# International Travel Guidelines

## Introduction

The landscape for international travel has changed significantly and become more highly regulated with greater potential institutional risk. This guidance aims to assist travelers in understanding developing changes, clarify existing guidelines on international travel, and provide new guidance for use of all university systems and institutional technology while overseas.

We understand that these interim measures may cause inconvenience and disruption for some travelers, but it is essential to comply with applicable laws, federal regulations, and our own internal policies. The university anticipates having more complete guidance available within the next several months. These International Travel Guidelines are subject to change and are current as of the effective date. The Guidelines supplement existing university policies and processes, including:

* [Policy Manual II-19 (Acceptable Use of Information Technology Resources)](https://opsmanual.uiowa.edu/community-policies/acceptable-use-information-technology-resources)
* Policy Manual [V-22 (Travel)](https://opsmanual.uiowa.edu/administrative-financial-and-facilities-policies/travel)
* Human Resources Temporary Overseas Work Arrangement [(TORWA)](https://hr.uiowa.edu/employee-well-being/workplace-flexibility/work-arrangement-application/temporary-overseas-remote) policy (for personal travel when work is being performed for 14 days or more)
* Division of Sponsored Programs [Export Control Program](https://dsp.research.uiowa.edu/export-controls-home)
* UI Research Security Policy *<working on getting a link for this>*

Travelers must also follow other obligations that may be imposed by law or externally funded grants or contracts. Even personal travel may be impacted by one or more policies depending on the circumstances.

## Individual Responsibility

**The** [**UI Travel Policy**](https://opsmanual.uiowa.edu/administrative-financial-and-facilities-policies/travel) **requires prior approval of all business travel, foreign or domestic, and registered in the ProTrav system. All employees should discuss their travel plans with their DEO, Supervisor, or HR representative before any planned international travel.** This includes university or research related travel paid for by a third party. Reasons for travel, length of travel destinations, and the traveler’s activities and access to UI systems and information should be discussed well ahead of the proposed travel dates to allow for appropriate assessment and risk management. If travel involves organizational business, teaching, research conferences, research purposes, or sponsored travel offers for research or professional purposes, then a mandatory pre-travel educational briefing will be provided by the Research Integrity & Security Office (RISO). For business-related travel, appropriate permissions must be obtained. For personal travel appropriate leave must be logged for those who have access to vacation.

Whether the travel is university-sponsored or occurs for personal reasons, employees are responsible for the institutional data and systems they bring, use or access while abroad. There are numerous legal and other security risks associated with accessing protected data and systems when present in foreign countries, regardless of the reason for travel. These risks evolve and may be country dependent. Past travel experience does not predict current or future risk. Travelers must plan for and evaluate the specific data and system access requirements for their destinations before traveling.

## Compliance and Risk Management

## The changing regulatory environment and its associated risks calls for active risk management of university data, systems, and potential legal/tax liabilities. The university recognizes that preparing for and meeting these requirements can be challenging, and in some circumstances, may limit or lessen productivity during travel. The University will continue to monitor the environment and compliance requirements to minimize the impact wherever possible.

## Data Privacy Expectations

When traveling abroad, employees should operate under the assumption that any systems or data that they access, transmit, or store may be accessed by a third party, regardless of the employee’s awareness or consent. Some foreign governments forbid the use of certain encryption technologies and may require the decryption of sensitive data pursuant to their laws.

Additionally, U.S. Customs and Border Protection (CBP) is lawfully authorized to inspect any electronic devices crossing the border (<https://www.cbp.gov/travel/cbp-search-authority/border-search-electronic-devices> ). CBP may legally demand your passwords, PINs, and/or encryption keys and are authorized to detain you for compliance. Technology may be confiscated during these searches.

## Access Restrictions– Moderate and High Risk Destinations

This guidance is meant to help travelers in a complex regulatory environment – travelers are advised to consult with their HR and IT professionals to ensure that planned activities and access or use of certain technologies complies with university policy, state and federal law.

When traveling internationally, the destination country informs the access restrictions that will apply to the traveler. Countries are grouped into two tiers – Moderate Risk and High Risk. Currently, most countries are in the Moderate Risk tier.

For both tiers, there are restrictions on activities and access to university data and IT systems. While traveling internationally to any country, travelers may not access sensitive information classified as Restricted or Critical. See <https://itsecurity.uiowa.edu/it-policies/it-guidelines/data-classification-guidelines> for more information about data classification.

## Traveling to Moderate Risk Destinations

When traveling to countries in the Moderate Risk tier, travelers should follow these general guidelines:

1. Discuss travel plans with your DEO, Supervisor, or HR representative before any planned international travel to ensure travel is permitted.
2. If travel involves research purposes, the Research Integrity & Security Office (RISO), may need to conduct a risk assessment of the planned activity or project, and if necessary, provide mitigation strategies to reduce researcher or UI risk involved with activity or project.
3. If permitted, discuss your travel and access needs with your IT and HR support staff to ensure your needs can be met for your specific travel plans and that all planned activities are compliant with university policy.
4. If you plan to access ANY IT systems or information, set up the VPN before you travel (link)
5. Considered limiting the devices and information you take with you during your travels

(Note 1: we plan to eventually have a single landing page for all international travel)

(Note 2: we will be revising the web page linked below to follow this guidance)

For more information on accessing university systems and information, please see:

<https://itsecurity.uiowa.edu/policies-standards-guidelines/it-guidelines/travel-guidelines>

## Traveling to High Risk Destinations

Due to regulatory, privacy and IT security risks, travelers to countries in the High Risk tier will not have access to any UI resources. The current list of High Risk countries include, Russia, China (including Hong Kong), Cuba, Iran, North Korea, Sudan, Syria, India, and the Crimea Region of the Ukraine. This list is subject to change. If the traveler intends to visit a country in the High Risk tier for university-sponsored or personal travel, they must notify their HR representative and IT professional as early as possible. Conducting University work from these countries may be prohibited, especially during personal travel.

**Access to any University of Iowa systems, data, and information is not allowed from High Risk countries. This includes Office365, MAUI, Workflow, ICON, Epic, Research Shared Drives, etc.**

Travelers should keep in mind that even if obtaining access may be technically feasible in High Risk countries, any utilization of such access is unacceptable under these Guidelines. If there are extenuating circumstances for these restrictions, exceptions may be requested through (TBD).

## Working During Personal Travel

Conducting University business from an international location, especially for prolonged periods, may expose the University to financial/tax liability as an employer. Consequently, if the purpose of travel is personal and the traveler wishes to work from the international location for more than 14 days, the traveler must complete a Temporary Overseas Remote Work Arrangement request in Employee Self Service in advance of travel. Please consult with your HR representative with any questions.