CHRISTOPHER NEWPORT
UNIVERSITY

Information Security Foreign Travel Guidelines

VERSION 1.1

June 2023

Department: Information Security

Proprietary Statement

This document was developed specifically for and by Christopher Newport University. The concepts and methodologies contained herein are proprietary to Christopher Newport University. Duplication, reproduction, or disclosure of information in this document without the express written consent of Christopher Newport University is prohibited.

All Trademarks, Registered Trademarks, Service Marks, and brand and product names used in this document are the property of their respective owners.

Review and Revision History

Date	Version	Description of Change (Affected Sections)	Author
June 2021	1.0	Initial Release	Wendy L. Corrice
June 2022	1.1	Annual Review	Wendy L. Corrice
June 2023	1.2	Annual Review	Wendy L. Wilde

TABLE OF CONTENTS

Introduction

University faculty, staff and students who travel internationally with laptops, phones and other mobile devices are subject to many risks, namely that of loss, seizure or tampering. Please use these recommendations as a guide to reduce the risks associated with traveling with these devices. If you have any questions regarding these recommendations, please contact the Information Security Team at iso@cnu.edu

Scope

Foreign travel is all travel that does not include travel within the fifty (50) United States, Puerto Rico, Guam, and the U.S. Virgin Islands.

Privacy, Censorship and Encryption

Depending on where you plan to travel abroad, electronic communication devices, may be subject to involuntary official governmental review and possible duplication of the hard drive's contents.

The Commonwealth of Virginia Information Technology standard (VITA SEC 501) requires agencies to encrypt laptops with sensitive information, therefore, Christopher Newport University requires the use of encryption on all University-owned laptops. Use of encryption to protect information may be forbidden in some countries, you should check with Information Security before you travel abroad to ensure compliance with foreign countries' laws. And, if your encryption product allows you to "hide" information, those "hidden" areas can be detected, and you could be subject to criminal charges by the country's government. Because it is difficult to monitor encrypted traffic, use of secure ("https") websites and/or use of virtual private networks (VPNs) may be blocked by some countries.

Some countries may censor certain content or sites. Attempts to circumvent national censorship of websites, such as some mainstream western social media sites, is discouraged by the Information Security. You should only use VPN to access necessary files and sites to conduct your business or studies. If you are found to be using a product to circumvent the blocking of censored websites, you may be warned, have your electronic devices confiscated, or you may become subject to criminal charges.

Personal privacy may not be respected. Even private spaces such as hotel rooms, rental cars, and taxis may be subject to video, audio, or other monitoring. This type of surveillance may be able to track your whereabouts, what you may be doing, what's on your electronic device, and what you may be entering into it. Conversations either in person or on a phone may be monitored. Local colleagues may be required to report any conversations held with foreigners.

Import Restrictions

Some countries restrict the import of encrypted devices and U.S. regulations prohibit the export of an encrypted device to embargoed countries.

The following countries restrict the import of encrypted devices and do not recognize a personal use exemption. If you are traveling to any of these countries, leave your devices in the U.S., or take a clean unencrypted laptop.

The following list is subject to change. Please review the U.S. Embassies website at https://www.usembassy.gov for up-to-date country lists and the US State Department Travel Advisories page here: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/.

Belarus	Israel	Saudi Arabia
Burma (Myanmar)	Kazakhstan	Tunisia
China	Moldova	Ukraine
Hungary	Morocco	
Iran	Russia	

General Recommendations

1. Configure a password to logon to any personal devices you are taking. A password prevents others from accessing your data if your device is lost or stolen.

2. Be sure that any device with an operating system and software is fully patched and up-to-date with all recommended security software (e.g. Antivirus).

3. Research your destination on the State Department website.

4. Encrypt your personal devices, but check with Information Security before you travel abroad to ensure compliance with foreign countries' laws.

5. When not in use, turn off or lock the devices.

6. **DO NOT** store Class 1 Restricted or Class 2 Moderately Sensitive data (e.g., social security numbers, protected health information, credit card numbers) on any devices you are taking with you.

7. **DO NOT** copy Class 1 Restricted or Class 2 Moderately Sensitive data to memory sticks or other easily lost media.
8. **DO** store data that you need for your trip in a secure Google share or on the University's network storage server. You can access your files stored on the University's network and other campus resources through the University VPN.

9. Upon your return, immediately change your CNU password and the passwords of any accounts used while abroad. IT Services may scan your device to ensure no malware is on it.

Security Checks

Sometimes airport or other security officers will ask you to start your device to prove that it works. Comply by starting your system and entering the password yourself. If the security officer wants you to give them the password, state that it is Christopher Newport University Information Security policy to NOT share passwords. If they still require you to provide the password to them, give them the password, and change immediately following the check.

Traveling to High Cyber-Risk Countries

Traveling with IT devices to some countries, most notably **China** and **Russia**, is considered high cyber-risk. The U.S. government has issued several advisories that travelers be aware that they could be targets of espionage activities when visiting these countries. Travelers are strongly encouraged to follow these recommendations:

1. **DO NOT** travel with encrypted devices to China unless you have advance approval from China. China severely restricts the import of unapproved encryption. If you attempt to cross the border with an encrypted device, you may be asked for the decryption key or your device may be confiscated.

2. The U.S. government prohibits traveling with encrypted devices to countries that are considered to support terrorism, namely Cuba, Iran, North Korea, Sudan, and Syria. **DO NOT** bring encrypted devices to these countries.

3. Use caution when connecting a USB device to an unknown computer or charger as it may become infected with malware.

4. Upon your return, immediately discontinue use of the devices. The hard drive of the devices should be reformatted, and the operating system and other related software reinstalled, or the device properly disposed of. Contact IT Services to assist you.

Additional Recommendations

1. Avoid using public or shared workstations. The security of these systems cannot be trusted especially in high risk countries. Anything you may enter into the system - Your user ID, password, data, may be captured and used.

2. Be aware of your surroundings when logging in, or inputting data onto your devices. There have been many cases where user credentials or confidential information has been compromised simply by watching the person input the information.

3. Set Wi-Fi to "do not automatically connect to Wi-Fi" on all devices capable of wireless connections.

4. **DO NOT** update your computer while connected to a public or hotel wireless network.
5. Disable Bluetooth on your laptop, mobile phone, and other devices.

6. Set your mobile device to be wiped after 10 login attempts. Backup your device before traveling in case your device is wiped.

7. Tape over any integrated laptop cameras, or disable them to prevent a hacker from viewing you while you use your laptop.

8. Ensure host based firewalls are configured and enabled on Windows and Mac laptops.

9. Leave unneeded car keys, house keys, smart cards, credit cards, swipe cards, or fobs you would use to access your work place, or other areas, and any other access control devices you may have at home.

10. Clean out your purse or wallet of any financial information such as bank account numbers, logins and passwords..