

Safe Travel Checklist



Easy to Do; High Impact:

No Matter Where You Are or Where You're Going:

- Never use a borrowed charger**, a public charging station, or a hotel room charging port.
- Disable** Wi-Fi autoconnecting, Bluetooth, fingerprint access/facial recognition, and Near Field Communication (NFC) like Airdrop or mobile payments.
- Avoid open/free Wi-Fi!** Use a VPN or mobile hotspot instead.
- Enable** remote locking and device erase functions.
- Only connect to known Wi-Fi networks;** beware of network names that have typos or extra characters.
- Use a privacy screen** to prevent "shoulder surfing."
- Don't share!** Turn off file sharing, printer sharing, GPS, and location sharing—and avoid social media!



At the Office (before you depart):

Your IT department may:

- Update your operating system.**
- Update your **software** (including antivirus) and install available patches.
- Install a password manager** to give an extra layer of protection.
- Encrypt the hard drive** and any external drive(s).
- Install and setup VPN** if you don't already have it.

You should:

- Copy files** you might need.
- Clear your browser** history and cookies.
- Back up all files** to a separate device and/or secure online storage location to be left behind.
- Get your cell phone and your tablet ready:
 - **Update your operating system.**
 - **Clear your browser history.**
 - **Set your device for password or PIN access only.**



What to Pack:

- Webcam cover (or opaque tape!)
- IT Contact info (on paper)
- Device chargers
- RFID-blocking wallet or card sleeve
- Laptop privacy screen



At the Airport:

- Always keep track of your boarding pass.**
- Never check your briefcase or laptop bag.**
- Put electronic devices (including watches) on the belt last.**
- Keep devices in view** (or know where they are) during security checks **and** when charging.
- Set devices to "airplane mode"** whenever possible.

In the Airplane:

- Shut down your laptop/tablet when leaving your seat.**
- Carry your phone at all times—even to the restroom!**



At Conference Settings and Hotel Rooms:

- Never use an **unknown flash drive**, external drive, mobile or USB-based device.
- Don't accept **any thumb drive "give-aways."**
- Discuss sensitive corporate info **in person only.**
- Never use hotel/in-room safes.** Instead, keep your devices and valuables with you at all times.



Back in the Office:

- Scan devices** for malware.
- Consider **changing passwords and PIN** numbers.
- Shred** old boarding passes and luggage check tags.
- Check with IT department** or consult travel policy so that you take all required steps.

