Research, Integrity, Security and Ethics
Loaner Laptop Program for International Travel Program Plan
October 5, 2026

Table of Contents:

- International Travel Security Risks
- Export Control Implications
- ORCP's Loaner Laptop Program for International Travel
  - Types of Laptops Available
  - Software Installed
  - Accessories
  - VPN Access
  - Download Duo Mobile App to Your Smartphone
- Request a Loaner Laptop
- Sensitive Data
- Username and Password
- Connecting to FSU while Abroad
- Returning the Loaner Laptop
- Protect the Laptop and Information while Traveling Abroad
- Reporting a Lost, Stolen, Confiscated, or Maliciously-Destroyed Loaner Laptop
- Returning the Loaner Laptop

- ***Loaner laptops are available on a first-come, first-served basis****. Submitting a request does not guarantee that a device will be available.*
- ***The length of checkout should not be longer than 30 calendar days.***
- ***You must complete and submit this Request no later than 10 business days prior to your departure date****. This is required to ensure that a device is available, and its services can be successfully provisioned prior to your departure.*
- ***The laptop must be picked up within 2-3 business days prior to Travel Departure Date,*** *or your reservation will be cancelled. Only the traveler will be allowed to pick up the laptop. Allow sufficient time for pickup due to the onboarding process that ITS requires. Contact ITS to schedule a time to pick up the laptop.*
- ***The laptop must be returned within 5 business days of Travel Return Date****. Contact ITS to schedule a time to drop off the laptop.*

International Travel Security Risks

Traveling anywhere with mobile devices involves risks, including the loss of the device or malicious hacking of the device. Loss of the device can mean the loss of data and can afford unauthorized

individuals the opportunity to use the device to get access to your personal or professional accounts and information. In addition, a lost device that falls into the wrong hands can provide individuals a path into university systems. Hacking is a possibility in any location including home or the office but is especially likely in places like airports and hotels when accessing unsecured networks.

The best practice for managing risks for these devices is to not take your own device with you and instead use a device from RISE's Loaner Laptop Program that has been prepared for your travel. The Program is described in detail below.

Export Control Implications

The U.S. Export Controls laws and regulations exist to protect the national security, economic interests, and foreign policies of the United States. The Office of Research Integrity, Security, and Ethics (RISE) at FSU was created to provide best practices advice and hands-on assistance to the University community for compliance with various laws and regulations. These regulations apply to research equipment, mobile technology, software, data, etc.

For individuals traveling internationally, two major issues will drive the applicability of export restrictions: type of technology and travel destination. Consult RISE well in advance to determine if an export authorization will be required. Note that obtaining a license, if required, can take up to several weeks or months.

RISE's Loaner Laptop Program International Travel

The risks associated with carrying electronic devices while traveling arise from two sources: the likelihood that your device will be compromised and the impact of such a compromise. These risks fall into two main categories: exposing information the university is required to protect (i.e., restricted, classified, controlled-unclassified, or export-controlled data) and being compromised by malware while traveling. The likelihood of being compromised by malware is greatest when traveling outside of the US and especially high when governments operate and manage the Internet. Taking your work laptop while you travel significantly increases the possibility of data and identity theft. Therefore, international travelers should take *extra* precautions. Understand that foreign universities, governments, and companies are often linked.

Any inquiry regarding your research may have an ulterior motive, such as stealing intellectual property. Be cautious of unsolicited requests and questions about your research or other sensitive information. A clean laptop provides you and FSU extra security in the event that the laptop is compromised and will assist with maintaining export control compliance.

The Loaner Laptop Program for International Travel is sponsored by the Office of Research Integrity, Security and Ethics (RISE), in collaboration with Information Technology Services (ITS). The Program offers loaner laptops free of charge to individuals traveling abroad to lessen the associated security risks while allowing full use of most software applications.

Laptops are available only to FSU faculty and staff for the purpose of conducting University business and program activities during international travel. The use of one of the loaner laptops is free; however, costs of lost, stolen or damaged equipment may be the responsibility of the borrower and his or her department.

It is strongly recommended that your work laptop is not transported to any of the below countries.

