CYBER SECURITY

KENT STATE UNIVERSITY
Division of Information Technology

Several countries that 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.

Security & Access Management highly recommends that you encourage the user to contact our office to let us know that they are leaving the country and on which dates they are will be out. This will allow our office to make sure they retain seamless access to their account while traveling.

If there are any questions, concerns, or if you have recommendations on additional items for this or the user checklist please contact our office.

GENERAL:

- □ Suggest that they attend a Security Awareness Training
- □ Offer to help with setting up a pin/passcode on their personal phone
- □ When possible encourage the user to use a loaner laptop
- □ Go over how to do the following:
  - Disable wireless
  - Disable blutooth
  - Connect to the VPN on mobile devices
- □ What to do if any of their devices are lost or stolen
- □ Schedule a time to meet on the day they return to office

SETUP LOANER LAPTOP:

It is highly recommended that each support area that have users who often travel retain a few extra laptops for users to use as loaners. These systems should not contain any sensitive data and only the bare minimum of user data that is required should be copied to the loaner laptop.

Complete the following items before the laptop is given to the user for their use. 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 laptop/tablet is encrypted
- □ Verify that any and all tablets have a pin or password enabled

□ Install the KSU VPN or GlobalProtect (if the user needs GlobalProtect)

□ Make sure the loaner does not have sensitive data on it

  - ○ Install Run Spirion IdentityFinder

□ 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 (disk encryption is already approved)

□ If the department has a cellular modem "hot spot" try to get it assigned to the user

SETUP/CONFIGURING USER'S WORK LAPTOP:

Complete the following items if you are unable to provide or a loaner laptop or the user is required to take their daily use laptop with them.

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

□ Install Spirion IdentityFinder and search for sensitive data

  - ○ Notify Security so that they can work with you

□ Backup any files to a Network file share or using Druva inSync backup software (after scanning for sensitive data)

□ Make sure a VPN is installed

  - ○ Both the FortiClient and GlobalProtect can be installed on the same system

□ Make sure the system is fully patched for:

  - ○ 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 (FDE is permitted)

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