MISSISSIPPI STATE UNIVERSITY™
OFFICE OF RESEARCH
COMPLIANCE AND SECURITY

International Travel IT Best Practices

General Security Issues

To keep your devices secure when traveling abroad, follow the tips on this page.

- Use Two-Step Login (Duo); if you are unable to access your wireless/mobile device for any reason, use the instructions here to generate a temporary passcode.
- Whenever possible, arrange to use loaner devices while traveling. This greatly reduces the risk of theft or compromising university data.
- Leave unneeded devices at home
- Keep physical device security in mind. Portable equipment such as phones, laptops, flash drives, CDs, and PDAs are especially vulnerable to theft and loss while traveling. They should be kept secure and locked when unattended.
- Do not leave electronic devices unattended or transport them in your checked baggage.
- Regularly change your passwords. Cybercriminals from numerous countries buy and sell stolen financial information, including credit card data and login credentials.
- Before your trip, back up all files and leave a copy on an MSU departmental file server.
- Scrub your social media of any references to your trip or its purpose. Also scrub social media of any references to your work if it involves sensitive research.
- Do not use any electronic devices you did not personally bring with you.
- Do not allow anyone to offer to take a photo of you with their phone and offer to send it to you.

Device Security

- Use MSU's Cisco AnyConnect virtual private network (VPN) client to browse the web or securely access email, calendar, or files on a departmental server. MSU's Cisco

AnyConnect VPN allows for a secure connection into MSU's private network over the public network; for help, see About the MSU VPN.

- Enable security settings to protect data on your mobile device. Protect the data on your mobile device by keeping it physically secure and enabling security features: set a PIN or passcode, set the device to time out (and require a password) when idle, and set the device to auto-wipe its contents after several incorrect login attempts.

- Ensure that your operating system software is up to date for both your laptop and mobile devices. Your work laptop should update automatically; however, we recommend you still check prior to departure by typing "Update" in the Windows search bar, then selecting "Check for updates." For your mobile device, apply all software patches and updates from Apple and Android.

- Ensure encryption is turned on for your computer. If it is an MSU computer, it is most likely preconfigured with encryption, but we recommend you double check by following these instructions. We also recommend you encrypt your personal computer if you plan to bring it, especially if you've used it to access MSU files or the MSU network.

- If you are using a loaner laptop, login to your secure Microsoft 365 account at https://m365.msstate.edu to access your full account features. Alternately, access https://outlook.msstate.edu to securely access your MSU Exchange mailbox anywhere from any computer connected to the Internet, without having to configure Microsoft Outlook or another email client.

- Use free, built-in tracking tools where available; for instance, Find my iPhone can locate a missing iPhone, iPad, iPod touch, or Mac.

- If your university-provided laptop has been lost or stolen, contact the Service Desk and notify the Export Control Officer immediately.

- If you lose university information during travel (e.g. university-provided laptop, mobile device (e.g., Outlook for iOS or Android, or Microsoft 365 for Personal Use on a laptop), visit this website for options on how to delete your data remotely, or contact the Service Desk for advice.

- Wipe data if your mobile device is lost or stolen. If you use Exchange, log into your Outlook email on another computer and wipe your device remotely. If you use an Apple device without Exchange, log into your iCloud account, click the registered device, and then select the option to wipe the device.

- Turn off Bluetooth and Wi-Fi when not in use. Unless you are actively using these features, you should disable them to limit attack vectors for your devices.

- Turn off file and print sharing to prevent unauthorized access to your files.

- Clear browser history, cache, and cookies to delete any saved passwords or identifying information. Disable the "remember me" password feature provided by most browsers for the full length of your trip.

- Avoid public wireless access points (i.e., Wi-Fi)

Powering Your Devices

Bring the appropriate plug adapter for foreign AC converters so that you can plug a US charger into electrical outlets. Be wary of free charging stations and juice jacking. Use a wall outlet if available or carry an external battery pack or second battery. World Standards is a great resource to look up your destination's plugs, sockets, and voltages.

When you Return

- Turn in loaner laptop to ORC&S, if applicable. If not:

- Have your laptop examined for malicious software by ITS or ask to have it reimaged

- Change passwords

Global Plans and Roaming Rates

- Contact your service provider regarding cost-effective global plans and features for the country to which you're traveling. Don't forget to deactivate global features upon your return. AT&T has an International page, as do Verizon, T-Mobile, and C Spire to help you look up international rates, coverage, global services, and carrier information.

- To avoid roaming charges, it may be cost effective to purchase either a prepaid phone, or a SIM card with data/minutes from the local provider while you are in-country.

- If you do not have a cost-free international roaming plan from your provider, or you do not purchase a prepaid phone or local SIM card, we recommend you quit applications. Once in-country, go into your settings menu, disable data roaming, and quit all applications running in the background to avoid excessive data charges whenever possible.

Laws and Regulations

- Comply with any requests from a border official to log into your laptop or mobile device.

- If your device is seized by a foreign agency, obtain a contact name, phone number, and written documentation that the device was seized. Contact the local US embassy or consulate for advice on resolution in the local country. If the incident involves the US government, report it to your department and contact the MSU ORC&S.