- Belarus
- Cambodia
- China
- Cuba
- Iran
- North Korea
- Russia
- Sudan
- Syria
- Ukraine (Crimea and other Russian-held Regions)
- Venezuela

Types of Laptops Available

- Windows Laptop
- MacOS Laptop

Software Installed

- Microsoft Office O365
- Adobe Creative Cloud Application Manager
- Adobe Acrobat DC Cloud
- Microsoft Edge (Windows)
- Safari (Mac OS)
- Mozilla Firefox
- Google Chrome
- VLC Media Player
- Microsoft Security Suite
- FSU Virtual Private Network client
- Remote Support Client

RISE and ITS will consider requests to install specialized software or applications that are available through the University. However, ITS will only install software or applications on a device if the licensing agreement includes international use rights.

Accessories

- Carrying case
- International Universal Power Adapter
- Charging cable

VPN Access

Appropriate VPN software will already be installed on the laptop. During ITS's onboarding process with the traveler, they will ensure that traveler is able to log in to VPN.

Download Duo Mobile App to Your Smartphone

Two-factor Authentication (2FA) is an extra layer of security designed to prevent unauthorized access to your FSU account. It protects your data from phishing attempts and other digital threats by determining that you are who you say you are, and not just someone using a stolen password. 2FA requires you to verify your identity twice—once with your password and once with a device—before you can access certain FSU systems and protected information. After you sign in with your FSUID and password, you will verify your identity with a smartphone or token. The process takes just a few clicks or taps.

Download the Duo Mobile app to your smartphone before leaving the U.S. If you do not have a smartphone or prefer not to use your phone for this purpose, you can authenticate with Touch ID or a Duo Token from the FSU Bookstore.

Request a Loaner Laptop

Laptops are available on a first-come, first-served basis. Submitting a request does not guarantee that a device will be available. You must submit the Request ***no later than 10 business days prior to your departure date.*** This is required to ensure that a device is available, and its services can be successfully provided prior to your departure.

The length of checkout should not be longer than 30 calendar days. If you must keep it longer, specify the reason in your request. Note that ITS may be unable to accommodate your request due to laptop availability. Laptops are not available for extended travel, sabbaticals, or as departmental replacements.

Complete and sign the *Loaner Laptop Request Form* and submit it to RISE via DocuSign or email (research-compliance@fsu.edu). RISE will forward the Request Form to ITS for final approval. ITS will notify you when the reservation has been approved, but at least within 5 days prior to your departure.

THE TRAVELER IS THE ONLY PERSON THAT CAN PICK UP THE LAPTOP. Upon notification that your reservation has been approved, contact Darryl Sims (850-645-8038; dsims2@fsu.edu) to schedule the pickup. The loaner laptop should be picked up at Rod K. Shaw Building (RSB) on FSU main campus. You will need to provide University identification and sign the checkout sheet when picking up the laptop, in addition to completing the loaner laptop onboarding process.

Sensitive Data

In order to comply with the University's security policy, as well as with federal export and privacy laws, travelers should not copy or download any sensitive data or information onto the internal storage of a loaner laptop. Sensitive data includes, but is not limited to, non-public research data (e.g., export-controlled; controlled unclassified, etc.), University business information, student information, and personally identifiable information of university employees. Contact RISE if you must take sensitive information abroad.

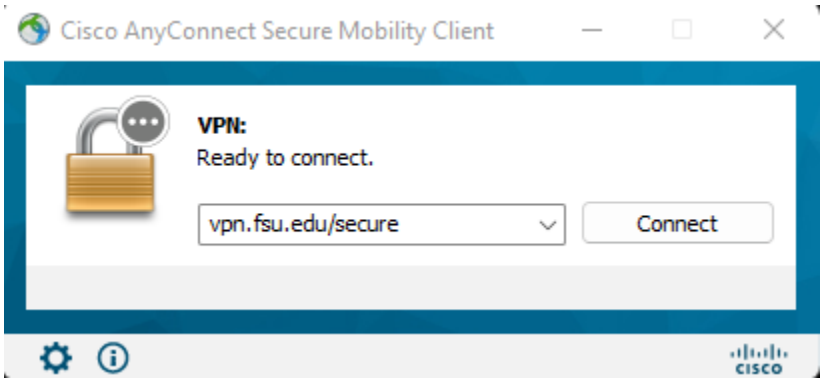
Failure to comply with export and privacy laws could result in fines to be paid by the traveler and the University, and/or imprisonment of the traveler. If such export is approved and an export license is not required, an encrypted[1] USB flash drive must be used to store the data. If an export license is required, the security measures outlined in the license must be followed.

