Information Security Travel Guidelines

Traveling can present some unique security challenges. If you are planning domestic or international travel, please take extra precautions to safeguard personal and university assets. Data may fall into the wrong hands as a result of your device being hacked, inspected, confiscated, stolen, or lost.

Use this document as a checklist and consider the safeguards listed to protect your personal and university information.

Before Leaving:

- ***If it's not necessary, consider leaving it behind.***
    - Leave behind devices or media that are not necessary. Proprietary research information & confidential staff and student information are at the largest risk.
    - Don't save personal information such as credit card numbers or passport information on your device.
- **Are you traveling with sensitive or confidential information?** – Only travel with the data that you absolutely need. If you don't need it, don't take it. Check with ITS to obtain a loaner laptop that you can use while traveling instead of bringing your own.
- ***Inventory and back up your data.*** Take note of what's on your device in case it is lost or stolen. Even if you are taking some files with you, back it up before you leave. Make sure to store the data in a secure location, such as a department share.
- ***Secure your device.*** Contact ITS for tips. Some additional reminders:
    - Disable file and print sharing, Bluetooth, and network connections when not in use.
    - Run an anti-virus scan using Cylance or Kaspersky to set a baseline for a clean system.
    - Ensure your operating system and software are up to date with the latest security patches.

While you are away:

- ***Use caution when accessing the internet and university resources.***
- ***Use the STOP THINK CONNECT Approach:***
    - Avoid free Wi-Fi services, including cyber-cafes, libraries, and business centers. These networks are not secure and you could even be a victim of a low-tech attack such as shoulder-surfing. Your hotel room will be the safest place to use the internet.
    - Do not enter or access university data when using a shared or public computer.
    - Never accept software updates on hotel internet connections or public Wi-Fi.

- ***Always lock your screen****.*
    - On Windows computers, press Control-Alt-Delete and select Lock Computer. It will prompt you for your login information the next time you need to access it.
    - On Mac computers, in the Security section of the Security Preferences panel, check the *Require password to wake this computer* option, then go to the Desktop and Screensaver section in System and Preferences and turn on a screen saver.
- ***Keep your device with you.***
    - Whenever possible, keep your device(s) on your person rather than leaving them behind. Never place your device(s) in a checked or gate-checked bag when boarding an airplane.
    - Try to be discreet – for example, keep your laptop in a backpack instead of a purpose-built laptop bag. If you must leave your devices in a vehicle, lock them in the trunk or on the floor in the back seat, covered with a jacket or similar.
- ***Report Information Security Incidents if devices are lost or stolen****.*
    - Immediately change your password if you suspect it has been compromised. Contact ITS security for assistance, if needed.
    - Clayton State University faculty, staff, and researchers should report suspected or actual breaches of sensitive university information by emailing ITS Security. This includes loss, theft, or breach of both Clayton State-owned and personally-owned devices that store sensitive information.
    - Contact local authorities to report losses or thefts.

When you return:

- ***Change your Clayton State password.*** If away for an extended period or traveling abroad, change your password immediately upon your return.
    - ***Scan your device****.* Run another Cylance or Kaspersky scan and follow any recommended remediation steps.

Additional Guidelines When Traveling Internationally

Accessing Computer Resources:

Some countries have laws and rules that restrict Internet access. **Always** respect the local laws of countries you will be visiting.

- ***Prepare for limited access.***
    - You may not be able to access sites like Facebook, Twitter, YouTube, Skype, or even Google in some countries consistently. If you need material while traveling, consider downloading them before you leave.
    - Email access may be spotty or very slow. It may be easier to access email from a phone via a cellular network than from a computer. Check with your phone carrier about international data plans, or consider getting a local phone with a pre-paid card.
- ***Use a Virtual Private Network (VPN).***
    - Using a VPN service before accessing Clayton State University websites and applications will help protect yourself and university assets. It can also help bypass countries' firewalls, allowing you to access the sites listed above, and many others. Use it when connecting from your laptop, tablet, or smartphone.
    - Be aware that some countries may copy data from your computer and/or log your internet activity without your consent or knowledge.
    - VPN access may be blocked in some countries. Never attempt to bypass the block, as it may be considered an act of cyber espionage!

Protecting Devices and Information

- ***Take a loaner device, if available.*** If possible, take a device that contains only the files and applications needed for your trip. Some countries officials will inspect devices and even download files from them. Check with the ITS to see if laptops and other mobile devices are available.
- ***Keep devices close to you or locked up.*** Loss or theft is the largest risk to devices and sensitive information.
- ***Change your password.*** Change your Clayton State password before you leave and again after you return, as well as any other passwords you expect to use while away.
- ***Take only the information*** which you will present or discuss at the conference or other event. Back up your data and leave a copy in a safe and secure location. encrypt all information.

- ***Use encryption.*** The ITS group can help you encrypt your device to provide an extra layer of protection in case it is stolen. See the associated guides for Windows computers and Mac Computers to make sure your computer is protected.
- ***Consider purchasing tracking software*** in case of theft or loss.

- ***Do not access sensitive information.*** Confidential information can be captured in an increasingly large number of ways, and will occur when you least expect it. When in high-risk areas, do not use systems that provide access to sensitive data, even when using a VPN.
- ***Disable Bluetooth, Wi-Fi, and GPS when not in use.*** This will limit access to your device and data.
- ***Turn devices off when not in use.*** Powering off devices and even removing batteries can mitigate the risk of cameras or microphones being turned on remotely.
- ***Clean your device when you return.*** Running a Cylance or Kaspersky scan or completely wiping your device upon your return can help to insure that malicious software does not infect the university network. Taking a loaner device can make it easier to do this without losing needed information.

Additional Resources

- FBI Business Travel Brochure
- State Department Travel Advisories for Specific Countries