Northeastern University

INFORMATION TECHNOLOGY SERVICES

Effective Date: February 28, 2020

Date Revised:

Supersedes: N/A

Related Policies:

Policy on International Travel
Policy on Mobile Devices
Policy on Export Control
Policy on Appropriate Use of Computer and Network Resources
Policy on Confidentiality of University Records and Information

Responsible Office/Department:

Office of the Provost

Office of the General Counsel

Office of Information Security

Keywords: Information security, Intellectual property, cybersecurity risk, international travel, university-issued devices

Policy on Computers and Mobile Devices for Travel to Destinations with Heightened Cybersecurity Risk

I. Purpose and Scope

Northeastern University is committed to protecting the confidentiality of university records and information, including 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 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 electronic devices when traveling to such destinations, and the program for loaner devices whiletraveling on university business. It applies to all faculty and staff on university-sponsored travel, as defined in the Policy on International Travel, to any destination presenting heightened cybersecurity risk and to any sanctioned or embargoed country or region, as defined below.

II. Definitions

For purposes of this policy,

Destinations with Heightened Cybersecurity Risk refers to destinations that present an enhanced degree of cybersecurity risk, often because of government control of the internet and/or threats to cellular networks, that are identified by Northeastern on a "High Cyber Risk" list maintained on the international travel webpage as updated/revised from time to time.

Sanctioned countries refers to those countries subject to targeted trade or economic sanctions under U.S. export controls regulations which prohibit certain exports of items, data and/or software without a license authorization.

See https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

Embargoed countries refers to those countries or territories subject to embargo under U.S. regulations (Crimea, Cuba, Iran, North Korea, Sudan, and Syria) prohibiting all transactions (including imports and exports) without a license authorization. See https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

Confidential Records includes without limitation any personally-identifiable student and parent records, financial records (including social security and credit card numbers), and health records; contracts; research data; alumni and donor records; personnel records other than an individual's own personnel record; university financial data; computer passwords, university proprietary information and data; intellectual property; and any other information for which access, use, or disclosure is not authorized by any applicable law, privacy regulations, or university policy.

Loaner Device refers to university-owned devices available to faculty and staff for university-sponsored travel to destinations identified as presenting heightened cybersecurity risk.

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.

III. Policy

Traveling internationally with laptops, tablets, smart phones, storage devices or other electronic devices involves special considerations to reduce risk of theft of devices and/or data, and in some cases may require an export license. The likelihood of data loss is greatest when traveling internationally and especially high in countries where the government operates and manages 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 (e.g., China, Iran, Israel, Russia, Saudi Arabia, and others – check with the Director of Research Integrity and Export Controls, exportcontrols@northeastern.edu).

Accordingly, to protect travelers' and the university's interests, and to reduce the risk of theft, hacking, and/or loss of personal data or university confidential records, faculty and staff traveling to any destination with heightened cybersecurity risk, or to any sanctioned or embargoed country, as defined in this policy, must follow the requirements below as well as those set forth in Northeastern's Technology Guidelines for Travel in or Through Destinations with Heightened Cybersecurity Risk ("Guidelines").

University employees should not take their own university-issued or provided laptops, tablets or mobile devices when traveling to destinations with heightened cybersecurity risk,

or to sanctioned or embargoed countries. If such devices are needed for university-sponsored travel, then at least two weeks before the departure date employees must submit a request form (link) to the IT Service Desk to obtain a university-owned Loaner Device (e.g., laptop, tablet, or mobile phone) to use during travel. Once received, no intellectual property or confidential information should be downloaded to any Loaner Device. Loaner Devices will be configured with a limited package of software to provide access to email and the internet. Users are not permitted to modify system settings or install additional software and should not load any files or data on to these devices. During travel, users must follow the Guidelines for accessing cloud storage and the university's VPN.

Within two business days of returning to the university, the traveler should return the Loaner Device(s) to the IT Service Desk where it will be wiped, re-formatted, and re-imaged.

Subect to available inventory, travelers on short-term personal travel to destinations with heightened cybersecurity risk may be able to obtain loaner devices.

IV. Additional Information

Any travel, international or domestic, with electronic devices presents risks of hardware and data theft, as well as increased risk of infection from malware. Even for travel to destinations that are not deemed to present heightened cybersecurity risk, and for travel anywhere with personally-owned devices, no confidential university records or data may be stored on unencrypted devices.

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

Travel to embargoed countries/areas of Cuba, Iran, North Korea, Sudan, Syria or Crimea requires a license and approval through the Global Security and Safety Assessment Committee (GSSAC) and/or the Director of Research Integrity and Export Controls. You should not travel with or access any export-controlled data to, from or within these countries.

V. Contact Information

Office of the Provost: 617-373-2170
Office of Information Security: OIS@northeastern.edu
Director of Research Integrity and Export Controls: exportcontrol@northeastern.edu
International Security Office: mytravelplans@northeastern.edu