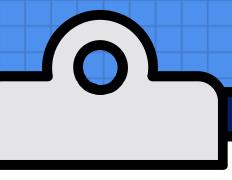
Research Security International Travel Recommendations



Mobile Devices

• Update to the latest operating system, antivirus software, and security application.

Use strong passwords.

- Avoid using public Wi-Fi networks.
 Use a <u>VPN</u> if possible.
 Enable two-factor authentication (2FA) (<u>DUO</u>)
- Be cautious of suspicious emails or links.
- Do not download files or attachments.
- Enable email encryption in Outlook.

Laptops

• Update to the latest operating system, antivirus software, and security application.

Use strong passwords.

Use <u>encryption</u> on your laptop.
Minimize the use of personal devices for Emory business by using Emory owned laptops as much as possible.
Use a loaner laptop when traveling.
Use a VPN if possible.

Maintain physical possession of your laptop.

- Have a data management plan.
 Know what types of data you are collecting, processing, storing, or sharing.
- Know who has access to your data and apply appropriate access restrictions.
- Avoid traveling with data that isn't necessary.

• De-identify data when possible.

Securely destroy unneeded data.

• Do not plug unknown peripherals (e.g., flash drives) into your Emory device.

Use SharePoint or OneDrive for file sharing and storage.

• Do not download or save files or attachments to your laptop.

• Report hacked, lost, or stolen devices as soon as possible

TikTok and any other <u>ByteDance</u> applications should not be present on any mobile device or laptop (personal or Emory owned/managed), and are prohibited when the devices are used for federally funded projects.

Rev 5.c

For More Information:



Email

- researchsecurity@emory.edu
- dataplans@emory.edu
- ORAITHelp@emory.edu

Websites

- OIT Protecting your data
- The National Counterintelligence and Security Center
- Office of Information Technology Information Security Travel Tips



Research Compliance and Regulatory Affairs