Username and Password

Do not use your normal FSUID and password to log into the laptop. ITS will provide a unique USERID and Password for you to use while you have the loaner laptop.

Connecting to FSU while Abroad

During your international travel, your device should be securely connected to the FSU network by accessing the virtual private network (VPN) profile: "vpn.fsu.edu/secure". **Be sure to use the special login provided by ITS during onboarding—not your usual FSUID credentials**.



Depending on where you plan to travel to, electronic communication devices when taken abroad may be subject to involuntary official governmental review or confiscation, and possible duplication of the hard drive's contents.

[1] Because encryption products can be used for illegal purposes many countries may ban or severely regulate the import and export of encryption products. The import of your laptop with encryption software to certain countries could violate the import regulations of the country to which you are traveling, and could result in your laptop being confiscated, fines, or in other penalties. Contact RISE if you know you will need to carry encrypted devices.

Attempts to circumvent national censorship of certain websites, such as some mainstream western social media sites, are discouraged. If you are found to be using a product to circumvent the blocking of censored websites, you may be warned, have your electronic devices confiscated, or you may become subject to criminal charges in your host country.

Personal privacy may not be respected in your country of destination. Even private spaces such as hotel rooms, rental cars, and taxis may be subject to video, audio, or other monitoring. This type of surveillance may be able to track your whereabouts, what you may be doing, what's on your electronic device, and what you may be entering into it. Conversations either in person or on a phone may be monitored. Local colleagues may be required to report any conversations held with foreigners.

Protect the Laptop and Information while Traveling Abroad

The guidelines and recommendations listed below outline and define steps you can take to protect yourself, your information, and your loaner laptop.

- When not in use, shut down the laptop completely. Do not use sleep mode.
- Minimize the data contained on the device. This is particularly true of logins and passwords, credit card information, your social security number, passport number, etc.
- Assume that anything you do on the laptop, particularly over the Internet, will be intercepted. In some cases, encrypted data may be decrypted.
- Keep the laptop with you at all times during your travel. Do not assume they will be safe in your hotel room or in a hotel safe.

Reporting a Lost, Stolen, Confiscated, or Maliciously Destroyed Loaner Laptop

In the event of a lost, stolen, confiscated, or maliciously destroyed loaner laptop, IMMEDIATELY notify the following individuals:

- Mary Sechrist, RISE: (850) 644-9947; m.sechrist@fsu.edu
- Darryl Sims, ITS: (850) 645-8038**;** dsims2@fsu.edu

The traveler's department may be held responsible for replacement costs.

Returning the Loaner Laptop

- **The loaner laptop must be returned within 5 business days of your return.** Contact Darryl Sims (850-645-8038**;** dsims2@fsu.edu**)** to schedule the drop off.
- Return the loaner laptop to the Rod K. Shaw (RSB) building where it was collected. Be sure to sign the check-in sheet.
- Travelers are responsible for transferring all data to an external storage device before returning the laptop. Do not connect the loaner laptop to the FSU network or to any wired network ports at the University. Any data left on a loaner laptop will be destroyed and will not be retrievable. Neither ITS nor RISE is responsible for lost data.

- For security reasons, laptops will be wiped, reformatted, and reimaged immediately upon return.
- **VERY IMPORTANT:** Upon returning to the United States, change your FSUID password as soon as possible. **DO NOT USE THE LOANER LAPTOP TO CHANGE YOUR PASSWORD.** Using your managed work device, change your FSUID password by logging into MyFSU, then clicking on *MyFSU Identify Management* under MyFSU Links. Click on *Change Password* and follow the instructions.

* * * * *