University Travel Policy

Overview for University Travelers
Agenda

- Overview
- University Travel Definition
- University Travel Policy Scope
- University Travel Policy Requirements and Restrictions
- Prior Approval and Registration of University Travel
- High-Risk Travel Destinations and Elevated Cybersecurity Risk Destinations
- Review of Travel to High-Risk Destinations
- University Devices or Data or Accessing University Data During Travel
- Resources
Overview

- In April 2023, the UMass Board of Trustees approved a new, systemwide University Travel Policy governing all University Travel

- The Travel Policy was created to:
  - Set guidelines for managing risk associated with University Travel
  - Create systemwide consistency in:
    - Definition of University Travel
    - Designation of High-Risk Destinations
    - Review of University Travel to High-Risk Destinations
  - Protect University Devices, Data and Property
University Travel Definition

- Section I (T) of the University Travel Policy

- Generally, University Travel, *regardless of the funding source*, includes but is not limited to any travel:
  - Associated with employment or recruiting
  - Bearing credit, or necessary for meeting a course or degree requirement, including graduate research
  - Funded with University funding, grants, scholarship, or sponsorship
  - Sponsored, arranged, endorsed, promoted, or administered by the University, Faculty or Staff
  - Related to a University-sponsored grant or contract
  - Involving physical transport of University Property
  - To an International Travel Destination when the Traveler will be performing any university-related work remotely on a regular basis
    - This includes Personal Travel when:
      - Traveling with a University Device or Data
      - Accessing University Data while traveling
University Travel Policy Scope

- The University Travel Policy pertains to all University Travelers on University Travel.

- A University Traveler is any person affiliated with any UMass campus conducting University Travel, including:
  - Employees
  - Students
  - Trustees
  - Recognized Student Organizations
  - Special State Employees (MGL 268A)
  - Non-employees (such as a speaker, lecturer, visiting professor, candidate for university employment, guest, etc.)
## University Travel Policy Requirements and Restrictions

### Requirements

- Prior Approval (also known as Pre-Travel Authorization) must be obtained by the Traveler for all University Travel
  - Campuses exemptions may be applicable

- All **overnight** travel must be **registered**
  - In-state
  - Out-of-state/domestic
  - International

### Restrictions

- Travel to designated **High-Risk Destinations** unless the respective Campus has conducted a risk review and approved the Travel

- Bringing University Devices or Data, or accessing University Data on either a personal or University-issued device, on Personal or University Travel to a designated **Elevated Cybersecurity Risk Destinations** unless authorized by the respective Campus IT Information Security Department
Prior Approval and Registration of University Travel

Prior Approval

- Prior approval of travel, also known as pre-travel authorization, must be obtained prior to booking travel.
- Pre-Travel Authorization includes supervisor review and, for international travel and where applicable, risk and export control review.
- Travelers should submit requests for pre-travel authorization in accordance with their campus’ requirements, but at least three weeks prior to travel.

Registration of Travel

- All overnight University travel must be registered. This includes:
  - In-state
  - Out-of-state/domestic
  - International
- Registration of travel must be completed once travel is booked.
- Travel can be registered in two ways:
  - Travel booked in Concur is automatically registered; no additional steps are necessary.
  - Travel booked outside of Concur must be registered via email following these guidelines.
High-Risk and Elevated Cybersecurity Risk Destinations

- **High-Risk Destinations** are any country, region, province or city posing substantive health, safety or security risk to a University Traveler and/or the University, or any comprehensively sanctioned country.

- **Elevated Cybersecurity Risk Destinations** are any international destinations posing substantive cybersecurity risk to a University Traveler and/or the University.

- Both are designated by the systemwide **Travel Risk Management Advisory Committee (TARMAC)**
  - TARMAC is comprised of representatives from each campus and the President’s Office
  - TARMAC does not review, authorize or deny Travel by University Travelers
Review of Travel to High-Risk Destinations

- Each campus has designated a Travel Risk Review Committee to review requests to travel to High-Risk Destinations by their respective Travelers
  - Traveler submits information regarding the proposed travel with their pre-travel authorization request

- Travel Risk Review Committee reviews requests and makes recommendation to Campus Travel Risk Approver

- Travel Risk Approver is authorized to approve or deny requests to Travel to High-Risk Destinations
Bringing University Devices and Data on or Accessing Data During Travel

- Travelers must obtain authorization through the travel pre-authorization request process from their respective Campus IT/Information Security(IT/IS) Department to bring University Devices or University Data, or access University Data while on travel to Elevated Cybersecurity Risk Destinations. This requirement pertains to:
  - University Travel and Personal Travel when traveling with University Devices or Data or accessing University Data
  - University Devices and University Data stored on or accessed from University or personal devices

- Campus IT/IS Department is authorized to:
  - Determine whether appropriate mitigation measures can be achieved
  - Prohibit the Traveler from bringing University Devices or Data, or accessing University Data while on said Travel when mitigation measures either:
    - Cannot be achieved
    - Cannot or will not be implemented

- Export Control review is required for all international travel
### Bringing University Devices and Data on or Accessing Data During Travel (continued)

The following chart details when IT Authorization and Export Control review is required.

<table>
<thead>
<tr>
<th>Type of Travel*</th>
<th>Is Destination an Elevated Cybersecurity Risk Destination?</th>
<th>Is Campus IT Authorization Required?</th>
<th>Is Export Control Review Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domestic</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Personal</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>International</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Personal</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Pertains to Travel when the Traveler intends to bring University Devices or University Data on Travel, or to access University Data while on Travel.
Resources

*NEW*
Travel & Expense Website

Campus Pre-Travel Risk and Export Control Forms

- UMass Amherst
- UMass Boston
- UMass Chan Medical School
- UMass Dartmouth
- UMass Lowell
- UMass President’s Office