FLORIDA	OFFICIAL
POLYTECHNIC	UNIVERSITY
UNIVERSITY	POLICY

Subject/Title: Use of IT Resources When Traveling Abroad
FPU Policy Number: FPU-11.0014P
_X_ New Policy __ Major Revision of Policy __ Minor Technical Revision of Policy
Date First Adopted: September 23, 2015
Date Revised:
Responsible Division/Department: Information Technology Services
Initiating Authority: Tom Hull, Vice President and Chief Information Officer

A. APPLICABILITY/ACCOUNTABILITY: This policy applies to all University employees who plan to travel internationally and use University IT Resources (the University Network, technology and telecommunication resources, computing devices, or software including but not limited to computers, laptops, smart phones or other computing devices).

B. POLICY STATEMENT: University employees are expected to exercise due diligence when using University IT Resources while traveling internationally. Employees must comply with University policies to keep University data and IT resources secure. International travel places devices at increased risk of loss or theft and the data on the device may be at risk from networks managed by entities that monitor and capture network traffic for competitive or malicious purposes.

1. Accessing the Internet. Employees should avoid contact with the University network while traveling internationally, especially when traveling to high risk countries on the list located at: http://travel.state.gov/content/passports/english/alertswarnings.html/. By avoiding contact with the University network, employees reduce the risk of the ID and password to Florida Poly being captured and used to compromise Florida Poly systems and to reduce the risk of having data stolen or compromised.

   If an employee must access the University network while traveling internationally, the employee should employ their own device or a University loaner device, not a public work station. Employees should not use public workstations while accessing the University network because all entries (passwords, user ids, and data) can be captured and used. Employees should be aware of the surroundings when logging in/using devices and not allow someone to see the password and user name when typing. Some foreign governments in high risk countries monitor electronic communications over the Internet so email is not secure nor is email private.

   Employees must employ secure connections for computing and connecting to the University network via a remote connection method (VPN via a telephone dial-up or broadband Internet connection) so the connection does not compromise the security of the systems being used. Employees also must employ physical protection, access controls, cryptographic techniques when necessary, back-ups, and virus protection. Employees who travel outside the U.S. must change passwords upon return.

2. Limit sensitive information on computing devices when traveling internationally. Employees should limit the amount of sensitive information that is stored on or accessible to any mobile device taken on a trip. Employees should assess the sensitivity of the information taken on an international trip, and determine if it is sensitive, confidential, or proprietary, subject to import or export data control regulations or could be considered a trade secret. Data that should be left on campus or afforded exceptional protection includes information that might be considered sensitive by the host government when traveling internationally. If practical, Employees should contact IT via the Helpdesk@flpoly.org or by calling (863) 874-8888 at least thirty (30) days before traveling internationally and discuss the use of a loaner device (laptop or tablet). Before connecting to the University network upon returning from an international trip, contact IT to erase and wipe the hard drive and other components that store data. IT can help restore software to a trusted version. Employees should also consider renting a cellular telephone for use during an international trip to avoid having the Employee's smart phone become a back door into the University system.

3. Protecting devices from theft. Mobile devices and equipment carrying important, sensitive, and/or critical business information must not be left unattended and, where possible, must be physically locked away, or special locks must be used to secure the equipment. Mobile computing devices should be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers, and meeting places. Employees shall employ an auto-lock on the mobile device and use a complex password. Remote wipe, tracing and tracking software shall be used if available. Employees should back up data regularly if stored on mobile device. Employees must use inactivity timeouts of a reasonably short duration of fifteen (15) minutes or less. Employees must notify the University by contacting the Helpdesk by calling (863) 874-8888 or emailing Helpdesk@flpoly.org as soon as possible in the event of theft or data compromise.

4. Remote access to University email and data files during international travel. Employees should contact the Helpdesk and request an alternate email for use during an international trip. Access the email through an external email account. IT will delete the temporary account at the end of your trip. Employees should avoid using Remote Desktop or equivalent software to access an Employee's University desktop or other device from a high risk country as these transmissions may expose valuable information. Instead, Employees can access data during international travel by using an external storage service (e.g., Google drive). Employees can have a colleague add files to the Employee's external network drive in case a file was forgotten during preparations.

5. Know hardware and software travel restrictions (import and export controls). Employees are responsible for knowing import and export restrictions on hardware and software. Some countries have import controls that restrict the transport into the country of encrypted devices, hardware and software. The U.S. has export controls in the form of regulations restricting the transport of certain types of hardware and software to certain countries. Please contact the Contracts & Grants Manager if you have any questions.

6. Consequences of violating policy. Employees who violate this policy may be subject to disciplinary action up to and including termination.

POLICY APPROVAL	
Policy No. FPU-11.0014P	
Initiating Authority	Date 9/23/15
Policies & Procedures Review Committee Chair	Date 9-15-15
President/Designee	Date 9/20/15
Approved by FPU BOT, if required	Date

082015