STATEWIDE STANDARD ADDENDUM (8350): OUT OF COUNTRY EXCEPTION REQUEST

DOCUMENT NUMBER:	**A8350**
EFFECTIVE DATE:	**December 11, 2024**
REVISION:	**1.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Homeland Security, the Agency shall establish a coordinated plan and program for information security and privacy protections implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 41-4254 and § 41-4282.

2. PURPOSE

The objective of this State policy addendum is to establish guidelines for the submissions, management, and approvals/denials of Out of Country Exception Request (OOCE). This will ensure that all official State travel out of the country is aligned with department goals and State legal requirements. This policy promotes safety, accountability, and recognition of associated risk while supporting official international engagements that advance the State's interest in key areas.

3. SCOPE

3.1 Application to Budget Units (BU) - This policy shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 Application to State Employees - This policy shall apply to all State employees and contractors.

3.3 Application to Systems - This policy shall apply to all agency systems:

- **a. (P)** Policy statements preceded by "(P)" are required for agency systems categorized as Protected.
- **b. (P-PCI)**Policy statements preceded by "(P-PCI)" are required for agency systems with payment card industry data (e.g., cardholder data).
- **c. (P-PHI)** Policy statements preceded by "(P-PHI)" are required for agency systems with protected healthcare information.
- **d. (P-FTI)** Policy statements preceded by "(P-FTI)" are required for agency systems with federal taxpayer information.

3.4 Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services

a. BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services, BU SMEs shall consider statewide information security PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

4.2 BU has taken the following exceptions to the Statewide Policy Framework:

Section Number	Exception	Explanation / Basis

5. DEFINITIONS

5.1 **C-Suite Executives:** This is the classification of State employees who are high level senior executives that hold specific titles. These executives are responsible for overseeing departments, operations, and performance of their agency. Common titles are Commissioner, Deputy Director, Chief of Staff, Chief Financial Officer, Chief Operating Officer, Chief Information Officer, etc.

6. ROLES AND RESPONSIBILITIES

6.1 Arizona Department of Homeland Security (AZDOHS):

a. AZDOHS is responsible for reviewing all OOCE submissions, management of the tickets submitted in ServiceNow for the OOCE's, and presenting threat intelligence briefings to the traveling employee.

6.2 BU Directors:

a. All agency Directors and C-Suite executives are responsible for accepting any risk that may be associated with the employee's travel overseas.

b. All agency Directors and C-Suite executives are **required** to attend a threat briefing pre-travel and post-travel that pertains to the foreign country of travel.

6.3 Supervisors of agency employees and contractors:

a. Managers from the employee's agency are **required** to notify their agency Information Security Officer (ISO) about the requested travel.

b. Submitters of overseas travel requests must be submitted by the employee's agency ISO.

6.4 BU employees and contractors

a. All Arizona State employees who need to conduct foreign travel overseas for official State business are **required** to notify their manager of the travel.

7. POLICY

7.1 Submissions

7.1.1 Prior to submission of OOCE, ensure that form GAO-75: Request to Work Outside of Arizona has been completed, submitted, and approved.

7.1.2 Employees who need to travel overseas on official State business must send an email to their direct supervisor/manager **notifying them 45 - 60 days prior** to the upcoming travel.

7.1.3 Agency managers will forward the notification email to their agency ISO and request that the agency ISO complete an OOCE through ServiceNow.

7.1.4 Agency ISO's will fill out the OOCE form through ServiceNow **no later than 30 days prior** to the travel. All the information about the travel must be included on the ticket and the approved GAO-75 form must be attached to the ticket.

7.1.5 Any OOCE that is submitted with less then 30 days of notice will require the agency Director or Deputy Director to email the azsoc@azdohs.gov with justification as to why the request was not submitted 30 days prior (emergency request, mission critical, etc).

7.1.6 Agency Directors and C-Suite executives are still required to follow the above notification windows. In addition, they are required to attend a foreign threat travel pre-briefing and post-briefing with the AZDOHS. These briefings will be held either in person or virtually depending on the foreign location of travel.

7.2 Management

7.2.1 AZDOHS is responsible for the management of all submitted OOCE's through ServiceNow, threat briefings, and configuration changes.

7.2.2 Upon official notification of the travel AZDOHS will comment on the ServiceNow ticket that the request has been acknowledged and is currently under review.

7.2.3 An AZDOHS employee from the Arizona Security Operations Center (AZSOC) will then start analyzing all local laws, threats, and risks associated with the foreign country of travel. The AZDOHS employee will then collaborate with the Arizona Counter Terrorism Information Center (ACTIC) to conduct a threat analysis.

7.2.4 AZDOHS will comment on the OOCE ServiceNow ticket 1 week prior to the travel of the approval or denial of the requested travel.

7.2.5 Once the AZSOC has commented on the ticket, if approved, AZDOHS will make the configuration changes in Okta for the traveling employee.

7.2.6 All OOCE ServiceNow tickets will be left in the "in progress" or "open" status after the approval until 1 day after the end date of the foreign travel.

7.3 Approvals/Denials

7.3.1 The AZSOC is the first approving official in the OOCE process.

7.3.2 Once approval from the AZSOC has been entered on the ticket it will be sent to the Arizona State Chief Information Security Officer (CISO) and the State Chief Information Officer (CIO) for their approval as well.

7.3.3 Once the State CISO and State CIO have approved of the OOCE, AZDOHS will make the Okta configuration changes to the traveling employee's account.

7.3.4 Below is a following description of the denial criteria for submitted OOCE:

a. Any request submitted less than 2 business days prior to the travel regardless of mission criticality or an emergency request will be denied.
b. Any request with no approved GAO-75 form attached.
c. Any request that is for personal leisure travel (Agency Director's and Deputy Director's will be exempt from this denial criteria).
d. Any request that is submitted less than 30 days prior to travel and does not have justification from the agency Director or Deputy Director will be denied.
e. Any travel to a Level 4 DO NOT TRAVEL country listed under the U.S. State Department's website will be denied.
f. Any travel to a foreign country that has been determined by AZDOHS and the ACTIC to be of significant risk to the employee or the Arizona State network will be denied.

8. ADDITIONAL DEFINITIONS AND ABBREVIATIONS

8.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

9. REFERENCES

9.1 STATEWIDE POLICY FRAMEWORK 8350 SYSTEM AND COMMUNICATIONS PROTECTION

9.2 Statewide Standard 8350, System and Communication Protection

9.3 Statewide Policy Exception Procedure

9.4 National Institute of Standards and Technology, Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020.

9.5 US State Department Travel Advisories: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

9. ATTACHMENTS

None

10. REVISION HISTORY

Date	Change	Revision	Signature
12/11/2014	**Initial release**	**1.0**	