Standard PR.IP: International Travel and use of Education IT Services

September 24, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.09.24 12:24:50 -04'00'

Steven Hernandez **Date**

Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	8/5/2020	Initial draft
1.1	9/24/2020	Revised draft and updated format
1.2	10/21/2020	Updated section 2.1 Device International Travel Requirements section
1.3	11/13/2020	Revised draft to include section 2.3.1
1.4	11/18/2020	Revised draft to include note section in section 2.1.
1.5	12/8/2020	Updated section 2.2.2 to include Alias Email and Network Accounts
1.6	12/14/2020	Updated section 2.3 – Country Designations.
1.7	12/30/2020	Revised draft to include section 2.2.2.
1.8	1/11/2021	Updated sections 3 to include section 3.1- Security Practices During Travel
1.9	2/19/2021	Revised draft to include updated Risk Acceptance and Policy exception.
1.10	2/24/2021	Updated section 2.1 and 2.2 with rewording language.
1.11	3/24/2021	Updated section 2.4.1 and 2.4.2 with submission of EDSOC FTR process.
1.12	4/9/2021	Updated section 3.2 to combine copy of device data.
1.13	4/19/2021	Removed 2.4.1 and 2.4.2 from device section.
1.14	5/4/2021	Updated language in Section 1.2 and revised Section 2.2 to include Non-Sensitive Country List and Sensitive Country List titles. Added Section 4 – Noncompliance.
1.15	5/27/2021	Revised changes to all sections as well as changing focus from GFE to services
1.16	6/28/2021	Added 2.2.3 Other Country List (OCL) and updated section 3.1 during travel.
1.17	7/21/2021	Updated request days in 2.2.1 and 2.2.2
1.18	9/24/2021	Reviewed for accuracy

Table of Contents

1. INTRODUCTION

1.1 Purpose

This document establishes the Department of Education (ED) policy for authorizing Government Furnished Equipment and Services (GFES) usage while on travel outside of the United States and its territories. These services include ED email on privately owned devices, as well as for connecting GFES to ED information systems and networks while traveling internationally. In doing so, this document supersedes any prior documentation establishing such policies.

1.2 Scope

The standards established in this document apply to all ED employees, contract personnel, consultants, licensees, and any person or entity using, consuming, providing, operating, maintaining, or supporting ED information systems GFES to conduct official ED business.

As defined by OCIO: 3-112, *Cybersecurity Policy*, GFES are materials, equipment, services, identities, and information furnished by the Government to employee(s) or contractor(s). The following types of GFES equipment are governed by this standard:

- Laptops and IT devices, accessories, and peripherals
- Mobile devices including phones and tablets
- Bring Your Own Device (BYOD) devices

IT Services governed by this standard include but are not limited to:

- ED email,
- Remote desktop services,
- Microsoft Teams or comparable authorized virtual presence services,
- Video teleconferencing,
- Screen sharing,
- Two-factor authentication for other government systems,
- Any services permitting a user to conduct official ED business by or on behalf of the Department.

2 STANDARDS

2.1 Foreign Travel Authorization

ED GFES may be taken (equipment) or used (services) outside of the United States and its territories only after explicit authorization via the Foreign Travel Request (FTR) form. This form is meant for temporary travel, for a duration of up to 60 days and is not to be used for any changes of duty stations or remote work situations. GFES requests are not authorized for permanent relocations or changes in duty office to foreign countries, nor can GFES be used or provided to personnel residing in foreign countries.

Completed FTRs must be submitted to the ED Security Operations Center (EDSOC), (EDSOC.ed.gov) for processing prior to departure according to a timeframe determined by the destination country (see Section 2.2 below for information about destination countries). Federal Student Aid (FSA) users must also notify the FSA SOC (FSASOC@ed.gov) of all foreign travel requests. FTRs received by the EDSOC that are missing required data or signatures will be returned to the requestor for completion.

The destination country's sensitivity designation determines how far in advance of scheduled travel the form must be received by the EDSOC and determines the level of information that is required from the user.

The ED Chief Information Security Officer (CISO) or Designated Approving Authority will approve or disapprove all requests on a case-by-case basis. Decisions will be communicated to users via the EDSOC. If a user has received approval from the EDSOC, the user must inform their Information System Security Officer (ISSO) of their travel no later than ten (10) business days prior to travel to a NATO member country and twenty (20) business days prior to travel to any other foreign country The ISSO's primary responsibility is to provide additional information to the EDSOC regarding a user's travel, if requested by the EDSOC.

2.2 Country Designations

Country sensitivity designations are used to determine the level of risk when traveling with ED GFES outside of the United States and its territories.

2.2.1 NATO Member Country List (NMCL)

NATO[1] member countries have been deemed to present a lower risk to GFES. Any country which is a member of NATO is considered a non-sensitive country.

Any user traveling to a non-sensitive country with a standard GFES device must complete the FTR (see Section 2.1) and submit the completed form to the EDSOC, EDSOC@ed.gov, and must notify their ISSO at least ten (10) business days prior to travel. Any requests submitted less than **10** business days before travel may be denied.

Emergency requests will be considered for priority processing.

The NATO member country list can be found here.

2.2.2 Sensitive Country List (SCL)

SCL countries are high-risk for GFES and are designated as sensitive based on reasons of national security, nuclear proliferation, regional instability, threat to national economic security, or terrorism concerns. The Department's SCL includes countries listed by the Department of

[1] https://www.nato.int/cps/en/natohq/nato_countries.htm, https://nato.usmission.gov/about-nato/#member

Energy[2]. The EDSOC may deny or specify additional security controls for GFES requests for travel to countries considered sensitive.

