UNIVERSITY OF NEBRASKA UNK KEARNEY

# TRAVELING WITH ELECTRONIC DEVICES

## Information Technology Services

Protecting your devices and data when you are away from home, on personal travel or on university business, will prevent sensitive data being compromised if your device is hacked, inspected, confiscated, stolen or lost. There is risk associated with travel within the United States and with travel abroad. Also, extra precautions must be taken when traveling to high-risk locations.

### Travel in the United States

*Before traveling*

- Only take devices and media that are absolutely necessary.
- Make sure your laptop or mobile device has a strong password. A strong password has upper case, lower case, numeric and special characters; is at least 10 characters in length; is not a word in any language; and is not based on personal information.
- Ensure that all operating system security updates have been applied and that current anti-virus, anti-malware and firewall software are installed.
- Copy your work files to UNK OneDrive network storage so they can be securely accessed when traveling. Do not copy files with personal, confidential, or non-public information to OneDrive.
- Establish VPN access if you will need to utilize UNK/NU applications or connect to a UNK device. To request VPN access, go to http://ww.unk.edu/offices/help_desk/helpdesk_request_form.php
- Do not save personal information, such as credit card numbers, passport information, or social security numbers, on your device.
- Clear the browsing history and any other stored information in web browsers that you would not want others to access.
- Inventory the data that you are traveling with in case your device is lost or stolen.
- Back up data from your device(s) or media that you will take with you onto media that will not be taken on the trip.

*While Traveling*

- Avoid using free wireless services. Assume that any computer network you use is insecure, and avoid business centers, cyber-cafés, libraries, or friends you stay with.
- Never accept software updates on hotel Internet connections or public Wi-Fi.
- Never enter or access sensitive data using a shared or public computer.
- Use the VPN for UNK/NU applications or to connect to a UNK device.
- Keep your device with you and physically secured at all times. If possible, do not leave devices in hotel rooms, unless you can use a safe for storage of valuables. Do not use an obvious laptop storage bag that would make you a target.
- Do not plug USB powered devices into public charging stations because malware can be transferred to your device or data downloaded from it. Use your own charging cable plugged into an electrical outlet.
- Do not accept USB drives or other removable media from any source.
- If your device is lost or stolen, notify UNK ITS for immediate assistance in changing passwords and contact local authorities to report the loss or theft.

*After Traveling*

- Change your UNK and NU passwords immediately after returning.

**International Travel**

Given the current climate of dependency on technology, it is important to be aware of regulations, laws and information safety tips to consider when traveling abroad. Additionally there are strict laws and regulations around export controls which can include technology and data. Export control regulations apply to international travel in relation to items that individuals take with them on a trip to sanctioned or embargoed countries and the conduct of business with, or providing services to, restricted individuals, countries or entities.

Among the items that can be subject to export control regulations are:

- Laptops, web-enabled cell phones and other mobile devices containing encryption hardware or software and/or other proprietary software. This includes personal travel if the traveler has UNK applications on a personal cell phone or personal mobile device.
- Other high tech equipment, such as advanced GPS units or scientific equipment.
- Controlled, proprietary or unpublished data in any format—print, electronic or verbal.
- Data and technology, blueprints, drawings and schematics.
- Chemicals and biological materials.

To explore various countries travel restrictions, visit
http://travel.state.gov/content/passports/english/alertswarnings.html

Presentations and discussions must be limited to topics that are not related to controlled items or technologies, unless that information is already published or otherwise in the public domain. Your technology or information must fall into one or more of the following categories prior to traveling: (1) Research that qualifies for the fundamental research exclusion, (2) Published information, (3) Publicly available software, (4) Educational information, or (5) Patent applications. Depending on your international destination(s), an export license or other government approval may be required for your laptop computer, software or other equipment. There are exceptions for "tools of trade," but these exceptions depend on the equipment and the country of your destination. Encryption software is subject to special regulations and more stringent license requirements.

Prepare your laptop before leaving the U.S. by removing anything that constitutes a trade secret, proprietary information, export-controlled information, or technical data. Rather than just delete files, you must use a "shredder" program to erase the information so that it cannot be recovered or recreated.

You may encrypt and then email to yourself any information you need while overseas. Retrieve the email only after reaching your destination and remove it completely before returning to the U.S. or before crossing any international border.

To maintain contact with work, family, and friends, most of us traveling abroad prefer to use mobile electronic communication devices. Mobile electronic devices such as laptops, cell phones, and tablets may be successfully attacked with malware and automated attack tools. These devices, even when kept current with security software, may not be able to thwart such an attack.

You can minimize the risk to data by taking specific actions before, during and after your trip.

*Before Traveling*

- Ask the Technology Helpdesk at Information Technology Services (308-865-8363 or unkhelpdesk@unk.edu) or your department for a loaner laptop or other device. Only have essential data on the device. Determine if the country has encryption import restrictions that prevent you from encrypting data on your device.
- Make sure the laptop or mobile device has a strong password. A strong password has upper case, lower case, numeric and special characters; is at least 10 characters in length; is not a word in any language; and is not based on personal information.
- Only take devices and media that are absolutely necessary.

