Augusta University
Policy Library

International Travel Policy

Policy Manager: IT and Research Compliance

POLICY STATEMENT
This policy provides a framework of institutional oversight that promotes the safety and security of all Augusta University (AU) employees and affiliated persons traveling outside the United States on AU official business, AU-sponsored travel, in their role as an AU employee or representative, or in support of AU-directed activities, and **may** in certain circumstances apply to **personal travel**. This policy promotes measures that protect AU devices, AU assets, AU intellectual property, and sensitive AU institutional data. This policy also protects the security of AU's information systems and research data while fostering international collaborations and associated international travel.

International travel is conducted by AU employees, AU graduate and undergraduate students, AU fellows and visiting research persons, and AU affiliated persons for many worthwhile and beneficial purposes to support the mission of AU, particularly in the area of research. However, international travel can pose a risk to the integrity of electronic devices and the information systems to which they connect, as well as a risk to the security and protection of AU intellectual property and AU institutional data. For that reason, all international travel must be reviewed and approved in advance in compliance with AU policies and HR Work Rules.

Additionally, AU is committed to adhering to federal export-control laws and protecting all sensitive (SEI) and confidential information to include Protected Health Information (PHI), information protected under the Family Educational Rights and Privacy Act (FERPA), proprietary data or other research information or results, and/or regulated data by implementing physical security standards within facilities and within areas of a facility that contain or provide access to such information.

AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☐ Vendors/Contractors ☒ Visitors
☒ Other: Any associated AU affiliate assigned AU devices or retaining any sensitive information on behalf of AU.

DEFINITIONS
Covered Individual – Any individual who is an AU employee (faculty or staff), AU students, an unpaid AU adjunct faculty member, any unpaid person (including a postdoc or fellow) who has an AU email account and access to AU systems or AU institutional data, or any individual who is engaged in any activity on AU campus or in AU facilities pursuant to a visa sponsored by AU.

Covered International Travel – Any international travel outside the United States (A) by Covered Individuals who are traveling for AU business, teaching, conference attendance, research purposes, or who have receive offers of sponsored international travel for research or professional purposes; or (B) by Covered Individuals for which the traveler proposes to (i) access AU information systems while traveling,

and/or (ii) travel with an AU device (i.e. laptop), and/or (iii) travel with sensitive AU data. Covered International Travel does not include personal travel by a Covered Individual.

Personal Travel – Travel by a Covered Individual that is travelling for personal reasons and who (i) is not receiving any support for their travel from any person or organization, (ii) is not receiving any compensation from AU or any other person or organization during their travel, (iii) is not traveling with an AU device, and (iv) is not traveling with AU sensitive data.

Multifactor Authentication (i.e., Duo): Access security product used to verify a user's identity at login. It adds two or more identity-checking steps to user logins by use of secure authentication tools.

Loaner Device: Any AU computer laptop or similar electronic device provided for temporary use to a Covered Individual only during international travel, and which will have a limited user application set.

Sensitive AU data: Sensitive (SEI) and confidential information, including but not limited to Protected Health Information (PHI), information protected under the Family Educational Rights and Privacy Act (FERPA), information protected under HIPAA, AU intellectual property, and unpublished research data.

TRAVEL APPROVALS AND REVIEWS

All Covered Individuals planning to travel internationally are required to do the following **before their travel begins:** (1) obtain written pre-approval for their travel in accordance with AU and Board of Regents requirements; (2) submit a pre-travel expense authorization form as required by AU and Board of Regents policies if they wish to receive travel reimbursement from AU; (3) submit a request for Outside Professional Activity if travelling internationally but not on Personal Travel and/or not travelling on AU business; and (4) obtain a Travel Security consultation if the Covered International Travel will involve use of an AU device, travel with AU data, or access to AU electronic systems while traveling.

In addition, all Covered Individuals who intend to engage in Covered International Travel must review the following and comply as appropriate:

Travel Security Consultation

If any Covered Individual intends to travel internationally with an AU device, travel with AU data, or access AU systems while traveling, they must consult **before** their travel begins with both:

1) AU's Research Security Officer for a Travel Security Consultation (the consultation must be **in-person** for travel involving US State Department Category 3 and 4 countries), and

2) AU's IT Cyber Defense.

The recommendations developed from the Research Security consultation and the AU IT Cyber Defense consultation will be provided to the traveler and their supervisor to aid in planning.

