Doc. T22-066, as amended
Passed by the Board of Trustees on April 12, 2023

UNIVERSITY OF MASSACHUSETTS TRAVEL POLICY

PURPOSE

The Policy provides systemwide uniformity for addressing safety, security, and compliance during University Travel (as defined below). It also establishes additional requirements for travel to high-risk destinations. This Policy applies to all University Travel and all University Travelers as defined in this policy, regardless of funding source.

INTRODUCTION

The University of Massachusetts (UMass or University) recognizes the import and necessity of travel for educational, research and business purposes in furtherance of the University's mission. In supporting these opportunities, the University must manage the associated travel risks and liabilities while promoting the health, safety, and security of all members of the UMass community.

The University establishes this Policy pursuant to the authority granted in M.G.L. c. 75, § 32 to set requirements and expectations for University Travel. All University Travelers must comply with this Policy, associated Presidential Standards, and applicable campus guidelines.

I. DEFINTIONS

A. Approver: Duly Authorized university representative with authority to approve travel for budgetary and programmatic purposes.

B. Campus: Individual academic institution of the University of Massachusetts system (Amherst, Boston, Dartmouth, Lowell, Chan Medical School). For purposes of this policy, the President's Office is also considered to be a campus component.

C. Campus Travel Risk Review Committee: Committee authorized by each campus or the UMass President's Office (UMPO) to review requests by prospective Traveler(s) from the respective campus/UMPO for University Travel to High-Risk Destinations and to make recommendations to the Travel Risk Approver.

D. Comprehensively Sanctioned Destination: Countries and geographic regions subject to comprehensive U.S. trade, economic restrictions, or embargo.

E. Domestic Travel Destination: Any travel destination that is a state or territory of the United States.

F. Duly Authorized: With the authority of the University per Policy, Standard, or campus procedures.

G. Elevated Cyber Security Risk Destination: Any International Travel Destination designated by the Systemwide Travel Risk Management Advisory Committee or the campus as posing substantive cybersecurity risk to a University Traveler and/or the University.

H. High-Risk Destination(s): Any Comprehensively Sanctioned Destination(s); any country, region, province or city, including Domestic Travel Destinations and International Travel Destinations, designated by the Systemwide Travel Risk Management Advisory Committee or the campus as posing substantive health, safety, security risk to a University Traveler and/or the University.

I. High-Risk Travel Destination Request Review Protocol: The pre-departure process for identifying, reviewing, and approving or denying proposed University Travel to High-Risk Destinations.

J. International Travel Destination: Any travel destination that is not a state or territory of the United States.

K. Personal Side Trip: Personal Travel made by a University Traveler while on approved University Travel.

L. Personal Travel: Travel that is not University Travel including any Personal Side Trips.

M. Travel Risk Approver: Duly Authorized University representative(s) designated by the campus or UMPO with authority to approve or deny Travel to High-Risk Destinations, generally after evaluating recommendations of the Campus Travel Risk Review Committee.

N. Travel Risk Management Advisory Committee (TARMAC): Systemwide, five-campus and the UMass President's Office (UMPO) advisory committee established per Section II(G) of this Policy and authorized to designate and periodically review the University's systemwide High-Risk Destinations and advise on travel compliance and management protocols.

O. Unauthorized Travel: Any travel that has been denied or is unapproved by the Campus as University Travel.

P. University Business: Any activity, practice, commerce, trade, service, research, education, etc. in furtherance of the University's mission and functions.

Q. University Device(s): Electronic devices such as laptops/computers, tablets, mobile phones, smartphones, and the like which are owned by the University and used to collect, store, access, transmit, carry, use, or hold University Data whether during or outside of normal working hours and whether it is used at a normal place of work or not.

R. University Data: Data created, received, maintained or transmitted by or on behalf of the University through the course of its academic, administrative, research, or outreach activities.

S. University Property: University-owned equipment, specimens and/or materials.

T. University Travel ("Travel"): Any travel by Travelers for University Business regardless of funding source. University Travel includes, but is not limited to:
   i. Travel in the course and scope of the Traveler's employment at the University.
   ii. Travel financed, in full or part, through university funding, grants, scholarship, or sponsorship.
   iii. Travel sponsored, arranged, endorsed, promoted, or administered by the University, or by university faculty or staff members.
   iv. Travel that is credit-bearing, or necessary for meeting a course or degree requirement, including graduate research at the University.
   v. Travel that involves the physical transport of University Property regardless of funding source for such travel.
   vi. Travel directly related to a university-sponsored grant or contract.
   vii. Travel to an International Travel Destination when the Traveler will be performing any university-related work remotely on a regular basis.

U. University Traveler(s) ("Traveler"): Duly Authorized employee, student, recognized student group or organization, trustee and Special State Employee as defined in MGL Chapter 268A, or non-employee (e.g., speaker, lecturer, student, visiting professor, candidate for university employment, guest etc.) on University Travel.

