Office of the Vice President for Research
Iowa State University

Unit: Office of Research Integrity
Effective: Immediately
Reviewed/Revised: 5-19-17
Contact: vpr@iastate.edu

International Travel with Laptops and Other Electronic Devices Guidelines

Import Restrictions on Encrypted Devices

Encrypting your files, or the complete hard disk, is generally considered a best practice for data security. However, some countries restrict the import of encrypted devices, and U.S. regulations prohibit the export of an encrypted device to embargoed countries.

The information below is subject to change. Please check with the embassy of the country you are leaving from and/or traveling to for the most up-to-date information. If you have encryption enabled on your device please be sure to ask specifically about the regulations for encryption.

The following countries restrict the import of encrypted devices and do not recognize a personal use exemption. If you are traveling to any of these countries, leave your devices in the U.S., or take a clean, unencrypted laptop.

Belarus	Israel	Saudi Arabia
Burma (Myanmar)	Kazakhstan	Tunisia
China	Moldova	Ukraine
Hungary	Morocco	
Iran	Russia	

U.S. Embassies website: https://www.usembassy.gov/

Export Restrictions

Traveling outside the U.S. with laptops, tablets, smart phones, or storage devices involves special considerations and may require an export license:

- **Hardware**. Generally speaking, computer hardware is not subject to tight restrictions, as long as the hardware returns to the U.S. Many countries allow items for personal use.
- **Software**. Most commercial and public domain software is often already licensed for export — this can be confirmed by checking with the vendor (e.g., www.microsoft.com/exporting/). The most significant restrictions pertain to encryption software. Commercially-available software (including the software provided by Iowa State) can be installed on devices that otherwise qualify for the exemptions listed below. Noncommercial encryption software in source code or object code is likely to be restricted; please check with the Export Control office, export@iastate.edu, if you have questions.
- **Controlled data**. If you are working on a project that involves EAR- or ITAR-controlled technologies, your device may contain controlled technical data that cannot be shared with foreign parties without a license. **Do not take a device with such data outside the U.S.**
- **Other private data**. Aside from export control laws, Iowa State University policies regarding protection of financial, FERPA, and HIPAA-controlled data recommend that such data not be stored on devices taken outside the U.S.

If the computer or other equipment is owned by Iowa State University, the equipment as well as any pre-loaded encryption software may be eligible for License Exception TMP (Temporary Exports). To qualify for this exception, the equipment:

- Must be a “tool of the trade.”
- Must remain under your “effective control” while overseas. This means that it must remain in your personal possession or in a locked hotel safe (a locked hotel room is not sufficient) at all times.
- Must be returned to the U.S. (or destroyed) within 12 months.
- May not be taken to embargoed countries *(See table below).*

If you personally own the equipment, it may qualify for License Exception BAG (Baggage). To qualify for this exception, the equipment and pre-loaded encryption software must be for your personal use in private or professional activities.

Do not take with you ANY:

- Data or information received under an obligation of confidentiality or non-disclosure.
- Data or analyses that result from a project for which there are contractual constraints on the dissemination of the research results.
- Computer software received with restrictions on export to or on access by foreign nationals.
- Devices or equipment received with restrictions on export to or on access by foreign nationals.
- Private information about human research subjects.
- Devices, systems, or software that was specifically designed or modified for military or space applications.

Beyond export laws, you should also be aware that traveling with electronic devices may result in unexpected disclosure of personal information. Certain countries are known for accessing files upon entry, so you should be extremely careful about any proprietary, patentable, or sensitive information that may be stored on your device.

The information below is subject to change. Please check with the Office of Foreign Assets Control (OFAC) for the most up-to-date information. If you have encryption enabled on your device, please be sure to ask specifically about the regulations for encryption.

Embargoed Countries: If you are traveling to any of these countries, leave your devices in the U.S., or take a clean laptop. *(See below for program information)*

Crimean Region of Ukraine	Iran	Syria
Cuba	North Korea	Sudan

OFAC website: http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-AssetsControl.aspx

Recommendations

1. Leave your work and personal electronic devices in the U.S. and take a prepaid no-contract mobile phone.
2. If you must bring a laptop, do not take your normal device with you. Recommended best practice for international travel would be to take a "clean laptop," which is a laptop that does

not include any export-restricted hardware, software, data, or information. This is especially true when traveling to China or Russia. Never use shared computers in cyber cafes, hotel business centers, or a device belonging to someone else.

3. When not in use, turn off the device(s).
4. Protect the device(s) with a long and complex password that you do not use on work and personal devices.
5. Minimize data contained on the device(s).
6. Keep the device(s) with you at all times during your travel.
7. When you return to the U.S., immediately discontinue use of the device(s). The hard drive should be reformatted and the operating system and other software reinstalled.
8. Change all passwords you may have used abroad.