Title:	Policy Category:
Policy on Data and Devices for International Travel	**Risk Management & Security**
Issuing Authority: **Office for Research and Innovation**	**Responsibility:** **Information Technology &** **Office for Research and Innovation**
Publication Date: **07/24/2025**	**Next Review Date:** **07/24/2028**

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

Policy Statement/Background:

Stony Brook University ("University") is committed to protecting the confidentiality of University records and information, including University Data (defined below) proprietary information, sensitive research data, and intellectual property of the University, its faculty, and staff. Travel with electronic devices to destinations presenting heightened theft and cybersecurity risks ("High Risk Countries") increases the potential for such sensitive information to be procured from computers and mobile devices (collectively, "devices") without the owner's knowledge or consent, and for devices and/or the University's network to be infected from malware or spyware, and therefore requires special precautions.

This policy provides requirements and guidance about the transport and use of University Data and devices when traveling to any international destination. In addition, this policy provides additional requirements and guidance for travel to High Risk Countries.

Policy:

Any international travel with electronic devices presents risks of hardware and University Data theft, as well as increased risk of infection from malware. This includes travel to destinations that are not deemed to present heightened cybersecurity risk and for travel with personally-owned devices used for University business. Sensitive Information (as defined in the University's Sensitive Information Classification Policy) must be stored on encrypted devices when traveling internationally.

Traveling internationally with laptops, tablets, smartphones, storage devices, or other electronic devices requires special considerations to reduce the risk of theft of devices and/or University Data, and, in some cases, may require an export license (see more about export control requirements). The likelihood of University Data loss is greatest when traveling internationally and especially high in countries where governments operate and manage the Internet. Moreover, several countries restrict the import of encrypted devices and software, or require a license to bring encryption software/devices into the country.

To protect travelers' and the University's interests, faculty, staff, and students traveling to *any* international destination should closely follow published IT Security Considerations While Traveling, International Transfers: Shipments, Hand-Carry and Electronic Transmissions, and recommendations made within Enterprise Risk Management's (ERM) pre-travel safety briefing.

Additionally, when traveling to High Risk Countries as defined in this policy, University faculty and staff:

- must not take their University laptops, tablets, mobile devices or any device containing Sensitive Information with them.
- must not take personally owned laptops, tablets, mobile devices or any device (1) containing Sensitive Information or (2) connected to SBU resources with them.

Laptop Loaner Program for Travel to High Risk Countries

To assist travelers in complying with this policy, the University has an International Travel Loaner Laptop Program for travelers who need access to University Data or services while traveling to High Risk Countries. Travelers to High Risk Countries seeking to use a loaner laptop should contact the Office of Research Security (ovpr_researchsecurity_admin@stonybrook.edu) as soon as possible.

Compliance

Failure to comply with this policy and guidance may result in discipline, up to and including termination. Under export control and other federal laws relating to data protection, violations might also subject the violator to criminal or civil prosecution.

Definitions:

High Risk Countries: include Countries of Concern, countries with broad sanctions and embargoes by the Department of the Treasury Office of Foreign Asset Control (OFAC) embargoed/sanctioned countries, and other countries that are identified by the U.S. government as a heightened cybersecurity risk. The Office of Research Security maintains this list, which currently includes:

China, The People's Republic of
Cuba

Hong Kong
Iran
North Korea
Russia
Sudan
Syria
Ukraine - Crimea, Donetsk and Luhansk regions

Loaner Laptop: refers to university-owned devices available to faculty and staff for travel to High Risk Countries.

Encryption: means the software program or process for protecting sensitive digital information by converting data to an unrecognizable or encoded form to make it unreadable by unauthorized users.

Sensitive Information: is data classified in the Sensitive Information Classification Policy (see link below) as either Category 2 or Category 3.

University Data: information collected or created through a function of the University.

Contact:

Additional information about this policy is available here:

Susan Gasparo
Director of Research Security
(631) 632-1954
Susan.Gasparo@stonybrook.edu

Relevant Standards, Codes, Rules, Regulations, Statutes and Policies:

- University Travel Policy
- Export Control Policy
- Policy on International Engagements
- Responsible Use of Information Technology Resources Policy
- Sensitive Information Classification Policy
- Policy on Data and Data Access
- Research Data Ownership, Retention and Access Policy