STEVENS
INSTITUTE OF TECHNOLOGY

Traveling to High-Risk Cybersecurity & Privacy Countries

Stevens data is important, and international travel can expose it to new security concerns, such as different regulations, networks, and technology, as well as cybercriminals. To minimize the security threats and risks posed by international travel on Stevens data, we recommend the following:

- Be cognizant of where you travel. Certain countries may pose higher risks to your data and implementing security recommendations are critical: Afghanistan Algeria, Belarus, Burma/Myanmar, Cambodia, Central African Republic, China, Cyprus, Egypt, Eritrea, Ethiopia, Guinea, Hong Kong, Iraq, Liberia, Libya, Niger, Sierra Leone, Somalia, South Sudan, Sudan, Taiwan, Venezuela, and Yemen
- In addition, no Stevens devices are permitted in the following countries: Cuba, Iran, North Korea, Russia, Syria, Ukraine/Crimea and the Donbas Regions
- Carry minimal data and store data on the cloud. Never carry sensitive data like PII or research data while traveling.
- Ensure that your data, devices, and backups are fully encrypted.
- Use a loaner device if possible.
- Avoid using public WIFI unless for non-essential work
- When public WIFI is unavoidable, utilize a Virtual Private Network (VPN) to secure the connection and minimize the risk. Even with VPN, avoid any sensitive work.
- Okta Verify will continue to work for MFA authentication if connected to WIFI. However, Stevens can provide Yuibikeys as requested if avoiding foreign networks is necessary.
- If your device is stolen, immediately report it to both Stevens and local authorities.
- Contact security@stevens.edu for more information.