Guidelines for the Use of Portable Computing Devices
For Processing or Storing Export Restricted Data

The following guidelines pertain to only those portable electronic devices that are utilized to process and/or store export controlled restricted data and information. Export restricted data and information in this instance is any data or information that is controlled under the Export Administration Regulations, International Traffic and Arms Regulations, Office of Foreign Assets Controls or any other U.S. law or regulation that prohibits the export of data and information.

The security of portable electronic devices is very problematic because of their nature – they are portable and can be taken anywhere. When the processing or storing of export controlled information is added to a portable electronic device the issue of security becomes magnified. The issue is even more serious when the device is used to store export controlled data on a portable device.

In cases where portable computing devices are utilized to process or store restricted data, information or technology the following guidelines shall apply:

- All mobile computing devices for use with restricted data and information will be university owned and maintained devices.
- The following items shall be installed, correct operation verified and certified to the Office of Research Security via an e-mail notification by a university IT department.
  - All IT personnel that have any type of support privileges for the mobile computing devices, i.e. SysAdmin capability/passwords, etc. must be U.S. persons as defined by the ITAR §120.15 definition (ITAR 22 CFR Chapter I, Subchapter M, Part 120 – 130) and also must adhere to export control policy of the university for training and awareness.
  - The data, information or technology must be stored on a single-user portable device in a volume that utilizes strong encryption (e.g. AES-256 or equivalent) protection, with a unique decryption passphrase known only to the device’s authorized primary user. SysAdmin will establish and maintain an “escrow” account with a separate decryption password/passphrase in the event of a loss or malfunction of the primary decryption password/passphrase.
  - When the mobile computing device is no longer required for use in support of restricted data, information or technology processing or storage the unit shall have its memory capability overwritten. In the case of a laptop, a program such as Wipe Drive Pro shall be used and the memory overwritten at least 3 times.
The mobile device, if it is a laptop computer, must be protected by a university approved software firewall.

The mobile device must be accessed using a login account with a password of no less than eight (8) characters in length, a mixture of upper and lower-case letters, numbers and symbols. The password shall be subject to change on a no less than annual basis or when the possibility of password exposure is suspected.

Any transmission of restricted data, information or technology containing restricted data, shall be encrypted and utilize a secure method of transmission, i.e. VPN, SSH, etc.

Inbound remote login to any mobile computer device containing restricted data, information for technology is prohibited; only approved SysAdmin performed functions are allowed.

If data backup is required, all restricted data and information must remain encrypted.

All mobile computing devices that are utilized for restricted data, information or technology will have a conspicuous label denoting this fact so the device can protected accordingly. (ITAR labels are available thru the Office of Research Security)

When not in use by the authorized primary user, the mobile computing device will utilize the one-lock methodology. One lock methodology is where there is at least one type of lock mechanism between the device and being in the open.

Foreign travel with a portable computing device that contains export controlled data or information is not permitted no matter what protections are installed on the device. Taking export controlled material out of the United States is considered an export and is a violation of export control laws and regulations. Even travel within the U.S. with a portable computing device that contains export controlled information can present risks to the traveler.