High-Risk Travel

I. Introduction

The University of Denver (DU) is committed to protecting the confidentiality of University records and information, including proprietary information, sensitive research data, and intellectual property of the University, its faculty, and staff. Travel with electronic devices to destinations presenting heightened theft and cybersecurity risks increases the potential for such sensitive information to be procured from computers and mobile devices without the owner's knowledge or consent and for devices and the University's network to be infected by malware or spyware, and therefore requires special precautions.

II. Policy Overview

This policy provides requirements and guidance about the transport and use of electronic devices when traveling to such destinations and the program for loaner devices while traveling on University business. It applies to all faculty and staff on University-sponsored travel, to any destination presenting heightened cybersecurity risk, and to any sanctioned or embargoed country or region with a travel advisory level 3 and above, as defined by the U.S. Department of State. Please visit the Department of State Travel Advisory website for more details.

III. Policy Process

A. Requirements

1. When traveling to heightened cybersecurity destinations, sanctioned, or embargoed countries, there are additional considerations and cybersecurity requirements. See the IT Cybersecurity High-Risk Travel website for the latest updates and specifics. The University reserves the right in its sole discretion to designate other locations as "high-risk."
2. Should you need a device for University-sponsored travel, employees must submit an IT service ticket at least two weeks before departure to receive a University-owned loaner device. Subject to available inventory, travelers on short-term personal travel to destinations with heightened cybersecurity risk may be able to obtain loaner devices. See also University Policy 2.30.020 - *University-Owned Mobile Devices.*
   i. The High-Risk Travel Loaner Program allows staff to have access to the applications and information they need while minimizing the amount of sensitive data that is carried abroad.
3. No intellectual property or confidential information should be downloaded to any loaner device. Users are not permitted to modify system settings or install additional software and should not load any files or data onto these devices. For more information on the High-Risk Travel Loaner Program please visit the DU High-Risk Travel website.
4. After returning to the University, the traveler must return the loaner device(s) promptly to the IT Help Center where it will be wiped, re-formatted, and re-imaged.

B. Roles and Responsibilities

The Information Security Office (ISO) is responsible for this policy and its requirements.

IV. Definitions

- Sensitive Data**:** Sensitive data is information that a person or organization wants to keep from being publicly available because releasing that information can lead to harm, such as identity theft or other crimes. In some cases, sensitive data is related to individuals, such as payment information, birth date, etc. In other cases, sensitive data can be proprietary to the University or research information.
- High Risk Travel: International destinations that are posted to the U.S. DOS as a Travel Advisory Level 3 or Level 4.
- Malware: Malware is intrusive software that is intentionally designed to cause damage to computers and computer systems.
- Spyware: Spyware is a type of malware designed to enter your computer device, gather data about you, and forward it to a third-party without your consent.
- Mobile Device: Mobile Device a communication device that is portable and designed to be carried by a person to carry out business communication activities. Mobile Devices items include but are not limited to laptops, cell phones, smart phones, iPhones, iPads, Droid, and hands-free devices.