# Guidelines for International Travel and Export-Controlled Technology

International travel programs are an important part of the academic experience for many students. Similarly, Marquette faculty and staff often travel abroad on university business, research, or while representing the university at academic conferences or other activities.

International travel is one of the best ways to gain educational and cultural experiences. Still, international travel has risks, especially regarding the security of technological resources like laptops, smartphones, and mobile devices.

This document provides essential technology guidelines and tips for international travel. These guidelines are designed to help protect you and your devices, as well as university and personal data while traveling.

Please contact the IT Services Help Desk (414-288-7799 or helpdesk@marquette.edu) if you need assistance or have questions about the guidelines listed below.

### Who are the guidelines for:

All university personnel, including faculty members, visiting faculty members, students and staff who plan to participate in international research collaborations, international travel, or use computer software with encryption features or proprietary industry technology outside the U.S.

### Why are these guidelines important?

The reason for this guidance is that there are export control laws and regulations that exist to secure sensitive goods, technology, and information from other countries, individuals, and organizations. These guidelines are designed to protect national security, prevent the spread of weapons of mass destruction, and safeguard other important interests. The main export controls that align to the university are:

1. The US Department of Commerce, Bureau of Industry and Security (BIS) is responsible for administering and enforcing the [Export Administration Regulations](https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear) (EAR).
2. The US Department of State, Directorate of Defense Trade Controls (DDTC) is responsible for administering and enforcing the [International Traffic in Arms Regulations](https://www.pmddtc.state.gov/?id=ddtc_public_portal_itar_landing) (ITAR).

A person who violates these regulations may be subjected to civil and/or criminal penalties, including fines and/or imprisonment. In the United States, violations of export control regulations can result in severe penalties, including fines of up to $1 million per violation, imprisonment for up to 20 years, and the loss of export privileges. In addition, the U.S. government may impose sanctions on the individual or university that violates the U.S. export control regulations.

## General Technology Guidelines

### Assume all your connections are being monitored or intercepted

It is always best to assume that your Wi-Fi or ethernet connections are being monitored or intercepted. You should not trust the public or open networks in your hotel, local coffee shop, airport, or train station.

### Never use public Wi-Fi, computers, or devices

Public, free Wi-Fi connections cannot be trusted and may compromise your device if you attempt to connect. Public computers or workstations should be considered compromised, and you should not use them for work or personal reasons.

### Keep your device with you at all times

Do not let your devices leave your sight. If customs or law enforcement officials inspect your device while out of view, it is safe to assume it has been compromised. Do not leave your devices unattended in a hotel room, conference center, or foreign office.

### Do not use unknown storage devices

USB devices (flash or external storage) can be used to install malicious software on your devices. Do not connect any USB devices to your computer, cell phone, or tablet unless you have brought those devices with you. Public charging stations at airports or hotels should also be avoided, as they can transmit harmful software to your devices. Carry your own charging devices and electrical adapters.

### Be mindful of your surroundings

It is common for attackers to snoop or "shoulder surf" while you are entering usernames and passwords on your computer. Be mindful of your surroundings to prevent account and device theft.

### All devices should be erased, restored, or rebuilt upon your return

All devices should be considered compromised upon your return. They could contain malicious software that can infect the university or your home network. The best practice would be restoring your devices to a clean operating system or a restore point from before your trip. Always take a backup of your device before traveling. Contact the IT Services Help Desk (414-288-7799 or helpdesk@marquette.edu) for assistance with erasing, restoring, or rebuilding your device upon your return.

### Change your passwords

You should change your password for all services you access while abroad. This should be done for your Marquette University account and any personal email, social, or financial sites you accessed while traveling. Limit the websites you visit while abroad reduces the number of passwords you need to change.

### Do not accept certificate errors or warnings on your browsers

The techniques for intercepting communications can sometimes require you to bypass error or warning screens. Do not accept expired or self-signed certificates when connecting to foreign networks. These techniques can decrypt your internet traffic and allow attackers to steal usernames, passwords, and other sensitive data.

