NASA Procedural Requirements

NPR 2810.2
Effective Date: October 29, 2019
Expiration Date: October 29, 2024

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Subject: Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories (Updated with Administrative Change 1)

Responsible Office: Office of the Chief Information Officer

Chapter 1. Requirements

1.1 Introduction

a. NASA information, information technology (IT) and information systems, and the accounts that access these systems, must be protected. This NPR outlines requirements for protecting NASA information, IT and information systems while NASA personnel are outside of the U.S. and U.S. territories.

b. The use of mobile devices to transmit or receive information makes the transmitted information susceptible to eavesdropping, interception, and theft because of transmissions occurring over commercial networks. International travel increases these risks, particularly where telecommunication networks are owned or controlled by the host government. IT devices are always at risk for the introduction of malicious software and such risks are greater when devices leave the physical control of the traveler.

1.2 Use of NASA Information When on Official Travel

a. NASA travelers shall physically take only the minimum amount of NASA non-public information that is required to accomplish official duties on international travel.

b. Travelers shall not take their primary NASA computer unless the information stored on that computer is required for their official duties, is specific to the purpose of the international travel event, and is not readily accessible by other NASA-approved means.

c. NASA personnel on official international travel shall store NASA data only on authorized NASA devices. Computers used on official international travel must comply with all NASA requirements for the protection of sensitive information, including encryption requirements. Special handling may be required for data that is protected under export control and ITAR, as well as any personally identifiable information (PII), sensitive but unclassified (SBU), or controlled unclassified information (CUI).

d. Prior to official international travel, NASA personnel shall contact their Center Chief Information Officer's (CIO) office for assistance to back-up appropriate information. This backup is critical for data identification and recovery in the event of compromise, loss, theft, etc., of the traveler's IT device(s).

e. For NASA personnel who have the NASA Mobile Device Management (MDM) application installed on their personally owned devices, they shall not access the MDM application from a personally owned device while outside the U.S. and its territories.

1.3 Use of NASA Information Technology When on Official Travel

a. Prior to travel, NASA official international travelers shall contact the Center CIO for guidance on obtaining a NASA authorized IT device specifically designated and configured for NASA use while on official international travel, such as a loaner laptop, loaner tablet, or loaner smartphone.

b. NASA official international travelers shall take NASA IT devices or access NASA accounts only when authorized by the Center CIO or their designee, prior to travel.

c. NASA official international travelers shall use only authorized NASA IT devices to store, process, transmit, and access NASA information.

d. NASA official international travelers shall understand and comply with the Center guidelines for returning all IT devices used on international travel for assessment and verification to safely reconnect to NASA IT systems and networks, before reconnecting any device to a NASA network. The traveler shall not connect any NASA IT device used on international travel to NASA internal networks until cleared by the Center CIO.

e. NASA official international travelers shall, prior to mailing any IT equipment which contains NASA owned information to a foreign country, obtain approval from both the Center Export Control Administrator and the Center CIO. This requirement applies to computers and other devices, as well as portable and detachable media storage devices, such as USB drives. f. NASA official international travelers shall ensure that all NASA IT devices containing NASA information remain in their possession and are appropriately safeguarded while outside the U.S. and U.S. territories.

g. NASA official international travelers shall report any loss, damage, tampering, or suspected tampering of NASA IT devices or any IT devices containing NASA information to the NASA Security Operations Center (SOC), soc@nasa.gov, or call 877-627-2732, no later than 24 hours after the incident. Travelers shall ensure they know the dialing instructions to dial the United States from the visited foreign country prior to travel. Travelers are strongly encouraged to store this contact information separately for access if the device is compromised.

h. NASA official international travelers shall not connect any devices received from foreign national personnel to NASA networks. If using a detachable media storage device, such as a USB drive to present NASA data at an event such as an international conference presentation, NASA travelers shall not reconnect the detachable media storage device to the NASA IT device after the presentation. If collective presentations are provided via detachable media storage, these shall be cleared by the Center CIO before being accessed on a NASA IT device.

1.4 Accessing NASA Networks and Information Systems When on Official Travel

a. NASA travelers shall only access, from outside the U.S. and its territories, any NASA IT information or systems, through:

(1) Authorized secure access to NASA's internal systems, networks, and data from a NASA IT device authorized for international travel, using access guidance provided by the Center OCIO.

(2) Access to systems, networks, and data specifically intended for access by the general public (e.g., publicly accessible Web sites).

1.5 Engagements with United States Customs and Border Protection (CBP) Personnel or Foreign Authorities

a. All individuals traveling with authorized NASA IT devices shall observe the following requirements when entering or exiting the U.S., U.S. territories, or any other country, and during encounters with any customs officials or border control authorities.

(1) If U.S. CBP personnel or foreign customs or border authorities confiscate or attempt to confiscate a NASA-issued IT device, NASA personnel shall show their NASA credentials and request to retain custody and control of the device, noting that the device in question is the property of the U.S. Government.

(2) If the U.S. or foreign authorities insist on examining or confiscating the device, NASA personnel shall comply with the request to surrender the device.

(3) If U.S. CBP personnel or foreign customs or border authorities request access information for the NASA IT device, such as user identification or password, NASA personnel should restate their official status and that the device in question is the property of the U.S. Government.

(4) If the U.S. or foreign authorities insist on the device access information, NASA personnel shall request to input the information directly onto the device. If required, NASA personnel shall provide the access information to the U.S. or foreign authorities.

(5) If the device is returned, NASA personnel shall not unlock or open the device until it is returned to the issuing

Center.

(6) NASA travelers shall request the return of the NASA IT device following the surrender and examination of the device by U.S. or foreign authorities. If the device is not returned, NASA personnel shall proceed with their travel and notify the SOC.

b. Within 24 hours, travelers shall report any incident involving a NASA IT device, including an encounter with U.S. and/or foreign authorities, to the NASA SOC and the traveler's supervisor. An incident is any instance in which 1) the device is removed from the traveler's line of sight for any length of time, whether returned or not, or 2) the password is used to access the device at the behest of any official other than the traveler.

c. The NASA traveler's supervisor shall ensure the SOC, Center CIO, Counterintelligence Center, Office of General Counsel, and Center Export Control Manager are notified by the traveler.

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.