V. University Travel Registry: Platform for maintaining critical travel information of University Travelers for safety and security purposes.

II. POLICY

A. Prior Approval: All University Travelers must obtain budgetary, programmatic and, as necessary, risk approvals for University Travel prior to departure.

B. Registration of Travel: All University Travelers must register University Travel in the University Travel Registry and obtain associated approvals prior to departure.

C. Travel Expenses: The Business and Travel Expense Policy (T92-031, Appendix C) governs expenses associated with all University Travel.

D. Authority to Restrict Travel: The University reserves the right to restrict, deny, or postpone any University Travel in its sole discretion if the risks associated with the proposed travel outweigh the benefits to the professional or business purpose of the travel.

E. Authority to Require Travelers to Evacuate: The University reserves the right to require Travelers to leave or evacuate a given location when, in its sole judgement and discretion, it determines that continued presence in that location may severely endanger health, safety or well-being of University Travelers or others.
   i. University Travelers who fail to heed University instruction to evacuate do so at their own risk and are on notice that the University may not be able to respond with assistance. Such Travelers may forfeit emergency travel assistance and insurance coverage, academic credit, tuition payments or expense reimbursement, and may be held responsible for additional expenses incurred by the University due to the Traveler's refusal to follow policy. In addition, such Traveler(s) may be subject to local administrative requirements or law enforcement actions related to specific local conditions or restrictions.

F. Compliance with Laws and Regulations: Travelers are required to comply with applicable state, federal and international laws, including but not limited to the anti-bribery provisions of the U.S. Foreign Corrupt Practices Act ("FCPA"), which prohibits bribery of foreign officials; 18 USC Section 201, which prohibits bribery of US officials; and MGL Chapter 268A, the MA conflict of interest law.

G. Travel with University Devices and/or University Data.
   i. University Travelers traveling with University Devices, University Data, or by accessing University Data remotely shall not create data security or other confidentiality risks that cannot be effectively mitigated.
      1. Whether on University Travel or Personal Travel, Travelers traveling with University Device(s) and/or University Data must comply with cybersecurity, connectivity, telecommunication requirements as set forth in the Presidential, University Information Technology Services (UITS), and/or campus Information Security or Technology departmental standards and guidelines.
   ii. University Travelers must not travel with University Devices and/or University Data to International Travel Destinations with elevated cyber security risks. For clarity, this extends to international Personal Travel.
      1. Campuses may grant authority to travel with University Devices and/or University Data when mitigation measures can effectively be achieved.
         a. Traveler must obtain such approval from their respective campus prior to Travel.

H. University Travel to or Through High-Risk Destinations.
   i. This Policy establishes a University Travel Risk Management Advisory Committee (TARMAC) which is a systemwide advisory committee with representation from each campus and the President's Office (UMPO). TARMAC is authorized and charged with assessing and monitoring travel-related risks, designating High-Risk Destinations or criteria for designating High-Risk Destinations, advising the system on travel compliance and management protocols, and periodically reviewing this Policy and the associated Presidential Standards.
      1. The composition of TARMAC is detailed in the Presidential Standards.
      2. Each Campus Travel Risk Review Committee maintains the authority to designate additional High-Risk Destinations for their campus.
      3. TARMAC will serve as a resource for the Campus Travel Risk Review Committees.
      4. Each Campus, through its Travel Risk Review Committee and Travel Risk Approver, has the authority to approve or deny Travel to a High-Risk Destination by their respective Traveler(s) [see Section II.(H)(ii) and II.(I)].
   ii. Generally, University Travel to or through High-Risk Destinations is not allowed.
   iii. The University recognizes that, on occasion, there may be a compelling reason to consider allowing University Travel to or through a High-Risk Destination. In such cases, and always prior to departure, Travel Risk Approvers must approve or deny all University Travel to, or through, a High-Risk Destination(s).
      1. Each Campus, through its Travel Risk Review Committee and Travel Risk Approver, has the authority to approve or deny Travel to a High-Risk Destination by their respective Traveler(s).
         a. The Travel Risk Approver is authorized to approve or deny requests to travel to or through High-Risk Destinations, generally after reviewing the recommendations of the Campus Travel Risk Review Committee.

iv. Each campus and the UMPO shall designate a Travel Risk Approver with the authority and responsibility to approve or deny travel requests from their respective campus/UMPO for any Travel to or through High-Risk Destinations.
v. Each campus and the President's Office shall appoint a Campus Travel Risk Review Committee responsible for reviewing travel requests from their respective Travelers to High-Risk Destinations and making recommendations to the respective Travel Risk Approver.

