University of Massachusetts
Amherst • Boston • Dartmouth • Lowell • Medical • Law

Systemwide Travel and Risk Management Advisory Committee (TARMAC)

Criteria for Designation of High-Risk Destinations and Elevated Cybersecurity Risk Destinations

Updated January 10, 2025

I. High-Risk Destinations

TARMAC has set criteria for designating University Travel High-Risk Destinations. High-Risk Destination designations have applicability for all UMass campuses and the President's Office.

High-Risk Destinations are designated as those meeting the following countrywide ratings set by the respective source as denoted in Table 1 below. *Please note: each source title is a link to the source; please click on the link for more detailed information.*

Table 1: High-Risk Destinations

Source	Level	Rating Applicability
US Department of State	4	Countrywide or regional
	3	Countrywide or regional
Healix	5	Countrywide or regional
	4	Countrywide or regional
Centers for Disease Control & Prevention	4	N/A
	3	N/A
Office of Foreign Assets Control	NA	All comprehensively sanctioned countries

In accordance with BOT Travel Policy (T22-066), requests to travel to High-Risk Destinations must be reviewed by the Traveler's respective Campus Travel Risk Review Committee and approved or denied by the respective Campus Travel Risk Approver.

II. Elevated Cybersecurity Risk Destinations

Elevated Cybersecurity Risk Destinations are designated as those as those meeting the following ratings set by the respective source as denoted in Table 2 below. *Please note: each source title is a link to the source; please click on the link for more detailed information.*

Table 2: Elevated Cybersecurity Risk Destinations

Source	Level	Rating Applicability
US Department of State	4	Countrywide or regional
National Security Presidential Memorandum (NSPM)-33	NA	All countries defined in NSPM-33 as a Foreign Country of Concern
Office of Foreign Assets Control	NA	All comprehensively sanctioned countries
Countries with Encryption Restrictions	NA	Countries with encryption restrictions without personal use exemption

In accordance with BOT Travel Policy (T22-066), requests to bring University Devices or Data or access University Data while on travel to Elevated Cybersecurity Risk Destinations must be reviewed by the Traveler's respective Campus Information Technology point of contact (IT POC) before Travel.

The Campus IT POC may permit a Traveler to bring University Devices or Data, or remotely access University Data bring and/or access University Data while on Travel to an Elevated Cybersecurity Risk Destination. Permission may necessitate implementation of mitigation measures as identified by the IT POC. If necessary mitigation measures cannot be implemented, or the Traveler chooses not to implement mitigation measures, the IT POC may deny the Traveler permission to bring University Devices or Data or access University Data while on said Travel.