



EMORY
UNIVERSITY

TRAVEL LOANER EQUIPMENT PROGRAM

Ask RCRA – May 2023

 **IMAGINE... SCARY BUT TRUE**

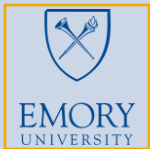
- Traveler leaves a laptop or phone in foreign hotel room... *it gets stolen or tampered with, including datasets and access to Emory systems*
- Traveler logs into foreign wireless or cell service... *traffic gets intercepted with communications, credentials, or data*
- Traveler logs into foreign wireless or cell service... *a malware agent gets installed, compromising the laptop and transported back to Emory*
- *Someone encrypts/locks the laptop and makes a ransomware request*
- ...



RESEARCH DATA PROTECTION UNDER NSPM-33



National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-supported Research and Development **obligates research institutions that receive in excess of \$50m per year in total Federal funding to establish research security programs.**



Emory's Research Compliance and Regulatory Affairs Office (RCRA) is leading the charge of preparing the institution for the upcoming compliance requirements, in partnership with relevant operational departments including Office of Global Strategy and Initiatives, Office of Information Technology, local IT units, and others.



Under the **new Emory Sponsored International Travel Policy**, a **Travel Loaner Equipment Program** will be implemented for Emory Faculty, Staff and Students traveling for Emory business outside of the United States to identified “high risk” countries, or under other restricted circumstances.



PROGRAM APPLICABILITY: WHO AND WHY?

- **Faculty and Staff*** who travel to a foreign country under “**high-risk**” **circumstances** for a purpose involving Emory-related electronic documents or remote access to Emory systems will **require use of the Travel Loaner Equipment Program**, regardless of funding source, booking service, or business purpose.

**Eventually, students as well.*

- Adding security controls on individuals’ Emory devices is not enough to safeguard Emory data and systems under high-risk foreign travel circumstances.



PROGRAM APPLICABILITY: WHEN?



TRAVEL DESTINATION

- **High-risk travel destinations** posing a risk to Emory data and system security.
- **About 40 countries**, based on the Office of Foreign Assets Control (OFAC) sanctions list and the Department of State Level 4 countries, plus China.

DATA TYPE*

- **High-risk categories of data** with greatest cybersecurity threats: sensitivity, impact of data breaches, certain funding sources, or other research restrictions.
- **Research subject to restricted conditions may already have a data management / control plan in place.**

**Future expansion*



LOANER EQUIPMENT: WHAT?

LAPTOPS

- Apple and Windows models, with travel accessories
- Essential software installed
- Research-specific customizations
- VPN, DUO and limited access
- Antivirus, security monitors

CELL PHONES

- Simpler models, iOS/Android
- Essential mobile applications
- International cellular/data plans