I. High-Risk Travel Destination Request Review Protocol.
   i. Each campus and UMPO must develop and implement a pre-departure High-Risk Travel Destination Request Review Protocol for identifying and reviewing all anticipated University Travel to or through High-Risk Destinations for the respective campus or UMPO.
      1. High-Risk Travel Destination Request Review Protocol must be compliant with this Policy, associated Presidential Standards and associated campus guidelines.
   ii. University Travelers seeking to travel to or through a High-Risk Destination must request and obtain travel authorization in accordance with High-Risk Travel Destination Request Review Protocol.
      1. Approval of Travel to High-Risk Destination.
         a. University Traveler authorized to travel to a High-Risk Destination must comply with all pre-departure requirements which may include, but are not limited to:
            i. Enrollment with the U.S. Department of State, "Smart Traveler Enrollment Program" (STEP) or the equivalent citizen service of the University Traveler's country of citizenship.
            ii. Registration with the University's international emergency travel assistance provider.
            iii. Obtaining a required license from the U.S. Department of Treasury Office of Foreign Assets Control for travel to a Comprehensively Sanctioned Destination, if applicable.
            iv. Completing and acknowledging completion of a safety, cybersecurity and security training or briefing.
   iii. Denial of Travel to High-Risk Destination.
      1. If the Travel Risk Approver denies a request to travel to a High-Risk Destination, the travel shall not be considered University Travel and shall not be supported with University funds. Any Traveler who makes the personal decision to travel to a High-Risk Destination despite the denial does so as a private individual and without university support. The University has no obligation(s) or liability in connection with such unauthorized travel, and such travel may not be eligible for support through the University emergency travel assistance program or University insurance coverage.

J. Export Control Requirements for Travel to International Travel Destinations.
   i. When traveling to any International Travel Destination, University Travelers are considered "exporters" of any tangible items and technical information they take with them and/or share abroad. Therefore, all University Travelers traveling to International Travel Destination(s) on University Travel shall comply with all established laws, regulations and requirements specific to Export Control, including requirements for the proper handling, transfer, access, storage, control, and release of export-controlled commodities, hardware, software, information, technology, and technical data.
      1. Campuses shall implement an export control review process for University Travel to International Travel Destination(s).

K. International Emergency Travel Assistance and Insurance Program.
   i. The University international emergency travel assistance and international travel accident and sickness insurance program provides risk management and emergency support and services for Travelers on approved international University Travel.
   ii. Travelers are responsible for reviewing all materials relating to University international travel assistance and international travel accident and sickness insurance program and for cooperating with the University in the event that any claim needs to be filed.

III RESPONSIBILITIES

A. Each campus is responsible for designating responsibility for compliance with this Policy and applicable state and federal law.

B. Each campus is responsible for designating responsibility for compliance oversight of the U.S. export control and economic sanctions requirements for the University.

C. The Travel Risk Management Advisory Committee (TARMAC) is responsible for designating, monitoring, and periodically updating the University's designation of High-Risk Travel Destinations as well as advising the system on travel compliance and management protocols. TARMAC is also responsible for periodically reviewing this Policy and the associated Presidential Standards.

D. Each campus is responsible for reviewing and approving or denying individual requests received from University Travelers from their respective campus for travel to or through High-Risk Travel Destinations.

IV. STANDARDS

The President, in consultation with the Chancellors and the Vice President for Administration & Finance and Chancellors, will issue administrative standards to implement this policy.

V. RELATED POLICIES

- Business and Travel Expense Policy Doc. T92-031, Appendix C, as amended.

UNIVERSITY OF MASSACHUSETTS
PRESIDENTIAL ADMINISTRATIVE STANDARDS
FOR THE UNIVERSITY TRAVEL POLICY

These presidential administrative standards ("Standards") pertain to the University of Massachusetts Travel Policy (Doc. T-22-066) (the "Policy"). In accordance with the Policy, these Standards apply to travel by a duly authorized University of Massachusetts employee, student, Trustee, or associate traveling on university business regardless of the source of funds.

Table of Contents

I. INTRODUCTION

These Standards provide guidance on the implementation of the University Travel Policy ("Travel Policy"), established pursuant to the authority granted in M.G.L. c. 75, § 32 to: set requirements and expectations for University Travel; provide systemwide uniformity for addressing safety, security, and compliance during University Travel; set forth approval requirements for domestic and international travel and travel to high-risk destinations; and set forth requirements pertaining to University Devices and Data when traveling to International Destinations.

All University Travelers must comply with the Policy, these associated Standards, and applicable Campus guidelines.

a. Applicability
   The Travel Policy and these Standards apply to all University Travel and all University Travelers as defined in the Policy, regardless of funding source.
b. Definitions
   i. Approver: Duly Authorized university representative with authority to approve travel for budgetary and programmatic purposes.
   ii. Campus: Individual academic institution of the University of Massachusetts system (Amherst, Boston, Dartmouth, Lowell, Chan Medical School). For purposes of the Policy, the President's Office is also considered to be a campus component.

iii. Campus Travel Risk Review Committee: Committee authorized by each campus or the UMass President's Office (UMPO) to review requests by prospective Traveler(s) from the respective campus/UMPO for University Travel to High-Risk Destinations and to make recommendations to the Travel Risk Approver.

