International travel has unique risks and challenges when compared with domestic travel. In consultation with ISC’s Security Group, College Hall Support has established this security primer for clients travelling internationally. For all clients, we promote the following 5 baseline strategies:

1) **Talk to College Hall Support in advance of your trip.**

Plan on meeting with College Hall Support well in advance of your trip to discuss details, timeframes, and best-practices. We understand that each of our clients has different requirements, and can work with you to provide a set of customized security recommendations before you travel. Be cognizant of export control restrictions and discuss these with College Hall Support and the Office of Research Services. For example, use of encryption is illegal in Cuba, Iran, North Korea, Libya, Sudan and Syria.

2) **Take advantage of loaner devices (i.e. laptop, tablet, and mobile) when possible.**

This is perhaps the single most effective step that you can take to enhance your security. The devices we use every day can contain extremely sensitive data – including local documents, images, pictures, and user history - that is not relevant for your trip. A loaner device starts in a clean state, is pre-configured by College Hall Support with appropriate security measures, and only has the information that you introduce in support of your trip. Upon your return, a loaner device can also easily be erased, mitigating any risks of advanced persistent threats introduced to the system during your trip. Be sure to take advantage of College Hall Support’s Technology Loan Program (TLP).

3) **Leverage secure cloud services (Penn+Box) over local data.**

Systems in foreign countries are vulnerable to localized security failures, whether they are physical (i.e. someone steals your laptop) or virtual (i.e. someone “hacks” your laptop). The safest way to work is to not have any local data on your system at all. Leveraging cloud resources means you limit your exposure to localized failures because there is no data on your local system.

Specifically, web-based access to Penn+Box uses high-grade SSL encryption in transit and 256-bit AES encryption at rest. If you’re using a College Hall Support loaner device, not only is the device itself encrypted (using either Microsoft BitLocker, Apple Filevault, or mobile technology), but all network communication is encrypted using ISC’s Secure Remote Access (Junos Pulse) VPN solution.

4) **If you don’t need it and you can’t lose it, don’t use it.**

The safest data is no data. Data that you don’t bring with you and don’t have access to has virtually no chance of being exposed to cyber-theft. Take stock of the bare minimum of what you’ll need before you travel, and only access these resources. Don’t check your bank account, access your personal e-mail, or log into your favorite recipe site if you don’t need to.

5) **When you return, contact College Hall Support to scan and wipe systems, and to cycle passwords to any sensitive credentials.**

Take the stance that anything you use while abroad can return compromised. When you return, work with College Hall Support to wipe any borrowed systems, cycling any passwords you used (and limit these via step 4!), and scan systems to discover any introduced threats.