RUTGERS UNIVERSITY
Office for Research

This checklist is intended primarily for the Principal Investigator and members of the research community traveling internationally with research data or devices. This aims to provide practical guidance to help reduce research security and cybersecurity risks during international travel.

Researchers traveling to Foreign Countries of Concern (FCOC) — China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, Venezuela— should especially review all sections of this checklist.

This guidance does not replace Rutgers University policy or sponsor requirements.

Research Regulatory Affairs FCOC Departure Checklist for Researchers and Investigators

Checklist for Researchers and Investigators
Before You Travel: Research & Risk Review
☐ Review destination-specific cybersecurity and geopolitical risks by reviewing current information on the Department of State website. If your travel has additional risk, please contact Rutgers Global, Research Security, Export Control, your local IT department, and the Office of Information Technology (OIT) Security
☐ Always register your trip with the U.S. government's Smart Traveler Enrollment Program to get destination-specific alerts
☐ Confirm whether VPNs or encryption are restricted in the destination country (click here for more information)
☐ Countries with **Total VPN ban:** North Korea, Belarus, Iraq, Turkmenistan
☐ Countries with **Heavy VPN ban:** China, Russia, Iran
Note: Travelers to Hong Kong and Macau should be aware that authorities may require **access to personal devices and passwords** under their National Security Law
☐ Countries with **Moderate VPN ban:** India, Turkey, United Arab Emirates
☐ Identify whether your research involves:
☐ Controlled Unclassified Information (CUI) ☐ Personally Identifiable Information (PII) ☐ Human subjects' data ☐ Export-controlled or proprietary information ☐ Classified or Sensitive Information
☐ Check with your Department IT office whether a clean device (laptop or phone) is recommended or if a loaner can be provided.
Before You Travel: Secure Your Devices
☐ If bringing Rutgers-owned or personal devices with Rutgers data, make sure to remove non-essential and sensitive research data (i.e., any datasets, draft analysis, presentations, manuscripts, survey results, etc.) that you do not need while traveling. If you need the data, please consult with your local IT department on how best to protect it (i.e., bringing the data on a CD or thumb drive in lieu of bringing your device).
☐ Back up data to Rutgers-approved cloud storage or external media (leave backup at home)
☐ Install the latest operating system and security updates with your local IT
☐ Enable full-disk encryption (where permitted)
☐ Enable strong passwords or PINs (6+ characters) and multi-factor authentication (DUO)
☐ Remove saved Wi-Fi networks and Bluetooth connections

☐	Uninstall non-essential applications (e.g., social media, networking apps)
☐	Install Rutgers-approved VPN software and obtain login information (where permitted*)
☐	Install end-to-end encrypted messaging applications (where permitted*)
While Traveling: Cybersecurity Best Practices	
☐	Assume devices and communications may be monitored
☐	Never leave devices unattended (ex. in hotel rooms)
☐	Bring your own cables, chargers, and adapters; avoid public USB charging stations and unknown cables
☐	Use institutional VPN when accessing the internet (where permitted*)
☐	Do not access or download sensitive or controlled data
☐	Disable Wi-Fi, Bluetooth, GPS, AirDrop, and NFC when not in use
☐	Avoid scanning QR codes; type website URLs directly
☐	Use private ("incognito") browsing when possible
☐	Power-cycle devices daily (e.g., power off, unplug, wait 30 seconds, plug in, power on)
If Something Goes Wrong	
☐	Immediately report lost, stolen, confiscated, or temporarily taken devices to your contact from your local IT department and OIT-Secuirty
☐	Report signs of device compromise (unexpected battery drain, performance issues, unfamiliar software behavior)
☐	Contact your local IT Department and Research Security for guidance
When You Return	
☐	Contact your Department IT before reconnecting to the Rutgers network if device compromise is suspected
☐	Power-cycle devices before reconnecting to any network
☐	Restore devices from a clean backup or wipe devices if advised
☐	Change all passwords used during travel
Need More Information?	
☐	Please contact Rutgers Global, your local IT department, Export Control, and the Research Security Department with any additional questions you may have
☐	Rutgers Research Regulatory Affairs would like to thank NSF SECURE for the Basic and High Risk Travel checklist