iv. Comprehensively Sanctioned Destination: Countries and geographic regions subject to comprehensive U.S. trade, economic restrictions, or embargo.

v. Domestic Travel Destination: Any travel destination that is a state or territory of the United States.

vi. Duly Authorized: With the authority of the University per Policy, Standard, or campus procedures.

vii. Elevated Cyber Security Risk Destination: Any International Travel Destination designated by the Systemwide Travel Risk Management Advisory Committee or the campus as posing substantive cybersecurity risk to a University Traveler and/or the University.

viii. High-Risk Destination(s): Any Comprehensively Sanctioned Destination(s); any country, region, province or city, including Domestic Travel Destinations and International Travel Destinations, designated by the Systemwide Travel Risk Management Advisory Committee or the campus as posing substantive health, safety, security risk to a University Traveler and/or the University.

ix. High-Risk Travel Destination Request Review Protocol: The pre-departure process for identifying, reviewing, and approving or denying proposed University Travel to High-Risk Destinations.

x. International Travel Destination: Any travel destination that is not a state or territory of the United States.

xi. Personal Side Trip: Personal Travel made by a University Traveler while on approved University Travel.

xii. Personal Travel: Travel that is not University Travel including any Personal Side Trips.

xiii. Travel Risk Approver: Duly Authorized University representative(s) designated by the Campus or UMPO with authority to approve or deny Travel to High-Risk Destinations, generally after evaluating recommendations of the Campus Travel Risk Review Committee.

xiv. Travel Risk Management Advisory Committee (TARMAC): Systemwide, five-campus and the UMass President's Office (UMPO) advisory committee established per Section II(G) of the Policy and authorized to designate and periodically review the University's systemwide High-Risk Destinations and advise on travel compliance and management protocols.

xv. Unauthorized Travel: Any travel that has been denied or is unapproved by the Campus as University Travel.

xvi. University Business: Any activity, practice, commerce, trade, service, research, education, etc. in furtherance of the University's mission and functions.

xvii. University Device(s): Electronic devices such as laptops/computers, tablets, mobile phones, smartphones, and the like which are owned by the University and used to collect, store, access, transmit, carry, use, or hold University Data whether during or outside of normal working hours and whether it is used at a normal place of work or not.

xviii. University Data: Data created, received, maintained or transmitted by or on behalf of the University through the course of its academic, administrative, research, or outreach activities.

xix. University Property: University-owned equipment, specimens and/or materials.

xx. University Travel ("Travel"): Any travel by Travelers for University Business regardless of funding source. University Travel includes, but is not limited to:

1. Travel in the course and scope of the Traveler's employment at the University.

2. Travel financed, in full or part, through university funding, grants, scholarship, or sponsorship.
3. Travel sponsored, arranged, endorsed, promoted, or administered by the University, or by university faculty or staff members.
4. Travel that is credit-bearing, or necessary for meeting a course or degree requirement, including graduate research at the University.
5. Travel that involves the physical transport of University Property regardless of funding source for such travel.
6. Travel directly related to a University-sponsored grant or contract.
7. Travel to an International Travel Destination when the Traveler will be performing any university-related work remotely on a regular basis.

xxi. University Traveler(s) ("Traveler"): Duly Authorized employee, student, recognized student group or organization, trustee and Special State Employee as defined in MGL Chapter 268A, or non-employee (e.g., speaker, lecturer, student, visiting professor, candidate for university employment, guest etc.) on University Travel.

xxii. University Travel Registry: Platform for maintaining critical travel information of University Travelers for safety and security purposes.

II. STANDARDS

Section 1.01: Prior Approval

a. Travelers must obtain budgetary, programmatic and risk (see Sections 1.09, 1.10, 1.11) approval prior to departure and in accordance with the timeframes set by their respective campus.
   i. Campuses may grant an exception to compliance with their respective timeframes.
b. Campuses have the discretion to grant blanket approvals to Travelers for domestic University Travel.

Section 1.02: Registration of Travel

a. Registration of University Travel not only makes it possible to deliver destination-specific travel advice, but also assists the University in identifying and supporting Travelers potentially impacted by itinerary-specific threats and/or compliance requirements and in providing, as appropriate, assistance in response to events that might present health, safety and security risks to Travelers.
b. Travelers must register all ***in-state (Massachusetts) overnight*** and ***out-of-state (outside of Massachusetts) domestic*** Travel and ***international*** Travel in the University Travel Registry prior to departure and in accordance with the timeframes set by their respective campus.
   i. Each instance of Domestic overnight University Travel approved through a blanket approval is required to be registered.
c. Travelers must update the University Travel Registry with any changes in Travel itinerary such as travel dates, destinations and on-site contact information as soon as the information becomes available.
   i. Changes to Travel may be subject to review and approval.
   ii. Changes to Travel are subject to University Device and Data restrictions (see Section 1.10).

