

# Secure Travel Recommendations

## Secure Travel Recommendations

On this page:

- Overview
  - [MIT International Travel](#)
  - [Secure Devices for International Travel](#)
  - [Applying the Secure Travel Recommendations below](#)
- Recommended Configurations
  - [Laptops](#)
  - [iPads](#)
  - [Mobile Devices/Phones](#)
- [Approved Applications](#)
- [When you return](#)
- [Useful Links](#)

## Overview

When traveling to any country, it is wise to be aware of your surroundings and to take precautions to protect your devices, data, and on-line identity. The use of a [VPN](#) and common sense may be enough in some countries – in other “high risk” countries, stricter measures must be taken.

## MIT International Travel

MIT uses travel warnings and alerts issued by the U.S. Department of State, Centers for Disease Control and Prevention, and World Health Organization to categorize countries with a travel warning level of Extreme, High, or Medium.

For a list of locations with current ratings designated by this policy, check out the [International Travel Risk Policy Country Warning Levels](#) page. For questions and further MIT information please see the [MIT International Travel Risk Policy](#) site hosted by MIT's [Global Support Resources](#) site.

## Secure Devices for International Travel

IS&T maintains a pool of computing equipment available for loan to eligible MIT students, faculty, and staff who are traveling outside of the United States. IS&T recommends leaving your standard MIT-issued and personally owned equipment at home and using loaner equipment when traveling internationally.

- [Secure Devices for International Travel](#)

## Applying the Secure Travel Recommendations below

In general, the below recommendations should be followed for all travel to or through countries designated by MIT with a **High Travel Warning** or higher, designated Level 3 or higher by the US State Department. In addition, several countries present an increased risk to traveling with digital technology in particular, due to digital surveillance concerns or VPN use restrictions. These countries may be rated **lower than the above warning levels**, but the secure travel recommendations listed below should still be followed. Consider [VPN Blocking by Country](#) and [Internet Censorship and Surveillance by Country](#) for more information.

These destinations present different challenges as the use of a [VPN](#) is prohibited, and most of your on-line activity can be monitored or accessed easily.

It is recommended that you do not bring your primary computer and smartphone. A travel device should have a minimal configuration (OS plus only necessary applications), and also be something you can be without in case of loss, theft, or confiscation. See [Secure Devices for International Travel](#) for more information on obtaining a loaner device.

## Recommended Configurations

### Laptops

- [Operating System \(OS\)](#) – Should be latest version with all updates.
- [Microsoft Office](#) – Should be latest version with all updates.
- [PDF Reader](#)
- Email – Use [owa.mit.edu](mailto:owa.mit.edu) (for O365 email users [outlook.office.com](mailto:outlook.office.com)) to view mail on-line.
- Documents – Should be stored on an [encrypted](#) USB device.

## iPads

- **Operating System** latest version of iOS with all patches/updates.
- **Email** should be configured to download 1 week on your mail app.
- **Apps** limited to only travel approved applications. Users will not be able to install any apps, as the device will be locked down, and unable to provide iTunes or other credentials.

## Mobile Devices/Phones

- **OS** Latest version with all updates.
- **Phone number** should be forwarded to travel phone (leave your phone at home please).
- **Email** should be configured to download 1 week on your mail app.
- **Apps** limited to only travel approved applications. Users will not be able to install any apps, as the device will be locked down, and unable to provide iTunes or other credentials.

## Approved Applications

- [TripCase](#) for iOS by Sabre Inc  
TripCase is an all-in-one solution for managing your travel itinerary. This app comes in handy for managing your flights, hotel reservations, and car rentals in one consolidated library.
- [Bing app](#) for iOS by Microsoft  
China has some restrictions on what websites and services you are allowed to use. Google Maps does not work, but Bing maps work and can serve as an alternative to Apple Maps depending on preference.
- **Microsoft Word, Excel, and PowerPoint** by Microsoft  
The Microsoft Office applications Word, Excel, and PowerPoint may be used, but pay careful attention to how you store your files. We recommend that you store any potential sensitive materials on an encrypted flash drives. Note: Microsoft Outlook is not recommended. Only [owa.mit.edu](mailto:owa.mit.edu) should be used from Laptop computers and Apple Mail configured to sync 1 week of email on loaner iPhones.

## When you return

- Change your [Kerberos password](#).
- If you checked your [voicemail] while traveling, change your voicemail passcode.
- If you brought your computer, save any documents you created while traveling to an external drive, then erase your computer's hard drive and restore from your pre-departure [backup](#) upon return. Scan the documents on the external drive with a virus scanner like [Sophos](#) before copying them to your newly restored computer.

## Useful Links

- [MIT's Travel Risk Advisory](#)
- [US State Department Travel Advisories](#)
- [MIT – Risk Classifications](#)
- [Travel and Technology Landing Page](#)