Travel Alert

Department of Homeland Security announces new security protocols

Wednesday, March 21, 2017 – The Department of Homeland Security has announced new security protocols impacting the transport and use of personal and Vanderbilt issued technology. If a traveler's itinerary includes direct travel from, or a transfer through, these 10 airports to the United States:

- Queen Alia International Airport (**AMM**) - Jordan
- Cairo International Airport (**CAI**) – Egypt
- Ataturk International Airport (**IST**) – Turkey
- King Abdul-Aziz International Airport (**JED**) – Saudi Arabia
- King Khalid International Airport (**RUH**) – Saudi Arabia
- Kuwait International Airport (**KWI**)
- Mohammed V Airport (**CMN**) – Morocco
- Hamad International Airport (**DOH**) – Qatar
- Dubai International Airport (**DXB**) - United Arab Emirates
- Abu Dhabi International Airport (**AUH**) - United Arab Emirates

The new protocol states: *ALL electronic devices larger than a cell phone, excluding necessary medical devices, can no longer be carried aboard in carry-on items. They must be secured in checked luggage.* For more information, please see the Department of Homeland Security fact sheet and Q&A. Items affected:

- Laptops
- Tablets
- E-Readers
- Cameras
- Portable DVD players
- Electronic game units larger than a smartphone
- Travel printers/scanners

There is no impact on domestic flights in the United States or flights departing the United States. Electronic devices will continue to be allowed on all flights originating in the United States.

Travelers should keep updated on restrictions. In addition, based on security guidance there are similar restrictions for air transport routing through United Kingdom airports originating from Turkey, Lebanon, Jordan, Egypt, Tunisia and Saudi Arabia. Egypt has similar requirements on direct flights from the U.S. to Egypt.

Individuals traveling with university owned devices or university data on personal devices are advised to:

- Consider if electronic devices are necessary for their travel, and leave unnecessary devices behind
- Remove all sensitive data and proprietary information from devices that is not pertinent to their travel
- Encrypt devices, especially if you must take sensitive or proprietary data
- Choose strict passwords for devices and online accounts
- Back-up all data
- Enable remote wiping capabilities, in case your device is lost or stolen
- Ensure that your devices remain fully charged in case you are required to enable it for inspection
- Have the device scanned by their department's IT staff or VUIT upon return to detect and remove any malicious spyware

Those individuals traveling with electronic devices that must be stored as checked luggage are advised to plan for safe storage of their devices, including the use of TSA recognized locks for their checked baggage.