Section 1.03: Travel Expenses

a. Travel expenses are governed by the Business and Travel Expense Policy (T92-031, Appendix C) and associated Standards.
b. Travelers must abide by the Business and Travel Expense Policy and associated Standards for allowability of travel expenses and reimbursement of travel expenses.

Section 1.04: Authority to Restrict Travel

a. Travelers must abide by the Business and Travel Expense Policy and associated Standards for allowability of travel expenses and reimbursement of travel expenses:
   i. The risk associated with the Travel, despite mitigation measures, poses an unacceptable risk to health, safety, or well-being of the Traveler or
   ii. The risk associated with the Travel, despite mitigation measures, poses an unacceptable liability risk to the University.
b. Restrictions may include delay, abbreviation or indefinite postponement of Travel to a given location.
c. Such restrictions can be implemented prior to, or during, Travel.
d. Such restrictions may include prohibiting the Traveler from traveling with University Devices and/or University Data or accessing University Data during Travel. See Section 1.10.

Section 1.05: Authority to Require Travelers to Evacuate

a. In accordance with M.G.L. c. 75, § 32, the University has the authority to require a Traveler to leave or evacuate a given location in the event of a voluntary or mandatory evacuation order by the U.S. Government or when, in its sole judgement and discretion, the University determines continued presence in that location may seriously endanger health, safety or well-being of University Travelers or others.

Section 1.06: Travelers Must Comply with Laws and Regulations

a. Travelers must comply with all local, state, federal and national laws and regulations, even if such laws are more restrictive than those applicable in their home jurisdiction.
b. Travelers must comply with the U.S. Foreign Corrupt Practices Act ("FCPA") and 18 USC Section 201, which prohibit bribery of and by foreign officials.
c. Travelers must comply with all export control requirements for all University Travel to International Destinations.
d. Travelers must adhere to the Massachusetts conflict-of-interest law (MGL Chapter 268A) and related University conflict-of-interest policies while conducting University Travel.
e. University Travelers are responsible for tax compliance associated with international Travel (Value-Added Taxes (VAT)).
   i. Campuses should consider consulting with the University customs broker (Highland Forwarding) for those unique, bespoke or high-value items that may trigger tax compliance and to advise on the applicability of necessary documentation.
f. It is the responsibility of the Traveler to be or become familiar with and maintain compliance with said laws, regulations and requirements.
g. University Travelers are responsible for determining and complying with all visa and entry requirements associated with Travel to International Destination(s), noting that visa requirements vary depending on the Traveler's citizenship and planned activities. Travelers can contact the University's travel management company or international travel emergency services provider for personalized guidance.

Section 1.07: Personal Travel

a. Personal Travel is travel that is not University Travel.
b. Personal Side Trips are Personal Travel made by a University Traveler while on University Travel. Personal Side Trips include travel adjacent to and during University Travel.
   Examples of Personal Side Trips:
   - *A Traveler is on approved University Travel to Germany from June 14 through June 24. The Traveler arranges and goes on Personal Travel to another destination from June 2-14.*

- *A Traveler is on approved University Travel to Germany from June 14 through June 24. The Traveler arranges and goes on Personal Travel to another destination for a weekend during this timeframe.*
- *A Traveler is participating in a Study Abroad Program in Germany and makes a weekend trip to another destination.*

i. Personal Side Trips are generally covered by University travel accident and sickness insurance provided the Personal Side Trip meets the coverage conditions (i.e., within the duration limit specified in the insurance policy – generally 7 days or less). Additional information can be obtained through the UMass Treasurer's Office.

ii. If a Personal Side Trip involves travel to a High-Risk Destination, the Campus may require the Traveler to complete a release of liability.

c. Personal Travel and Personal Side Trips are subject to Section G of the Policy (*Travel with University Devices and/or Data)* and Section 1.10 of these Standards.

Section 1.08: Designation of High-Risk Travel Destinations

a. Travel Risk Management Advisory Committee (TARMAC).

i. The University shall establish a systemwide Travel and Risk Management Advisory Committee (TARMAC).

1. TARMAC Responsibilities and Authorities.

a. TARMAC has authority to designate High-Risk Destinations and set criteria used in designating High-Risk Destinations.

b. High-Risk Destinations designated by TARMAC and/or High-Risk Designations meeting the criteria set by TARMAC shall have systemwide applicability.

c. Each Campus/UMPO has the authority to designate additional High-Risk Destinations for applicability to their respective Campus/UMPO.

i. Campuses may delegate this responsibility to the Campus Travel Risk Review Committee.

d. Each Campus/UMPO has the authority to allow Travel to a High-Risk Destination when the campus Travel Risk Approver has approved such Travel. See Section 1.08(d).

e. TARMAC does not have the authority to approve or deny requests for Travel to a High-Risk Destination; the authority to approve or deny requests to High-Risk Travel Destinations resides with the respective campus/UMPO Travel Risk Approver of Traveler.

f. TARMAC may share travel risk information and resources among members.