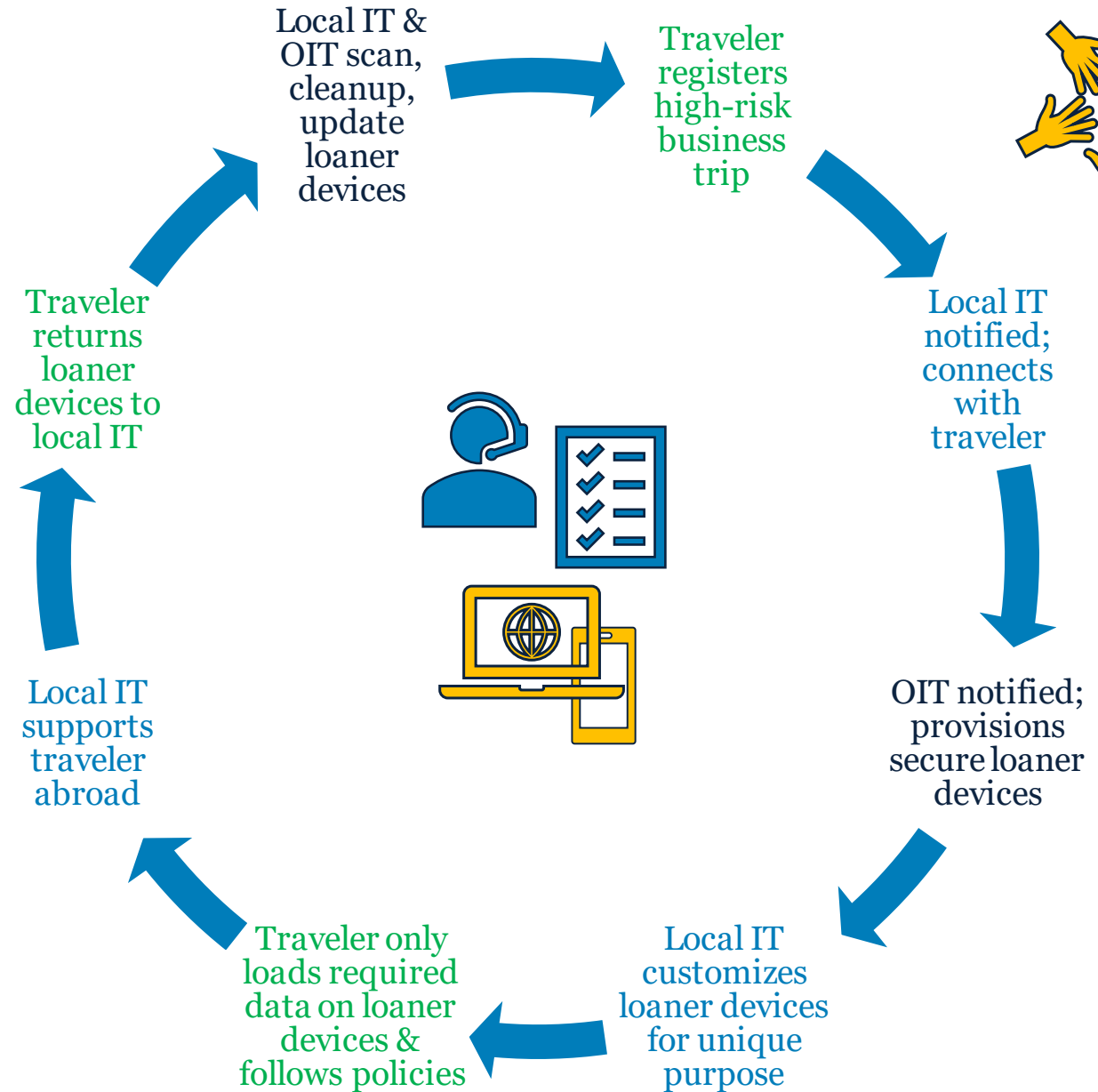


LOANER EQUIPMENT: HOW?

OIT: Loaner device inventory centralization and maintenance

Local IT: Loaner device distribution and customized support to travelers

Traveler: Responsibility to limit the amount of data on loaner devices and to follow IT security and foreign travel policies





IMAGINE... LIMITED IMPACT & PEACE OF MIND





- Traveler leaves a laptop or phone in foreign hotel room... *only limited data are exposed/lost, and the device can be wiped from Emory if it is stolen or tampered with*
- Traveler logs into foreign wireless or cell service... *specific configuration with VPN, DUO, and up-to-date security monitors limit the potential for traffic to get intercepted, or malware to be installed without detection*
- Traveler logs into foreign wireless or cell service... *upon return to Emory, the device is scanned for malware and compromised security*
- Someone encrypts/locks the laptop and makes a ransomware request... *the device can be wiped from Emory and only limited data are exposed/lost*

CONSIDERATIONS: WHAT NOW & NEXT?

- Always follow research data & information security recommendations
- **Plan ahead** for travel registration and safety approvals
- Always follow (international) travel security tips
- Contact your local IT team: some may have loaners on hand or can coordinate with OIT
- **Tentative timeline:** Approvals in Summer, Pilot in Fall, Roll out in Winter

Research Data Security Recommendations

- 
- Update and patch hardware and software.
 - Use encryption on your devices.
 - Use Emory owned and managed devices.
 - Minimize the use of personal devices as much as possible.
 - A clean loaner laptop should be used for remote access.
 - VPN must be used for remote access.
 - When travelling offsite, maintain possession of your devices.
 - Avoid travelling with data this isn't necessary.
 - Register with [International SOS](#) before your trip.
 - Know what types of data you are collecting, processing, storing, or sharing.
 - Do not plug unknown peripherals into your Emory device.
 - Do not download and save to desktop or a local drive.
 - Know who has access to the data and apply appropriate access restrictions.
 - Use SharePoint or OneDrive for data storage.
 - Use strong passwords on devices and folders.
 - De-identify data when possible.
 - Have a data management plan.
 - Securely destroy unneeded data.
 - Report hacked, lost, or stolen devices as soon as possible to [Emory Security](#)
- 

QUESTIONS?

researchsecurity@emory.edu

MORE INFORMATION

- International Travel for Research: <https://research.emory.edu/international-collaborations/travel.html>
- Information Security Travel Tips: https://it.emory.edu/security/protecting-data/travel_tips.html
- Travel to High-Risk Destinations: <https://global.emory.edu/services/travel/high-risk.html>
- Export Controls: <https://rcra.emory.edu/export-control/index.html>
- General Travel Information: <https://global.emory.edu/services/travel/getting-there.html>
- Research Security Office: <https://rcra.emory.edu/research-security/index.html>
- IT Security – Protecting Your Data: <https://it.emory.edu/security/protecting-data/index.html>