ITEMS FOR SUPPORT:

INTERNATIONAL TRAVEL

Several countries are considered to have higher risk associated with them for identity and data security than most other countries. The list of high-risk countries can be found on the State Department's website at: https://travel.state.gov.

Before the user leaves, you should work with them to determine if they are able to take a loaner laptop or if they have to take their work laptop. KSU Security and Access Management highly recommends that a loaner laptop be provided to the user to decrease/remove the risk of data loss and/or theft.

SETUP LOANER LAPTOP:

These items should be completed before it is given to the user. After the setup is complete have the user test the laptop from their home to make sure they can access their necessary files and resources.

- □ Verify that the loaner laptop is not bound to the Kent domain
- □ Create a local account for the user following Kent's password policies
- □ Install the KSU VPN or GlobalProtect (if the user needs GlobalProtect)
- □ Make sure the loaner does not have sensitive data on it
- □ Verify user still has access to all ***required*** resources they will need from off campus (optional)
- □ Record the serial number for the system
- □ Verify there are no export restrictions on the installed software
- □ If the department has a cellular modem "hot spot" try to get it assigned to the user

SETUP/CONFIGURING USER'S WORK LAPTOP:

If the user will be taking a loaner laptop this section can be skipped.

- □ Install IdentityFinder and search for sensitive data (work with Security)
- □ Backup any files to a Network file share (after scanning for sensitive data)
- □ Make sure a VPN is installed
- □ Make sure the system is fully patched for: OS, applications, browsers, browser plug-ins (i.e. flash)
  - ○ Browser Check: https://browsercheck.qualys.com/
  - ○ OS Updates
  - ○ Application Updates
  - ○ Have Security run an Authenticated Nessus scan on the computer (this could take 2-3 hours)
- □ Full Disk Encryption:
  - ○ Verify the device is encrypted
  - ○ Enable pre-boot authentication (BitLocker)

- □ Verify there are no export restrictions on installed software

WHEN RETURNING:

- □ Reimage the loaner laptop
- □ Assist user with changing their password
- □ Disable Pre-Boot authentication (optional)
- □ Consider re-imaging user's work laptop if they did not use a loaner laptop

ITEMS FOR USERS:

Several countries are considered to have higher risk associated with them for identity and data security than most other countries. The list of high-risk countries can be found on the State Department's website at: https://travel.state.gov.

The following is a list of suggested items that KSU Security and Access Management strongly encourages you to complete to help make your trip easier, but most importantly, safer for you and your data.

It is important that you complete as much of the checklist as possible, especially items that deal with your identity, student data, as well as your access to resources.

BEFORE YOU LEAVE:

- □ Review KSU's Travel Information: https://www.kent.edu/procurement/travel
- □ Review safety and travel checklists on https://travel.state.gov/content/travel/en/international-travel.html
- □ Consider enrolling in the Safe Traveler Enrollment Program: https://step.state.gov/step/
- □ Contact security and request an annotation placed on your account, be sure to indicate the country(ies) and dates of your trip
    - ○ Phone: (330) 672-5566 (on campus x25566)
- □ Test access to your computer from off campus using the installed VPN, this is critical if using a loaner laptop and remoting back to your desktop (optional if you do not use a desktop)
- □ Check with your department to see if they have cellular modem "hotspot"
- □ Verify your computer is encrypted
- □ If taking a tablet (i.e. Surface, iPad) ensure that the device is encrypted and a pin/password is configured to unlock the device
- □ Remove any and all sensitive data (SSN, Banner IDs,etc)
- □ Work with your local support to verify that all sensitive documents have been removed
- □ Work with your local support to back up your files
- □ Check with your department to see if you have a mobile hotspot that can be used while traveling, this allows you to avoid using any public hotspots

- □ Verify that there are no export restrictions for any software you taking with you (full disk encryption is permitted by US Law for most countries)
- □ Consider using a temporary “burner” phone while traveling
- □ Enable a pin/password on your phone if you are taking a personal device
- □ Inform your bank and credit card company that you will be traveling out of the US

WHILE YOU ARE TRAVELING:

- □ Do not use cell phone kiosk charging stations as there could be a computer on the other end used to copy your data and/or install malicious software
- □ Do not use public Wifi hot spots, if unavoidable, make sure to connect to the VPN
- □ Do not leave any of your electronic devices unattended
- □ Try to avoid using hotel safes as they are not considered secure for both high risk and low risk countries
- □ Do not allow anyone other than yourself to use your devices
- □ If your device is confiscated (not stolen) be sure to obtain written documentation that includes the following:
  - Name of the person taking the device, including their title
  - Why they are taking the device
  - If the device will be returned
  - Device serial number, make and model

WHEN RETURNING:

- □ Change your password from a different computer (not the one you took with you)
- □ Contact Security and Access Management to have your annotation removed
- □ Return loaner laptop (if provided)
- □ If your computer was taken from you and inspected when you arrived at the destination country:
  - Have the system re-imaged to remove any potential malicious software installed
  - Contact Security and Access Management
  - Change the password for any account that you had accessed while traveling