2. TARMAC Membership

a. TARMAC membership at a minimum must include representatives from each of the following:

i. Amherst Campus (2)
ii. Boston Campus (2)
iii. Dartmouth Campus (2)
iv. Lowell Campus (2)
v. Chan Medical School Campus (2)
vi. UMPO - President's Office Operations (1)
vii. UMPO - Office of the General Counsel (2)
viii. UMPO - Enterprise Risk Management (1)
ix. UITS Information Security (1)
x. Campus CISO (1)

b. Only members of Campus/UMPO Risk Review Committees can serve as their respective TARMAC Campus/UMPO representative.
c. TARMAC membership shall designate a Chairperson.
d. TARMAC shall designate a TARMAC member to be responsible for ensuring High Risk Destinations and associated criteria are made available to University Travelers.
e. TARMAC shall meet quarterly.
    i. TARMAC may set an alternate schedule with agreement of a majority of the membership.
    ii. As needed, TARMAC may request through the TARMAC Chairperson and at the TARMAC Chairperson's discretion that TARMAC convene.
    iii. The TARMAC Chairperson can add destinations to the High-Risk Destination list if such destinations objectively meet the criteria set forth by the TARMAC.

b. Designation of High-Risk Destinations.
    i. TARMAC shall set criteria for designation of High-Risk Destinations.
        1. Criteria shall be made available to University Travelers.
    ii. TARMAC, in consultation with UITS and Campus Chief Information Security Officers, shall set criteria for designation of Elevated Cyber Security Risk Destinations.
        1. Criteria shall be made available to University Travelers.
    iii. Using designated criteria, TARMAC shall designate High-Risk Destinations and Elevated Cyber Security Risk Destinations.
        1. Information on such Destinations shall be made available to University Travelers.
c. Campus Travel Risk Review Committee.
    i. Each Campus/UMPO shall designate a Campus Travel Risk Review Committee for the respective Campus/UMPO.
    ii. Responsibilities and Authorities.
        1. Campus Travel Risk Review Committee is responsible for reviewing requests by prospective Traveler(s) from the respective Campus/UMPO for University Travel to or through High-Risk Destinations.
        2. Campus Travel Risk Review Committee is authorized to make recommendations to the Travel Risk Approver on the approval, denial or modifications to the requested Travel.
    iii. Committee Membership.
        1. Each Campus/UMPO has the authority to designate the membership of their respective Campus Travel Risk Review Committee.
            a. Each Campus Travel Risk Review Committee should include at least three members.
                i. Each Campus/UMPO should ensure the membership of their respective Campus Travel Risk Review Committee includes individuals/disciplines that can address the risks specific to the respective Campus/UMPO.
            b. Each Campus/UMPO Travel Risk Review Committee may consult with additional subject matter experts from their respective Campus or with the TARMAC as the Campus deems appropriate.

d. Campus Travel Risk Approver.
    i. Each Campus/UMPO shall designate a Travel Risk Approver to approve or deny Travel to High-Risk Destinations by their respective Campus/UMPO Travelers.
        1. A Campus/UMPO may delegate the role of the Travel Risk Approver to their respective Campus Travel Risk Review Committee.
    ii. Role and Authorities of Travel Risk Approver.
        1. The Travel Risk Approver is authorized to approve, deny or require modifications to Travel to High-Risk Destinations.

2. Travel Risk Approver should evaluate the recommendations of the Campus Travel Risk Review Committee prior to making a decision.
    a. In cases where an expedited decision is required because of extenuating circumstances which exclude convenience, the Travel Risk Approver may decide without first consulting the Travel Risk Review Committee.

Section 1.09: High-Risk Travel Destination Request Review Protocol *(proposed content for discussion)*

a. Each Campus/UMPO must develop and implement a pre-departure High-Risk Travel Destination Request Review Protocol for identifying and reviewing all anticipated University Travel to or through High-Risk Destinations for the respective Campus/UMPO.
    i. Protocol should be written and publicly available for the University Travelers.
    ii. Protocol should include Export Control review for Travel to International Destinations (See Section 1.11).
    iii. Protocol should require the Campus Travel Risk Review Committee to review all requests from their respective Campus Travelers to High-Risk Destinations.
        1. Although TARMAC can serve as a resource for a Campus Travel Risk Review Committee, TARMAC does not play a role in the Campus Travel Risk Review Protocol.
    iv. Campus Travel Risk Review Committee makes recommendation to Travel Risk Approver about approving, denying or conditionally approving Travel to High-Risk Destination.
        1. In limited circumstances, Travel Risk Approver may be required to approve, deny or conditionally approve Travel to High-Risk Destination without prior review by the Campus Travel Risk Review Committee.
    v. Travel Risk Approver approves, denies or conditionally approves Travel.
        1. Approval of Travel to High-Risk Destination.
            a. University Traveler approved to travel to a High-Risk Destination must comply with all pre-departure requirements prior to departure, including but not limited to the following:
                i. Registration of Travel in University Travel Registry, including travel itinerary.
                ii. Export Control (see Section 1.11).
                iii. University Device and Data requirements (see Section 1.10).
                iv. Enrollment with the U.S. Department of State *Smart Traveler Enrollment Program (STEP)* or the equivalent citizen service of the University Traveler's country of citizenship.
                v. Registration with the University's travel accident and sickness insurance emergency services provider, including travel itinerary.
                vi. Becoming familiar with travel-related policies and guidelines.
                vii. Completing and acknowledging completion of a safety, cybersecurity and security training or briefing as required by the Campus.
                    1. Briefings are provided by the Traveler's respective Campus and may be in-person and/or through distributed materials.
            b. University Traveler approved to travel to a High-Risk Destination may also need to take the following pre-departure activities, including but not limited to the following:
                i. Enrollment with the U.S. Department of State *Smart Traveler Enrollment Program (STEP)* or the equivalent citizen service of the University Traveler's country of citizenship.
                ii. Registration with the University's travel accident and sickness insurance emergency services provider, including travel itinerary.

