated and patched.** Use work devices for work and personal devices for personal data.

SECURE CONNECTIONS

Use a **virtual private network (VPN)**, such as Husky OnNet. Make sure your device's **firewall is turned on**. Get to know the administrative interface on your router and change the default name and administrator password. Choose the **strongest form of encryption** possible, such as WPA2 or WPA3.

SECURE COLLABORATIVE TOOLS

Make sure you are using the **right collaborative tools for the type of data** that you are sharing with co-workers. The comprehensive file service comparison on IT Connect will help you determine the appropriate tools for various types of protected data. Review the list of Zoom security tips and best practices on IT Connect.

LEARN MORE

Security Tips for Remote Work
ciso.uw.edu/2020/04/03/security-tips-for-remote-work/

Scams Aimed at Remote Work
ciso.uw.edu/2020/03/17/scams-aimed-at-remote-work/

Working Remotely – IT Connect
itconnect.uw.edu/work/working-remotely/

UW File Services
itconnect.uw.edu/wares/mws/myworkstation/files/comparison/

Zoom Security Tips and Best Practices
itconnect.uw.edu/zoom-tips

OFFICE OF THE CISO
UNIVERSITY *of* WASHINGTON