International Operations Data Security Guide

The security of research and professional data while traveling internationally is an increasingly pressing concern for students, faculty and staf and a matter of increased regulation. In conjunction with UMB's Research Security Program, Center for Information Technology Services (CITS), and the Center for Global Engagement (CGE), International Operations (IO) has prepared the following guidance for UMB personnel conducting university business outside of the United States, particularly where University data or systems will be used.

This guidance is not intended to address personal travel or personal data. If you are a non-U.S. citizen and require advice concerning (re)entry to the U.S., contact the Ofice of International Services if you are on a UMB-sponsored visa or your personal attorney. It is the responsibility of the individual traveler to verify and comply with the applicable laws and policies of their destination countries and to comply with all University policies and federal laws related to the security of research data and protection of University property.

- **Ensure that travel documents and visas are valid and up to date.** Renew passports well in advance or otherwise make sure you have at least six months' validity and space for visa stamps in your existing travel document.
- **Understand and account for the political situation of all countries on your itinerary.** Consider temporarily removing social media accounts, multimedia and contacts if their presence may be considered ofensive or suspicious in the countries you are entering.
- **Inform others of your travel plans and discuss who to contact if you encounter issues upon entering a country.** International Operations ofers a template for an Emergency Action Plan, which individual or group travelers can customize to fit their needs. At minimum, share your itinerary and discuss with your contacts at each of your destinations (including your home country) what to do if you have encountered an issue or been detained. *International Operations, and UMB in general, are unable to provide direct support or facilitate the release of someone detained in another country, but where appropriate may be able to contact governmental authorities for assistance.*
- **Only take research and university data that you will need to access during your travel.** Remove sensitive, proprietary or confidential information that is stored on your hard drive before traveling. Remember to follow research protocols and store confidential research data on a UMB-approved cloud storage platform such as OneDrive or SharePoint and only access it via Microsoft's Azure Virtual Desktop (AVD). If you have questions what constitutes sensitive, proprietary or confidential information, contact CITS or Research Security well in advance of your proposed travel dates.

- **Use a Temporary Device.** If you can obtain a loaner device just for travel, you can avoid loading information on it that you do not need for your trip.
- **Use Private Browsing Mode.** Most browsers ofer a private browsing mode. In this mode, the web browser does not save browsing history to the hard drive.
- **Disable biometric access methods such as facial or fingerprint recognition for device unlocking, and power off devices prior to entering a country.** This adds another barrier to unauthorized access.
- **If there is any unauthorized access of a UMB-issued laptop or phone, inform CITS Security & Compliance and Research Security immediately.** Change passwords for any apps or accounts present on the device that was accessed.
- **Be aware of the customs and border policies of the countries you are entering and exiting.** All countries reserve the right to question people and conduct searches of property- including electronic devices such as laptops, phones and tablets- upon entry or reentry. In the United States, this includes US citizens, lawful permanent residents (green card holders) and those entering on temporary visas. The extent of a device search varies from country to country and the device may be retained temporarily or even indefinitely. The policies of the United State Customs and Border Enforcement can be found at: Border Search of Electronic Devices at Ports of Entry | U.S. Customs and Border Protection. Travelers should check the embassy websites of the countries they will be traveling to for entry requirements. International Operations can also assist in locating the policies of the countries you are travelling to.
- **Consult with UMB's subject matter experts before traveling if you have any questions or concerns.** UMB retains experts in research security, internet technology and travel safety and security who are well positioned to address any questions or concerns that you might have.

CITS: help@umaryland.edu

Security & Compliance: security-compliance@umaryland.edu

CGE: globaltimore@umaryland.edu

OIS: ois-info@umaryland.edu

Research Security: SPA-Research_Security@umaryland.edu

International Operations: globalhub@umaryland.edu