Covered Individuals are advised that federal laws deem that all information or materials in any form (physical, digital, personal knowledge) taken outside the US is an export. Some exports require an export

license prior to carrying/shipping/transmitting it outside the US. Some activities in Category 3 and 4 countries, e.g., teaching or presenting at a professional conference, may also require an export license. If it is determined that an export license is required for your travel, the Research Security Officer in consultation with Legal Affairs will provide guidance on how to obtain the appropriate license(s). This process may take as long as 6-12 months; additional time should be considered when planning international travel.

Additional Considerations:

Individuals are encouraged to consult the Department of State Travel Advisory Level prior to international travel for information related to travel health, safety and security. Individuals are encouraged not to travel to any country with a State Department "Do Not Travel" Level 4 Advisory for any reason.

Covered International Travel is **prohibited** in country that (i) is on the US State Department's List of "Countries of Particular Concern"; or (ii) at the time of travel has a Level 4 Advisory from the US State Department; unless a travel request has been approved in writing and in advance by the Covered Individual's supervisor, the appropriate Dean, **and** the Provost or the President.

Use of AU devices and access to the AU network or AU data is **prohibited even on personal travel** for any member of the AU community in country that (i) is on the US State Department's List of "Countries of Particular Concern"; or (ii) at the time of travel has a Level 4 Advisory from the US State Department; unless use of AU devices or access to the AU network or AU data has been approved in writing and in advance by the Covered Individual's supervisor, the appropriate Dean, **and** the Provost or the President.

US citizens that are travelling internationally are encouraged to register their travel with the State Department (https://travel.state.gov/content/travel/en/international-travel/before-you-go/about-our-new-products/staying-connected.html) in order to receive timely updates on safety and security information.

Electronic Devices and AU Systems Security:

Covered Individuals are responsible to ensure the confidentiality, integrity and security of all AU devices, data, and resources while engaged in Covered International Travel. Removing unnecessary confidential or sensitive data from any device reduces the risk of exposure to anyone gaining access to the information.

No AU devices are permitted to be taken to any destination where doing so is prohibited by export control laws (i.e. OFAC sanctioned destinations). Devices found to violate this will be locked from use and blocked from connecting to the AU network until the device is returned to campus and reviewed by Cyber Defense.

Covered Individuals are responsible to ensure a destination country does not have encryption import restrictions. If encryption tools are restricted in the destination country, AU's IT may be able to provide a loaner device that can be configured for use in the destination country.

There is no guarantee that a Covered Individual's AU-owned device will be approved for travel, and all individuals are therefore encouraged to obtain a temporary loaner device from IT to be purposed for travel to their desired destination(s).

Network connectivity when traveling is a potential security risk to AU resources. During international travel, travelers must:

- Validate that all connections are to legitimate networks, especially wireless networks by verifying valid network(s) names and passwords with official representatives of businesses, hotels, universities, etc. for use.
- Turn off wireless connectivity when the device is not in use or network connectivity is not required.
- Do not automatically join any wireless networks. Choose networks manually every time.
- **Never** provide another person or entity with your DUO Multi-factor access code at any time.
- AU reserves the right to terminate access to the AU system, restrict access to AU data, and/or inactivate remotely any AU device while an AU community member is traveling if AU deems there is a risk to the university or a violation of this policy.

Upon return to the US from Covered International Travel, all persons are encouraged to contact IT immediately upon return to ensure that any AU device that was taken outside the US is safe to connect back to the AU network.

If an AU device is lost, out of physical control of Covered Individual or there is any suspected inappropriate access to AU data the Covered Individual should immediately notify the AU Police Department at (706)721-2911 and AU Cyber Defense at (706)72-CYBER.

All Covered Individuals are encouraged to carefully review the following resources:

REFERENCES & SUPPORTING DOCUMENTS
Office of Foreign Assets Control

US State Department

Countries of Particular Concern, Special Watch List Countries, Entities of Particular Concern

RELATED TRAVEL AND CONFLICT OF INTEREST POLICIES
Individual Conflict of Interest Policy

Outside Activities and Off-Campus Duty

https://www.usg.edu/business_procedures_manual/section4/\

https://sao.georgia.gov/travel/state-travel-policy

RELATED TRAVEL FORMS AND RESOURCES
Travel Authorization Form

DUO International Access Request

AU Travel Office

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 5/10/2023

President, Augusta University Date: 5/10/2023