2. Denial of Travel to High-Risk Destination.
    a. When Travel to a High-Risk Destination is denied:
        i. Said Travel is Unauthorized Travel.
        ii. Said Travel is not University Travel.
        iii. Said Travel shall not be supported with University funds.
    b. Denied Travel is Unauthorized Travel.
        i. If a Traveler travels to a High-Risk Destination when the Travel has been denied, the Traveler travels:
            1. As Personal Travel
            2. In their personal capacity
            3. At Traveler's own personal expense
            4. Without University support
                i. The University has no obligation(s) or liability in connection with Unauthorized Travel.
                ii. Unauthorized Travel may not be eligible for support through the University emergency travel assistance program or University insurance coverage.
3. Conditional Approval of Travel to High-Risk Destination.
    a. Travel to a High-Risk Destination may be conditionally approved pending actions by the Traveler and/or modifications to Travel.
        i. All conditional approval requirements shall be in writing and acknowledged by Traveler.
        ii. Prior to departure, and within the timeframe required by the Campus, Traveler shall demonstrate in accordance with Campus processes that all conditions of travel have been met.
            1. Should conditional approval requirements not be met by the Traveler in accordance with the Campus processes and within the timeframe required by the Campus, such Travel shall be deemed denied and subject to section 1.09(a)(v)(2)(b) above.

Section 1.10: Travel with University Devices and/or Data

a. University Travelers traveling with University Devices or accessing University Data remotely shall not create data security or other confidentiality risks that cannot be effectively mitigated.
b. Travelers traveling with University Device(s) and/or University Data on University Travel to a High-Risk Destination or Elevated Cybersecurity Risk Destination must comply with cybersecurity, connectivity, telecommunication requirements as set forth by the Traveler's respective Campus as well as any pertinent state, federal or international requirement, regulation or law.
    i. Each Campus shall establish these requirements for their respective Campus and respective Travelers.
    ii. University Travelers traveling to a High-Risk Destination or Elevated Cybersecurity Risk Destination are responsible for securing permission from their respective Campus IT department or designated IT point of contact to bring or access University Devices or Data prior to traveling to these Destinations.
        1. The Campus IT department or designated IT point of contact is authorized to determine the measures required to be taken to effectively mitigate the cybersecurity risk. These measures must be implemented by the Traveler or IT Department to be allowed to bring and/or access University Devices or University Data while traveling to these Destinations.

a. If the Campus IT department or designated IT point of contact determines the cybersecurity risks cannot be effectively mitigated, University Travelers shall not be allowed to bring University Devices or Data on Travel or access University Data during Travel.

2. If a Traveler stores or accesses University Data on or from a personal device (which is strongly discouraged), said personal device is subject to the Campus IT department's requirements and mitigation measures while the Traveler is on University Travel to a High-Risk Destination or Elevated Cybersecurity Risk Destination. If mitigation measures are not feasible, or the Traveler chooses not to apply mitigation measures to the personal device, said Data or access to Data must be removed from the personal device.

iii. Personal Travel:

1. Individuals who intend to bring or access University Devices or Data on Personal Travel to a High-Risk Destination or Elevated Cybersecurity Risk Destination must comply with cybersecurity, connectivity, telecommunication requirements as set forth by the Traveler's respective Campus for University Devices and Data.
   a. Such individuals are responsible for securing permission from their respective Campus IT department or designated IT point of contact to bring or access University Devices or Data prior to commencing Personal Travel.
      i. The Campus IT department or IT point of contact is authorized to determine the requirements and measures that must be taken to mitigate the cybersecurity risk to University Devices or University Data. These measures must be implemented by the individual or Campus IT Department to be allowed to bring or access University Devices or University Data while on said Personal Travel to a High-Risk Destination or Elevated Cybersecurity Risk Destination.
2. If the Campus IT department or designated IT point of contact determines that that the cybersecurity risks to University Devices or Data cannot be mitigated, University Travelers are not allowed to bring and/or access University Devices or University Data while on said Personal Travel to these Destinations.
   a. If individuals who intend to access University Data on or from a personal device (which is strongly discouraged) while conducting Personal Travel to a High-Risk Destination or Elevated Cybersecurity Risk Destination, said personal device is subject to the individual's respective Campus IT department's requirements and mitigation measures. If mitigation measures are not feasible, or the individual chooses not to apply mitigation measures to the personal device, said Data or access to Data must be removed from the personal device.

