UNIVERSITY OF
SOUTH CAROLINA
College of Hospitality, Retail
and Sport Management

NUMBER: 1.00

SECTION: Information Technology

SUBJECT: Acceptable Use of Information Technology Resources While Travelling

DATE: November 20, 2015

REVISED: May 15, 2017

Policy for: All College of HRSM faculty, staff, adjuncts, and students
Procedure for: All College of HRSM faculty, staff, adjuncts, and students
Authorized by: Haemoon Oh
Issued by: HRSM ITS

Unauthorized attempts to access sensitive institutional data are growing in sophistication, especially during foreign travel. The College of Hospitality, Retail, and Sport Management (HRSM) acknowledges that its data and information are vital and valuable assets and is committed to establishing programs that ensure the appropriate use, availability, and risk mitigation for data and information assets. To protect its users and data while traveling, the College of HRSM has designed a travel procedure for all faculty, staff, adjuncts, and students (Users). The procedure applies when traveling with college-issued resources, including but not limited to laptops, mobile devices, and storage media. For more on Information Security responsibilities, refer to university policies IT 3.00 (Information Security), IT 1.06 (Acceptable Use), UNIV 1.51 (Data Governance), UNIV 1.52 (Responsible Use).

Procedure

Before you go:

1. Contact HRSM ITS to discuss your IT needs during your trip. This will reduce issues you could experience abroad.
2. Check out a preconfigured laptop. This eliminates potential downtime upon your return. (If you check out a laptop, skip to the next section, *During your stay*.)
3. If you must travel with your college-issued resource(s), back up your data to media that is not traveling with you, and remove any data not necessary for your trip.

During your stay:

4. Enable the university's VPN when connecting to wired or wireless networks.
5. Only use your device to access personal or university resources.
6. Keep your device with you at all times.
7. Avoid connecting foreign media to your device.

When you return:

8. If you checked out a device, return it to HRSM ITS.
9. Change your passwords to accounts accessed while abroad.

PLEASE NOTE: If administrative rights are required to make changes to the resource for any reason before or during the trip, it will be considered compromised. Once compromised, HRSM ITS must disable its access to domain resources. Before re-enabling access, it must be securely wiped and reformatted. Understand that HRSM ITS can not save any data, configuration, or software, as this negates the integrity of the security process.