INTERNATIONAL TRAVEL INFORMATION SECURITY

Guideline WyIT-3024-G

Prior to Departure

- Complete a pre-travel briefing with members of the Wyoming Information Analysis Team (WIAT). Arrangements for this briefing will be made through the Wyoming Office of Homeland Security (WOHS).
- Identify electronic equipment needed – If the device is not essential, Do Not Take It!
    - Use a "clean" laptop, phone and new email account while traveling.
    - Sanitize all devices. Cell phones can be hacked to steal contact lists, usernames, passwords, and browser history. Contact the service desk to aid in backing up and the subsequent purging/wiping of all data on the devices or substitute another piece of equipment that does not contain data.
    - Remove apps requiring user accounts and passwords that are not necessary.
    - Identify any data, internet access, or cloud access needed. Assume all information accessed while traveling will be compromised.
    - Make an inventory of all devices that will be taken on the trip, including serial number, make, and model. Store it in a safe place with other key information (1 copy at home and 1 with you).
    - Identify any accessories needed; cables, power adaptors and converters. Accessories are routinely swapped for those with surveillance capabilities.
    - Leave Bluetooth earpieces and keyboards at home and turn off devices' Bluetooth function, which can enable eavesdropping.
    - Lock devices with a PIN or strong password (a combination of upper and lowercase letters, numbers and symbols at least 14 characters in length).
    - Utilize whole disk encryption to protect stored data.
    - Disable file sharing on computers.

- Avoid using your laptop/computer to charge any additional external devices while traveling (i.e. phone, camera, etc.)
- Patch, update and secure device (antivirus, antispyware, firewalls, encryption, VPN)
- Tape over or disable any integrated camera and disable integrated microphones.
- Review any guidelines or laws related to electronics for the country visiting and verify all websites/cloud services needed can be accessed while traveling
- Create temporary accounts with strong passwords and do not use any of the passwords tied to current US accounts, including voice mail passwords.
- For international travel information and alerts, visit these Department of State websites:
  - https://travel.state.gov/content/travel/en/international-travel.html
    http://travel.state.gov/content/passports/en/alertswarnings.html
- For cybersecurity tips for traveling overseas with mobile phones, laptops, PDAs, and other electronic devices, visit the Director of National Intelligence website:
  - https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-travel-tips

- Leave unneeded car keys, house keys, smart cards, credit cards, swipe cards, and access control devices at home.

During Travel

- Always carry electronics in carry-on luggage and always keep them in your possession.
- Always keep devices in sight and be aware of surroundings. Consider the use of a privacy screen to prevent shoulder surfing.
- Turn off geolocation services.
- Set email to retrieve manually and only download necessary email on trusted connections.
- Use a Virtual Private Network (VPN) when on the Internet.
- Never use public Wi-Fi, cyber cafés, or other people's devices to access information electronically.
- Do not allow other people's electronic storage devices to connect to your device and do not connect to their devices.
- Do not use any USB drives given to you.
- Do not post to social media.
- Accept that any information accessed will be exposed.
- Turn off devices when not in use.
- Respectfully but firmly decline to let customs officers take devices to another room to inspect them without you.

- Report any lost or stolen equipment immediately to the service desk and US Embassy or Consulate.
- Beware of phishing or other social engineering attempts.

Upon Return

- Scan all data for viruses prior to copying it to another device.
- Wipe or format any electronic equipment immediately (treat as a compromised device).
- Consider destroying and replacing all SIM cards, depending on where you have traveled.
- Change all passwords used during travel and delete any temporary accounts used.
- Clear temporary internet files.
- Beware of any unexpected contacts from foreigners after your return.
- Complete a post-travel briefing with members of the WIAT. Arrangements for the briefing can be made through the Wyoming Office of Homeland Security.

REFERENCES:

WyIT-3024 INTERNATIONAL TRAVEL INFORMATION SECURITY Policy