CONNECTICUT COLLEGE

ENTERPRISE AND TECHNICAL SYSTEMS

What can I do to protect my electronic devices and my personal information when I am traveling abroad?

The guidelines and recommendations listed below outline and define steps you can take to protect your information, your electronic devices and your college-owned laptop when traveling outside the United States. They have been developed in concert with the College's Chief Information Security Officer based on best practice as is currently known.

- If possible, do not take your College or personal devices with you. Use a temporary device, such as an inexpensive laptop and/or a prepaid "throw-away" cell phone purchased specifically for travel.
- If you must take your College or personal electronic device(s) with you, delete all data and information except what you will need for your travel. Be sure to backup your device before removing any information.
- Be sure that any device with an operating system and software is fully patched and up-to-date with all College recommended security software.
- When not in use, turn off the device(s). Do allow them to be in "sleep" or "hibernation" mode when they are not in active use.
- Be sure to password or passcode protect the device. Do not use the same passwords/passcodes that you use on your College and personal devices. The password/passcode should be long and complex. Here are some examples of passwords that would follow the necessary criteria: Suce$$ful 2S!ncere Etc&etc Came12oo4
- Minimize the data contained on the device. This is particularly true of logins and passwords, credit card information, your social security number, passport number, etc.
- Assume that anything you do on the device, particularly over the Internet, will be intercepted. In some cases, encrypted data may be decrypted.
- Never use shared computers in cyber cafes, public areas, hotel business centers, or devices belonging to other travelers, colleagues, or friends.
- Keep the device(s) with you at all times during your travel. Do not assume they will be safe in your hotel room or in a hotel safe. Do not transport your device in checked luggage.

CONNECTICUT COLLEGE

ENTERPRISE AND TECHNICAL SYSTEMS

- Upon returning from your travels, if you're using a temporary device, immediately discontinue use of the device(s). The hard drive of the devices should be reformatted, and the operating system and other related software reinstalled; or dispose of the device properly.
- Change any and all passwords you may have used abroad.
- We recommend that you encrypt your device in case it is stolen, however, be aware that use of encryption may be forbidden in some countries. The College does utilize whole disk encryption to protect personally identifiable information (PII) on laptops, some countries (such as China and the Russian Federation) do not allow importation/ exportation of encrypted devices. While some whole disk encryption products, such as TrueCrypt, allow you to attempt to conceal encrypted disk partitions, attempts at hiding encrypted disk partitions may nonetheless be detected, and lying in response to border official questioning about the existence of encrypted disk partitions may be a potentially serious criminal offense.
- It is NOT recommended that you transport your laptop in checked luggage unless you are forced to do so. Regulations vary depending on the country you travel to. You may be able to exit the country without checking your laptop, but you may not be able to return with it.
- If you are forced to check your laptop in luggage it is recommended that you wrap the laptop or mobile device in bubble wrap. Make sure the device is powered off or shutdown, not in sleep mode as it could overheat. As an extra precaution attach a security cable to your laptop and wrap the cable around the bars that the suitcase handle slides into inside of your suitcase. You can purchase a security cable here: http://www.computersecurity.com/laptop/csp625_b.htm

July 5, 2017