Data Security and Technology Protection for International Travel

For members of the campus community, a trip to a foreign country presents unique data security challenges. The nature of international travel requires you to use your technology (laptop, tablet, or smartphone) in various unfamiliar places that may expose Bates' data and devices to malicious people and software. Following are a series of steps that you should take throughout your trip (before, during, and after) to safeguard your technology.

In addition to voluntary cybersecurity and technology protections, international travelers need to consider US export control laws and import restrictions imposed by the destination countries. Bates' Dean of Faculty Office has a website dedicated to export control that provides specific steps Faculty need to take prior to travel. US Export control laws are federal regulations that control the conditions under which certain information, technologies, and commodities can be transmitted overseas to anyone, including U.S. citizens, or to a foreign national on U.S. soil. Failure to comply with these laws can result in significant fines to you as an individual. Routine educational and research activities at Bates are generally exempt from export controls. If you have any questions about US Export control laws, please contact the Director of Sponsored Programs and Research Compliance at sparc@bates.edu.

If you have any questions about securing your data on your trip, please contact the Director of Information Security, Privacy, and Compliance at infosec@bates.edu.

BEFORE YOUR TRIP

1. Identify if the place you will be traveling to is defined as a "high risk" country by the U.S. Department of State as they issue current travel advisories and alerts that may affect your travel. The State Department establishes risk indicators based upon crime, terrorism, civil unrest, health, natural disaster, etc. While not specific to data security the State Department describes the risks and provides clear actions we should take to help ensure our safety. Follow the State Department's recommendation for whichever country you intend to visit.
    a. **Beginning May 5, 2022** - If you are visiting any of the following countries/regions please contact the Support Desk so you can have your Duo account put into bypass mode - this will allow you to access Bates resources without needing to use Duo's Two-Factor Authentication.
        i. Cuba
        ii. North Korea
        iii. Iran
        iv. Sudan
        v. Syria

vi. Crimea region
vii. Sevastopol region
viii. Donetsk region
ix. Luhansk region

2. The following nations restrict the import of encrypted devices and do not recognize a "personal use exemption". A group of nations negotiated a set of rules attempting to facilitate traveling with encryption software known as the "Wassenaar Arrangement." One of its provisions allows a traveler to freely enter a participating country with an encrypted device under a "personal use exemption" as long as the traveler does not create, enhance, share, sell or otherwise distribute the encryption technology while visiting. In general, low-risk countries, e.g., the EU, Australia, and Canada are safe. If traveling to one of the following countries, it is best to leave your laptop home and consult with the Bates IT Service Desk to borrow a loaner laptop for your trip.

Belarus	Hungary	Morocco	Sudan
Burma (Myanmar)	Iran	North Korea	Syria
China	Kazakhstan	Russia	Ukraine
Cuba	Moldova	Saudi Arabia	

3. Regardless of where you are going abroad, be sure your Bates laptop is configured with Bates' VPN software. Using the VPN will allow you to access campus resources (e.g., campus network drives, Banner). Consult with Bates IT Service Desk for assistance.
4. Backup your data. Whether you are traveling with a loaner computer, your regular computer, tablet, or smartphone, you should always backup your data. Consider moving your documents pertaining to Bates to a College-provided folder (i.e., Google Drive) that you can access remotely instead of carrying these files on your local device(s).

DURING YOUR TRIP

1. Do NOT leave your device unattended, especially in your checked bag on your flight. If you ever leave your computer, make sure to turn it off completely instead of just hibernating it or putting it to sleep. When the computer is off, it is fully encrypted.
2. Connect only to known wifi networks. Anyone can create a network and give the network a legitimate-sounding name, hoping to lure unsuspecting travelers to connect while capturing personal information transmitted through the network. This is especially prevalent at public cafes, hotel lobbies, and airports. When connecting to a network, find out the correct network name from the staff at the business and connect to it.
3. Use EDUROAM where available. It provides easy, secure connectivity from thousands of hotspots across more than 100 countries. Eduroam (education roaming) is the secure, worldwide roaming access service developed for the international research and

education community. Eduroam allows students, researchers, and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions.

4. Turn off your wifi when not in use. Attackers can easily spoof Wifi network names to connect to devices within range for eavesdropping. To help you avoid accidentally connecting your device to rogue wifi networks at a later time, once you are finished using the network, turn off wifi on your device.
5. Do NOT enter your credentials into public computers. Public computers such as hotel business center workstations and internet cafe computers are often poorly managed and provide minimal security protection for their users.
6. US Customs and Border Protection may request that you be subject to an inspection of your electronic devices for a variety of reasons. Please review their Quick Reference to familiarize yourself with the process.

UPON YOUR RETURN HOME

- Upon returning home and returning your loaner device, change any passwords you used while you were traveling. Use a trusted computer, whether it's your own or one provided by the IT support staff, to reset credentials that were used during the trip. For example, if you use your Bates credentials during the trip, go to the Bates IT Service Desk website to reset your Bates password.