- Copy your work files to UNK OneDrive network storage so they can be securely accessed when traveling. Do not copy files with personal, confidential, or non-public information to OneDrive.
- Do not save personal information, such as credit card numbers, passport information, or social security numbers, on your device.
- Clear the browsing history and any other stored information in web browsers that you would not want others to access.
- Check for sanctions or local laws that will affect your access. Some governments restrict access. For example, you cannot access Google Apps from Crimea as of 1/31/2015. Prepare for limited access and consider downloading materials to your device before traveling and think about how you will read and respond to email.
- You may have better access to email from your phone over a cellular network than from a computer connected to the Internet. Check with your phone carrier about international data plans before traveling. You can also get a local phone with a prepaid card in the country you visit.
- You may need a personal email account for communication but do not use it to share sensitive institutional data.
- Follow export control regulations, a body of federal law intended to prevent the transfer of sensitive items and technology to foreign nations, organizations and individuals. For more information, contact the Export Controls Officer.
- Tokens for two-factor authentication are subject to export controls and may not be transported or sent to embargoed nations as identified by the federal government. If you are traveling to an embargoed nation, delete or uninstall the software from your device and leave your hardware token at your campus office.
- Inventory the data that you are traveling with in case your device is lost or stolen.
- Back up data on your device(s) or media that you will take with you onto media that will not be taken on the trip.
- Run a full scan for malware with both anti-virus and anti-spyware tools.

*While Traveling*

- Always use a secure internet connection. Your cellular carrier's network is your best choice.
- Avoid using free wireless services. Assume that any computer network you use is insecure, and avoid business centers, cyber-cafés, libraries, or friends you stay with.
- Never accept software updates on hotel Internet connections or public Wi-Fi. Use the VPN. VPN access may be blocked from China and other locations. Do not attempt to illegally bypass the blocks.
- Never enter or access sensitive data using a shared or public computer.
- Turn off wireless and Bluetooth when not in use.

- Remember that governments in some countries can copy data from your computer and log your Internet activity without your knowledge or consent.
- Always use screen lockout when not using your device and require a password or code to unlock it.
- Keep your device with you and physically secured at all times. If possible, do not leave devices in hotel rooms, unless you can use a safe for storage of valuables. Do not use an obvious laptop storage bag that would make you a target.
- Use your web browser's private browsing feature.
- Turn off devices when not in use.
- Do not plug USB powered devices into public charging stations because malware can be transferred to your device or data downloaded from it. Use your own charging cable plugged into an electrical outlet.
- Do not accept USB drives or other removable media from any source.
- If your device is lost or stolen, notify UNK ITS for immediate assistance in changing passwords and contact local authorities to report the loss or theft.

*After Traveling*

- Change your UNK and NU passwords immediately after returning.
- Run a full scan for malware with both anti-virus and anti-spyware tools.
- Re-install your two-factor authentication token application.

**Additional Information**

**Laptop technology restrictions.** While mobile electronic devices such as laptops, cell phones, and tablets have become part of our day-to-day life, they can be successfully attacked with malware and other automated attack tools, even when kept current with updates and security software. Due to this vulnerability, when you travel to Cuba, Iran, N Korea, Sudan or Syria, you may only use a "clean laptop". A "clean" laptop is a device which has a new image installed, so you will probably want to borrow a "loaner laptop" for the duration of your travels. Other countries where a clean laptop would be recommended for export controls are the D-1 (national security level countries): Albania, Armenia, Azerbaijan, Belarus, Cambodia, China, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Libya, Macau, Moldova, Mongolia, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Vietnam.

**Availability of loaner laptops:** A loaner laptop or mobile device from the Technology Helpdesk at Information Technology Services (308-865-8363 or unkhelpdesk@unk.edu) may be available for travel to any of the above countries. Your department may have a loaner laptop available for travel, too. Tell the Technology Helpdesk or your Technology Coordinator that the loaner device is for international travel. If you do not plan to use a loaner device, ensure that all operating system security updates have been applied and current anti-virus, anti-spyware and

firewall software are installed. Any laptop or other mobile devices should also have a strong password applied.

**Encryption of devices.** Encryption laws vary from country to country. To determine your destination's current laws regarding cryptography, please visit http://www.cryptolaw.org/ for information specific to the country you are visiting. China, in particular, does not allow encrypted devices into their country. If legally permitted, you should consider encrypting the hard drive of your device. Contact the Technology Helpdesk at Information Technology Services (308-865-8363 or unhelpdesk@unk.edu) for further information.

3/18/2016

| | **Responsible** | **Summary of Change** |
|---|---|---|
| September 2015 | ITS Policy Team | Guidelines Developed in support of Export Control Policy |
| March 2016 | ITS Policy Team | Formatting updated. |