TECHNOLOGY INFORMATION GUIDE *for International Travel*

Notre Dame faculty, staff and students who travel to international destinations to conduct University business must comply with the guidelines in the IT Security for International Travel Standard. You can review the IT Security for International Travel Standard, at: ntrda.me/travelstandard.

NOTE: This standard only applies to faculty, staff, and students engaged in activities, programs or business related to the University.

WHAT YOU NEED TO KNOW

When traveling to any international destination, you must follow these guidelines to keep University data and mobile devices (laptop, mobile phone and tablet) safe:

- Do not travel with or access *highly sensitive University data* during your trip.
- If you need access or have been approved for access to sensitive University data while traveling, remove all unnecessary sensitive data from any mobile device you will take on your trip before you leave. You should store this data in a University approved storage service such as Box or Google Drive.
- Familiarize yourself and comply with any export control restrictions for any data you may have on your mobile device or may access during your trip.
- Be sure to protect your mobile devices and data by:
  - Configuring a password or PIN to log on to your mobile devices helps prevent others from accessing your data if the device is lost or stolen.
  - Encrypting the data on your mobile devices helps prevent unauthorized disclosure. Your departmental IT support staff or the OIT Help Desk can assist you with encryption.

Specific countries have been identified with known threats that target the information technology resources of travelers. As a result, restrictions were put in place to minimize the risk of University data and mobile devices while traveling in those areas. These countries are divided into two risk zones:

- **High Risk countries: China (including Hong Kong), Russia:** Identified by the U.S. government as having foreign intelligence services known to target the information technology resources of travelers and represent a high risk to travelers with mobile devices.
  - If you need access to a mobile device while traveling, you need to make arrangements for a rental device through your departmental IT support staff or the **OIT Help Desk** at **574-631-8111** or **oithelp@nd.edu** at least two weeks prior to your departure.
- **Export Control countries: Cuba, Iran, North Korea, Sudan, Syria:** Under embargo for U.S. export control restrictions for encryption technologies.
  - If you need access to a mobile device while traveling, you need to obtain approval from the head of your department and the Director of Information Security at least two weeks prior to your departure.

You must not take your University issued laptop, tablet or mobile phone to High Risk of Export Control countries. We strongly recommend leaving your personal devices at home.

If you are a first-time traveler to a High Risk or Export Control country, a representative from the Office of Information Technologies Information Security division will contact you at least two weeks prior to your departure. Additional details on what you need to do before, during and after your trip is located on the back of this card.

For information on traveling safely with your mobile devices, visit: **ntrda.me/international.**

If you have any questions about traveling internationally with a mobile device, contact your departmental IT support staff, or the **OIT Help Desk** at **574-631-8111**, **oithelp@nd.edu** or chat online at **help.nd.edu.**

UNIVERSITY OF NOTRE DAME | INFORMATION TECHNOLOGIES

Checklist for HIGH RISK & EXPORT CONTROL COUNTRIES

MOBILE DEVICE REQUIREMENTS

You must not take your University issued laptop, tablet or mobile phone to a High Risk or Export Control country. The Office of Information Technologies (OIT) Information Security division strongly recommends leaving your personal mobile devices at home as well.

BEFORE YOU LEAVE

1. If you are a first-time traveler to a High Risk or Export Control country, a representative from the Office of Information Technologies Information Security division will contact you at least two weeks prior to your departure. Returning travelers are not required to do so.
2. Do not copy any files containing highly sensitive data (social security numbers, credit card numbers, etc.), onto any mobile device you will take on your trip.
3. Log out of your Notre Dame Box account, Google account, etc., on any personal or University-owned device before you leave.
4. Be prepared to use two step login when traveling away from the University in the United States or abroad.
   - ✦ Review the devices you have enrolled in two step login on your Two Step Device Management page at twostep.nd.edu.
   - ✦ Be sure to have at least two or more devices enrolled, and take the enrolled device(s) with you on your trip.
   - ✦ The Duo app on your smartphone can be used without a cellular signal over WiFi, or with no connection to generate a one-time use passcode.
   - ✦ A key fob is another option to use when you cannot bring your smartphone or tablet on your trip. It is a portable device that can be purchased using a departmental FOAPAL, at: ntrda.me/twostepkeyfob.

DURING YOUR TRIP

1. Maintain possession of your mobile devices at all times.
2. When connecting to the Internet, always login to the **Notre Dame VPN** first. Use **NetID.nosplit** as your username **(e.g., jdoe.nosplit).**
3. Be aware that some websites may only be available intermittently due to foreign government regulations, even when you use the Notre Dame VPN. For a listing of the countries that restrict Google access, go to: **ntrda.me/googleaccess.**
4. Do not apply updates or patches to your laptop or cell phone while traveling.
5. If a border agent requests access to your mobile device, offer to login to the device yourself. Do not give anyone the password to your device unless you are required to do so. Change your password as soon as possible if you must provide another individual with your password.
6. Do not connect to a USB flash drive, external storage drive, CD, DVD, or other media supplied in any High Risk country, and do not bring these devices back to Notre Dame.

WHEN YOU RETURN TO CAMPUS

1. Once you return from your trip, you need to return rented mobile devices to your departmental IT support staff or the OIT Help Desk as soon as possible. **Do not use any rental device on your home network or the campus network.** The device must be properly analyzed and cleaned before connecting it to the network.
2. Change your NetID password and any other password you used while traveling on a computer that you did not take on your trip, such as your home or office computer. **Do not change your password using the rental laptop computer.**

UNIVERSITY OF NOTRE DAME | INFORMATION TECHNOLOGIES