### Use a VPN (Virtual Private Network) if you must do university business while traveling

If you must connect to university email, applications, or systems while abroad, use a VPN to enforce strong encryption on your connections and data. Marquette's VPN client is available for download at <https://vpn.marquette.edu>. Guidance for setting downloading and setting up VPN access is located here: <https://www.marquette.edu/its/help/vpn/vpn.php>

## Laptops

### Keep your operating system up to date

The laptop's operating system, whether it be Windows, macOS, or Linux, should have the latest security patches.

### Uninstall applications that you do not need

Keep only those applications that are necessary for your travel. Uninstall any applications that you do not need or do not use. Ensure that all applications are up to date with the latest security patches. This is especially important for those applications that interact with the web, including web browsers, Adobe Acrobat, and Java. Be aware that U.S. export control laws preclude bringing some software applications across the borders of many countries.

### Update the settings on your web browsers

All web browsers should be set to automatically clear your browsing history and cache after each session. Here is an article that provides general guidelines on how to automatically clear your browsing history and chase for main browsers <https://www.pcmag.com/how-to/how-to-clear-your-cache-on-any-browser>. If you have questions or are having issues with applying these settings to your preferred web browser, please contact the IT Services Help Desk for assistance.

### Verify your antivirus software is up to date

Ensure the latest version of antivirus software is installed on the laptop. If you are using a university issued laptop, antivirus software will be automatically updated so long as the computer has been connected to the university network either while on campus or through VPN within the last 24 hours.

### Remove any sensitive or confidential data

Before your travels, remove any sensitive or confidential data from your laptop. This includes student information (grades, student work, information not available in a public directory), proprietary information (including research), University business or planning documents, personal/financial information, and other materials that should not be made public. Materials related to the travel arrangements, presentations, supporting materials, educational information, and any other public domain documents can reside on the laptop.

Data that is stored on Microsoft’s One Drive is not directly on your computer but is instead stored in the cloud managed by IT Services. When traveling internationally, efforts should be made to not access One Drive data, but if required should be done using VPN only.

**Borrow a Clean Laptop from IT Services for your Trip**

IT Services can provide you with a fresh loaner laptop for international travel, but notice should be given at least two weeks prior to the trip to ensure a loaner laptop is available and can be formatted for you.

## Cellphones and Mobile Devices

### Consider using a non-smartphone

Modern smartphones are essentially computers containing all our email, private communications, and contact lists. These are high-value targets for cybercriminals. When traveling abroad, the safest action is to procure a non-smartphone that will be used only for making calls.

### Back up and reset your device

If traveling with a smartphone or mobile device, you should back up the device and reset it to its factory default setting. This will clear all personal information from the device and allow you to selectively copy certain information back onto the device. Upon return, you can then restore the device to its previous state.

### Limit data contained on the device

Email and contact lists on cell phones often contain information useful to cybercriminals. Email can contain sensitive and highly confidential information. When traveling, it is best to remove email accounts from your device, including your university email account and personal accounts like Gmail.

### Use strong PINs or passcodes

Use a strong passcode to protect cell phones and mobile devices. This will prevent others from picking up your device and gaining access.

### Disable Bluetooth, Wi-Fi, and NFC

Unless you actively use these features, you should disable them on your phone. Enabling these services allows attackers to see and potentially gain access to your device.

## Marquette IT Services Assistance

### Inventory your equipment

Marquette IT Services can inventory your equipment before your travels. This will allow us to assist you in reporting lost or stolen devices, should you need to do so while traveling. We can then verify the state of your operating system and applications and determine whether sensitive data is on the devices.

### Monitor your accounts

Marquette IT Services will monitor the logins from your account to look for any abnormal behavior. We will contact you immediately to change your password if we identify any suspicious behavior associated with your account.

### Answer questions

Contact the IT Services Help Desk (414-288-7799 or helpdesk@marquette.edu) if you have questions about this document. If you suspect your account or university data is compromised, the Help Desk can notify our security team 24 to investigate.