Section 1.11 International Travel Export Control & Sanctions Requirements

a. When traveling internationally, University Travelers are "exporters" of any tangible items and technical information they take with them and/or share abroad.
b. Therefore, University Travelers traveling to an International Destination(s) must comply with all export control and sanctions laws, regulations and requirements including, but not limited to, proper handling, transfer, access, storage, control, and release of export-controlled commodities, hardware, software, information, technology, and technical data.
c. Export Control review is required for all University Travel to or through International Destinations, High Risk Destinations and Elevated Cyber Security Risk Destinations. Export Control approval is required for travel to High-Risk Destinations and Elevated Cyber Security Risk Destinations.
d. Campus Export Control Review and Approval Processes.
   i. Campuses / UMPO shall implement export control review and approval processes for all international University Travel conducted by their respective University Traveler(s).

ii. Campus Export Control Review Process will determine, document and communicate applicable licensing or documentation requirements related to:
    1. Office of Foreign Assets Control (OFAC) regulations (for travel to a sanctioned destination).
    2. Department of Commerce Export Administration Regulations (EAR).
    3. Department of State International Traffic in Arms Regulations (ITAR).
iii. At a minimum, international University Travelers must disclose the following information to campus export control offices for review and consideration. This disclosure may be accomplished through the process for obtaining pre-travel authorization for Travel.
    1. Purpose and details of Travel.
    2. Travel itinerary including dates, locations and modes of travel.
    3. University Traveler details (citizenship / passport / employment / student)).
    4. List of any University equipment and materials the Traveler will bring on Travel, such as data, technology, software, specimens, and samples.
iv. Campuses may require additional information disclosure(s) depending on the purpose, destination and scope of the trip, such as the individuals and entities with whom the Traveler will interact.
v. Campuses/UMPO will establish required timeframes for their respective Travelers' submission of information for export control review and compliance.
    1. Campus export control review will be conducted prior to the Traveler's departure, and, for Travel to High-Risk Destinations or Elevated Cyber Security Destinations, prior to a Campus Travel Risk Approver approving or denying Travel.
    2. Campus export control approval, if required, must be obtained by the Traveler prior to departure.
vi. Export Control Review and Approval Process may be embedded in the Campus Travel Risk Review Protocol (see Section 1.09).

e. Export Control requirements apply to University Devices and/or Data that are brought on Personal Travel to International Destinations, High-Risk Destinations and Elevated Cyber Security Risk Destinations.
f. Campuses will provide international University Travelers educational and awareness training or resources on export control and sanctions as needed to maintain compliance with regulations. Training and resources may include, but not necessarily be limited to:
    i. Export controls and sanctions programs awareness.
    ii. Information on "Tools of the Trade" (TMP) and "Baggage" (BAG) license exceptions.
    iii. Timeframes and expectations for obtaining applicable export license(s).
    iv. Restricted-Party Screening of Individuals and Entities with whom University Travelers will be meeting, communicating and collaborating while abroad.
    v. Cybersecurity requirements.
g. University Travelers are responsible for making determinations about applicability "Tools of the Trade" (TMP) and "Baggage" (BAG) license exceptions but may request assistance from Campus export control personnel with these determinations.

Section 1.12: International Emergency Travel Assistance and Insurance Program

a. Insurance: The University maintains international travel accident and sickness insurance.
    i. The insurance policy is maintained by UMass Treasurer's Office.
    ii. The insurance policy provides coverage to University Travelers while on approved University Travel to ensure Traveler access to medical support and services to support safety while on international University Travel.

b. Emergency Travel Assistance: The University maintains an emergency travel assistance program, typically associated with the University international travel accident and sickness insurance, to facilitate access to services in support of the health and safety of University Travelers while on University Travel. This program coordinates access to medical care and evacuation support to University Travelers when needed.
    i. University Travelers conducting University Travel to an International Destination may avail themselves of the resources provided by the emergency services provider, such as: obtaining pretravel assistance, downloading their mobile app and enabling location services to receive local alerts, and enabling one-touch emergency calls to the provider.
c. Travelers planning Travel to an International Destination are responsible for reviewing information on the University's emergency travel assistance and international travel accident and sickness insurance program prior to departure.
    i. Information can be obtained through the Traveler's Campus global program office or similar, or from the UMass Treasurer's Office.
d. Travelers are responsible for providing information to the UMass Treasurer's Office when a claim is or is anticipated to be filed.