The SCL Country list can be found here. Any user traveling to a sensitive country with GFES device must complete the FTR (see Section 2.1) and submit the completed form to the EDSOC, EDSOC@ed.gov, and must notify their ISSO at least twenty (20) business days prior to approved travel. Any requests submitted less than **20** business days before scheduled travel may be denied. Users will be issued alternate hardened equipment with alias accounts and limited information necessary for travel.

Emergency requests will be considered for priority processing.

2.2.3 Other Country List (OCL)

Travel to countries that are not a member of NATO nor on the Sensitive Country List will be considered on a case-by-case basis. Many factors will be considered when reviewing potential travel to the countries, to include Department of State[3] travel advisories or bulletins, offensive cyber capabilities, threat intelligence reporting from DoD, DHS, or other federal partners, or other geo-political factors. The EDSOC may require the use of a hardened[4] loaner device and alias accounts when traveling to destinations on the OCL.

Any user traveling to a OCL country must complete the FTR (see Section 2.1) and submit the completed form to the EDSOC, EDSOC@ed.gov, and must notify their ISSO after FTR approval but prior to approved travel. Any requests submitted less than **20** business days before scheduled travel may be denied. In most cases, users will be issued alternate hardened equipment with alias accounts and limited information necessary for travel.

Emergency requests will be considered for priority processing.

2.3 Assigned GFES

At the EDSOC's discretion, the EDSOC may scan all devices prior to travel and conduct or coordinate activities required to ensure the assigned GFES is authorized for foreign travel, properly configured, and secured before travel begins. All GFES laptops must have an approved Department VPN installed prior to traveling. Users are required to ensure connection and operability of their devices and the VPN solution before travel. Department provided GFES equipment returning from foreign travel may be scanned and imaged in accordance with department policy and posture or at the request of the EDSOC.

---

[2] https://site-security.lbl.gov/resource/personnel-security-resources/foreign-visits-assignments/sensitive-countries/
[3] https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/
[4] "Hardened" is a term used to refer to devices that have been reviewed from a cyber security standpoint, had unnecessary features removed, only operates with the minimum amount of user level services and programs, or only is running the absolute minimum number of programs required for Department mission requirements. Removal of non-critical software or features lessens the attack surface for an adversary.

2.4 Hardened Devices, Alias Email and Network Accounts

Standard issued GFES must not be taken or used in any country on the Department's sensitive country list. Users traveling to a country on the Department's SCL *are required* to use a separate hardened device with a temporary network and email alias for the duration of travel.

Users traveling to a country on the Department's OCL *may be required* to use a hardened device with a temporary network and email alias for the duration of travel at the discretion of the EDSOC.

When the EDSOC receives a completed FTR at least 20 days prior to the date of departure, the EDSOC will determine if hardened equipment and alias accounts need to be issued and assigned. The EDSOC will coordinate with our service partners to attain hardened equipment and alias accounts for the requester if required.

Any requests submitted with less than **20** business days before scheduled travel may be denied. If there are no hardened devices available for SCL travel, the EDSOC has the discretion to reject the GFES travel request.

Users whose GFES travel request has been approved will be issued hardened devices by the EDSOC. Only these hardened devices are authorized to connect to the Department's systems and networks while traveling outside the United States. Alias accounts are specifically configured to restrict access to the user's assigned ED network account and limit access to Department data and network during travel.

After the FTR has been approved, the EDSOC will work with users to ensure the user information and accounts necessary for use while on travel are transitioned to the alias account, as well as assisting with any new equipment or security controls required. Once the user returns from travel, the EDSOC will assist the user with transferring information or account access back to their regular GFES. Users are responsible for testing and troubleshooting alias accounts with the hardened device prior to departure. Hardened devices are retrieved when the user returns, inspected for malware/tampering, and all temporary alias accounts are deactivated after transferring user data to standard accounts.

Emergency requests will be considered for priority processing.

3 DEVICE PROTECTION

3.1 During Travel

Department users must maintain possession of GFES during international travel. GFES must not be placed in checked luggage and must not be left unattended. GFES must be turned off when not in use. All users must utilize secure remote access via an ED authorized VPN or authorized service during travel.

Any loss, compromise, suspected compromise, or unauthorized access to GFES must be reported immediately to the EDSOC (EDSOC@ed.gov) in accordance with incident reporting requirements.

Please note: GFES may not be used in route to the user's destination unless noted in the FTR

3.2 Return from Travel

Immediately upon return from travel, and at the discretion of the EDSOC, all GFES taken outside of the United States and its territories may be scanned and imaged by the EDSOC for malicious or suspicious activity (including, but not limited to, tampering and/or malware). This may involve physically shipping or bringing the GFES to a Government facility. Users must not connect GFES used to support foreign travel to the ED local network until the EDSOC analysis has been completed. Users must submit a request to the EDSOC, through EDSOC@ed.gov, to coordinate submitting the GFES to the EDSOC for inspection.

All hardened GFES will be scanned and imaged by the EDSOC and all information on the GFES will be deleted before being placed back into production. To obtain a copy of any data on a hardened GFES, a request must be sent to the EDSOC prior to the device being sanitized. The EDSOC will deliver the data to the user once confirmed there is no malware or indications of compromise.

4 NON-COMPLIANCE

Failure to comply with this standard may result in disciplinary action. Additionally, the Department may take one or more of the following actions:

- Immediately disconnect any unauthorized connections from foreign countries.
- Disable the user's account and GFES immediately. The user's GFES will only be re-enabled once the GFES has been retrieved by the EDSOC and a forensic scan has been performed to ensure that no malicious activity has occurred.

Any user found to exceed their approved dates may have their GFES disconnected from the network and their accounts disabled. The EDSOC is the primary authority on decisions regarding user account and GFES disablement.

5 RISK ACCEPTANCE AND POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures, or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO or his delegate. Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not

introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).