Travel Guidelines

Information Security Office

Work travel can expose you to unique security and privacy risks, which may lead to inconvenient or even damaging incidents if not properly addressed. To mitigate these risks, review Wharton recommendations before your trip to ensure data safety and minimize vulnerabilities while you're on the go.

Before Travel

- **Notify Wharton Computing.** Inform your Wharton IT representative of your international travel plans to make any necessary security preparations or monitoring, especially for BRICS (Brazil, Russia, India, China and South Africa) countries.
- **Review Security Restrictions and Travel Advisories.** Review current **travel advisories** and security restrictions to stay informed about any data security risks or limitations at your destination.
- **Limit Devices and Data.** Only take essential Wharton-managed devices and remove sensitive data whenever possible to reduce exposure and minimize the risk of loss or theft. Store sensitive data in secure services like Box, Dropbox, OneDrive, etc.
- **Update Software and Applications.** Ensure all travel devices have the latest software, operating system, and application updates, to address known security gaps and vulnerabilities.
- **Ensure Portable Storage Devices Are Secure.** If bringing a portable hard drive or USB drive, only use trusted and encrypted devices. Avoid using unfamiliar or untrusted storage devices.
- **Enable Strong Passwords and Multi-Factor Authentication (MFA).** Protect all devices and accounts with robust passwords and enable 2FA/MFA whenever possible. Turn off "remember me" settings and wipe stored passwords from all applications and browsers on travel devices. To keep secure records of your new passwords, check out Dashlane provided by the university.
- **Back Up All Devices.** Perform a full backup before departure to safeguard important information in case a device is lost or stolen. Reach out to your Wharton IT Representative for support.
- **Consider Using a Loaner.** A loaner device can reduce data loss risks by enabling work without exposing primary devices. Upon returning, it can be wiped to prevent malware spread to your network.

While Away

- **Keep Devices with You.** Ensure your devices are with you at all times, especially in high-traffic areas such as airport screenings, security checkpoints, and conferences. Use a hotel room safe when unattended.

- **Use a VPN for Secure Access.** Connect to the university's GlobalProtect VPN before accessing university or personal accounts. Be aware that some VPNs may be restricted in certain countries, so check with Wharton IT representative before travel.

- **Access Confidential Files via Secure Platforms.** Access confidential files through secure web platforms, such as O365's web interface, to maintain data security on the go.

- **Report Missing Devices Immediately.** In the event a device is lost or confiscated, report to local authorities and contact the Information Security Office (ISO) promptly to manage risks and recovery.

- **Avoid Untrusted Wireless Networks.** Refrain from using public networks, like those in hotels, airports, and cafés, for sensitive work. Disable Bluetooth and wireless file-sharing options, such as AirDrop, to prevent unintended access to your device.

- **Avoid Using Unfamiliar Devices.** Do not use public computers or unknown USB drives or chargers, as these may carry malware.

- **Exercise Caution with Links and Downloads.** Practice the same caution as you would at home: avoid clicking on links or downloading files from untrusted sources, and delete suspicious emails.

Upon Return

- **Reset Your Passwords.** Use a trusted device to reset your PennKey password and any other passwords used during your trip to ensure account security.

- **Return Loaner Devices.** Ensure any loaner devices are returned to your Wharton IT Representative.

Get Help

If you require user assistance at any stage of travel, please contact your Wharton IT representative. For more information on on how to protect Penn systems and data while abroad, **click here**.

If you are experiencing a known or suspected information security incident please email security@wharton.upenn.edu.

technology.wharton.upenn.edu/iso

Wharton
University of Pennsylvania