International Travel Tips to Secure Your Data and Laptop

International travelers should take extra precautions. When you travel abroad, everything you take with you is considered an export. What you take with you may be restricted, depending on where you are going and what you are doing.

This applies not only to tangible items (research equipment, biological agents, chemicals, and toxins) but also to intangible items (software, research data, encryption code). Certain information technology, software, and equipment you take with you may be subject to U.S. export control laws. Any computers or laptops that contain non-commercial, special purpose, or encryption software may be export controlled and require special considerations to export outside the United States. Radford University IT Security has information to consider prior to travel regarding laptop computers, tablets, and securing data.

You may take a laptop on international travel if it does not contain any work or data involving projects with:

**Foreign National Restrictions** – A grant/contract that contains a restriction on the use of foreign nationals.

Note: For export control regulation purposes, an individual is NOT a foreign national if he/she:
- Is a U.S. citizen;
- Is granted permanent residence (“green card”); or
- Is granted status as a protected person (political asylum)

**Publication Restrictions** – A grant/contract that contains a restriction on the publication or disclosure of results to the public or unapproved parties/

**Technology Control Plan (TCP)** – A TCP may be put into place on a grant/contract/project to control the dissemination of controlled information, data, or defense service as defined in ITAR to foreign persons.

**Proprietary Information** – A grant/contract/project that involves information that is not public knowledge (such as test results or trade secrets). The recipient is generally duty bound to desist from making unauthorized use of the proprietary information.

**Tips for Preparing for Domestic and International Travel**

- Back up your data and leave a copy of your files in a safe and secure location such as your office or a Radford University fileserver.
- Ensure that your operating system has a strong password or passphrase when it boots up.
• Password-protect, encrypt, or remove all student, personal and proprietary information stored on your laptop.

• Turn off file-sharing and print-sharing. *

• Apply all software patches and updates. *

• Ensure that anti-virus, anti-spyware, and personal firewall software is installed on your laptop. *

• Install a Virtual Private Network (VPN) client on your laptop so that you can securely access Radford University resources such as Banner, and OneCampus while traveling. If your department does not have a VPN client, have your Radford University IT representative install the Radford VPN client on your laptop prior to travel. *

• Plan ahead and purchase a tracking application for your laptop in case it is lost or stolen.

  Notes: Plan ahead and consult with your department’s IT point-of-contact on how to securely access your departmental fileserver, mail server, or desktop.

  *If you are not responsible for managing your laptop, consult with your Radford IT point-of-contact regarding this task.

• Remove all work from your laptop that contains export-controlled information or involves a project with foreign national restrictions, publication restrictions, or Technology Control Plans (TCP).

It is recommended that an export review be performed on the following types of international travel:

• Traveling to an embargoed or high security risk country
• Taking Radford University-owned property
• Conducting research abroad