Baldwin Wallace University Information Technology Guideline

Issued by:	**Information Technology**
Title:	**IT Guidelines for International Travel**
Number:	**ITG-BW-21-01**
Publish date:	**December 15, 2022**

Being prepared for safe international travel from a device and data security perspective is essential. Personal rights and privacy do not exist in many foreign countries, including perceived friendly European NATO members. Cybercrime, spying, and espionage are real and significant threats.

Before You Leave:

- Request a travel laptop and cell phone from IT Support Services and leave your personal devices at home.
    - If you must take your personal device(s), install all the latest software patches and updates as well as anti-virus software.
    - Backup mobile devices you are taking in case they are lost, stolen, or confiscated.
    - Request the use of a BW VPN (Virtual Private Network) from IT Support Services. A VPN creates a secure connection between your device and the websites you access. It protects both your passwords and data.
- Contact IT Support Services and request a temporary Office 365 email account to use while traveling. Request your email to be forwarded to the temporary account for the duration of your trip.
    - The temp account helps protect your information and BW's systems because you will not directly be accessing BW with your ID and password.
- Minimize the amount of data you take with you. Assume that any data you take into a country will be stolen. FYI: Even encrypted data is vulnerable.
    - If you need access to data while traveling, store it in the OneDrive app on your temporary Office 365 account and access it there. Do not download data to your device.
- Take an electrical wall outlet charger for your phone with you. Do not use the USB charging ports you find at a hotel or airport. That is an easy way to get your device infected.
- Consider purchasing and using a privacy screen filter for your laptop – a polarized sheet placed over the device screen that can help block unauthorized side views.
- **WARNING:** Do not travel with encrypted devices to China, Russia, India, Israel, and a few other locations unless you have advance approval from that country. They severely restrict the import of unapproved encryption. (Meaning they have the keys to unlock your information without your permission.) If you attempt to enter their country with an encrypted device, you may be

detained and asked for the decryption key or your device may be confiscated.

While Traveling:

- Avoid transporting electronic devices in checked baggage.
- Turn off WiFi, Bluetooth, and GPS to prevent your devices from being attacked and you from being tracked. (Yes, this actually happens.)
- If a customs official demands to examine your device, or if your hotel room is searched while the device is in the room and you're not, assume that the device's hard drive has been copied.
- Assume you are being monitored, even in your hotel room. Surveillance can and does take place in cabs, restaurants, and other venues.
- Never leave your electronic devices in your hotel room. Take them everywhere you go.
- Never use a USB charger in the airport or hotel to prevent catching a computer virus.
- Only use your VPN to access any sites on the internet.
    - Pro Tip: Try logging on to a public Wi-Fi using the wrong password before you trust it. If you can get on anyway, that's a sign that the network is not secure.
- Never plug someone's USB stick into your computer as it may contain a computer virus.
- Avoid using public workstations. The security of public workstations, especially in high-risk countries, cannot be trusted. If you must use a public workstation, assume that anything you enter into the computer - IDs, passwords, data - may be captured and used.
- If any of your BW devices are lost, stolen, or confiscated, contact BW IT immediately.
- If presenting or sharing research and data, be cognizant of different laws and social norms regarding intellectual property. Members of your audience may be subject to different legal and professional standards regarding the reproduction of your information or materials.

When You Return:

- **Stop using the devices you took with you. Do not connect any devices you took with you to your home network or BW's network.**
    - Immediately return BW devices to IT Support Services.
    - If you took any personal devices, assume they were infected. You should reinitialize laptops and perform a factory reset on phones and tablets.
- Contact IT Support Services and have your temporary Office 365 account deleted.
- Change all the passwords you used on the devices you did not travel with.
- Consider monitoring all the credit cards you used and accounts you accessed while traveling.

Travel to The People's Republic of China or Russia – Special Circumstances:

- Be aware that access to many sites such as Gmail, Google apps, Wikipedia, and Yahoo Web Mail may be blocked or filtered.
- Connections are not secure and may be monitored by the government.

- Those people who are using VPNs in these countries to keep their communications secure have reported that they are often unable to connect using their VPN for hours at a time, forcing them to use unsafe network connection methods.
- Hotel staff and government officials have been documented accessing hotel rooms and the safes in those rooms. Do not assume your computer or mobile device is safe there. Keep them in your personal possession at all times.