PHYSICAL DEVICE SECURITY

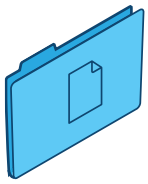
Devices used to access work-related information must be physically protected to prevent sensitive data from ending up in the wrong hands

COMMON ITEMS TO PROTECT IN THE WORKPLACE

LAPTOPS

DESKTOPS

USBs/HARD DRIVES



DIGITAL FILES

PASSWORDS

YOU ARE REQUIRED TO:

- PASSWORD PROTECT YOUR WORK DEVICE
- KEEP YOUR PASSWORDS SECRET
- LOCK OR SIGN OUT OF COMPUTERS WHEN YOU LEAVE YOUR WORK AREA
- AVOID ACCESSING CRITICAL WORK-RELATED INFORMATION FROM YOUR PERSONAL DEVICES
- AVOID CONNECTING WORK DEVICES TO GUEST WIRELESS NETWORKS

ONLY CONNECT USBs/HARD DRIVES AND OTHER DEVICES TO COMPUTERS YOU KNOW WILL BE FREE OF MALWARE

DON'T INSERT UNFAMILIAR USBs/HARD DRIVES INTO YOUR COMPUTER OR OPEN UNFAMILIAR FILES

FULLY AND PERMANENTLY DELETE DATA OFF OLD AND UNUSED DEVICES

DELETE OR DEACTIVATE ACCOUNTS THAT ARE NO LONGER USED

PRACTICE PROPER DEVICE DISPOSAL

SHRED, ERASE, OVERWRITE, AND RESET ANY DATA OR DEVICES BEFORE GETTING RID OF THEM

THIS INCLUDES COMPUTERS, PHONES, HARD DRIVES, USBs, AND CDs. ENSURE SENSITIVE DATA IS PROPERLY REMOVED AND NO LONGER ACCESSIBLE AFTER DEVICES ARE DISPOSED, DONATED, OR RECYCLED.