International Travel Policy for Mobile Computing Devices

Approved Date – 04/17/2017
Published Date – 04/17/2017
Reviewed Date – 06/07/2024

1. Purpose

Ensure the safeguard of District information and systems for all District workforce members (including contractors, vendors, consultants, temporary staff, interns, and volunteers) while on travel outside of the United States and its territories.

2. Authority

DC Official Code § 1-1402 et seq., provides the Office of the Chief Technology Officer ("OCTO") with the authority to provide information technology (IT) services, write and enforce IT policies, and secure the network and IT systems for the District. This document can be found at: *https://code.dccouncil.us/dc/council/code/sections/1-1402.*

3. Applicability

This policy applies to all District workforce members responsible for application identity and role definition on behalf of the District, and/or any entity who receives any enterprise services from OCTO. In addition, this policy applies to any provider and third-party entity with access to District information, systems, networks, and/or applications.

4. Policy

District agencies and departments must develop or adhere to a strategy which demonstrates compliance with this policy and its related standards. The following outlines the requirements for this policy. The District's agencies must develop and review or update annually and after changes to the policy, a procedure in support of this policy with the following requirements.

4.1. Transport of mobile computing devices via Air Travel:

4.1.1. In most cases, the user must follow the Transportation Safety Administration (TSA) recommendation and carry mobile electronic communication equipment (laptops/tablets/phones/mobile) devices onto flights instead of placing them inside checked baggage. A laptop, even if it is in a laptop bag, does not count as a flyer's carry-on item.

4.1.2. Before travel, the user must submit a request to their respective Agency Director. Agency Chief Information Officers (CIO) are responsible for forwarding the request to the Chief Technology Officer (CTO), via the Chief Information Security Officer (CISO). Agency CIOs must implement a process to ensure the user's compliance with paragraph 4.4. The device user must follow all current U.S. Department of State travel advisories, which can be found at https://travel.state.gov/traveladvisories.

4.2. VPN Usage

All devices connecting to the DC networks must connect using the OCTO configured DC VPN. VPN connections and devices are an extension of the network and are subject to the same rules and regulations that apply to DC government-owned equipment.

4.2.1. VPN connections from outside of the United States and its territories are blocked by policy. Users wishing to establish a communication outside of the United States and its territories must create a ServiceNow ticket to the Security Operation Center (SOC) via their Agency CIO.

4.2.2. Requests are limited to the duration of each trip with exact dates of travel provided in the travel request.

4.3. Personal Travel

Personal travel with and use of government-issued equipment (laptops, tablets, or smartphones) is not recommended. If required, take only devices required to maintain communications (e.g., government phone). This will minimize the opportunity for government issued equipment and data to be lost or stolen.

4.4. Business Travel

Business travel requires that the user utilize government-issued equipment only for business functions. Prior to traveling, all devices must be reviewed for sensitive data, such as Personal Identifiable Information (PII) and Protected Health Information (PHI). All data not required for the purposes of the travel to perform business functions should be removed from the device. The following requirements must be met when using government-issued devices when on travel:

4.4.1. Virtual Private Network (VPN): All users must follow the VPN policy when connecting to the network. VPN use is required for all devices (i.e., laptop, tablet, smartphone) at all times unless the device is put into “Airplane Mode”. The user must always use the VPN, even when not accessing the internal network, to reduce the risk of intercepted connections. DC VPN solutions and software purchased by DC GOV will not be installed on personal devices without prior written approval from the CISO.

4.4.2. Smartphones.

- Before departure, review devices to ensure removal of any sensitive data (e.g., PII, PHI, etc).
- Before departure, collaborate with the Agency Telecom Coordinator (ATC) to ensure that District Mobile Device Management software (e.g., Microsoft Azure, Intune) is installed and configured properly to ensure remote wipe, password reset, and allowing the device(s) to be placed in “Lost Mode”.
- While on travel, use only Wi-Fi connections provided by known and legitimate providers (e.g., hotel, business centers). Avoid using Wi-Fi in areas of unknown security.
- While on travel, if accessing the network, use the OCTO authorized and installed DC Enterprise VPN Client (e.g., Zscaler, Pulse Secure).

4.4.3. Laptops/Tablets.

- Before departure, review devices to ensure removal of sensitive data (e.g. PII, PHI, etc).
- Before departure, ensure the device has been encrypted using OCTO authorized Full Disk Encryption (FDE) technology.
- Before departure, ensure the device has the latest OCTO/Agency Management and Anti-Virus software (e.g., Ivanti, CrowdStrike) with the latest device updates, and anti-virus have been applied.
- Before departure, the user must ensure their password meets District guidelines for length and security.
- Ensure the device screen is locked and password protected, or powered off when not under the user's direct control.
- When traveling in a Level 1 or 2 country, as identified by the US Department of State, ensure that the laptop/tablet is physically locked in a private secure environment (e.g., hotel safe) when not under the user's direct control. When in a Level 3 or higher country, it is highly recommended that laptops and tablets remain in the user's immediate control and presence at all times. Explanations of the US State Department travel advisory levels and risk indicators can be found at https://travel.state.gov/content/travel/en/international-travel/before-you-go/about-our-new-products.html
- Ensure the use of Multifactor Authentication has been enabled and is in use before traveling outside of the United States.
- While on travel, use only Wi-Fi connections provided by known safe operators (e.g., hotel, business centers), and avoid using Wi-Fi in areas of unknown security.
- While on travel, if accessing the network, use the OCTO authorized and installed DC Enterprise VPN Client (e.g., Zscaler, Pulse Secure).

4.5. Cyber Security and Counter-Intelligence Threats

Cybersecurity and counter-intelligence threats are higher outside of the United States and require higher-level security precautions. Historic reports indicate that users should not expect that devices outside of their direct control are secure, and because of known threats, the following precautions within this section should be followed. Review and adhere to travel bans issued by the US Department of State, which can be viewed with an interactive map at https://travelmaps.state.gov/TSGMap/

4.5.1. Personal travel: When traveling to a country that the US State Department identifies as a higher-level security concern, travel with, and use of government-issued equipment (laptop, tablets, or smartphones) is strongly discouraged.

4.5.2. Business travel: When traveling to a country that the US State Department identifies as a higher-level security concern, District issued equipment (laptop, tablet, or phone) must not be taken or utilized without Agency Director and CTO approval. Agency CIOs must be responsible for forwarding the request to CTO, via the CISO, and must implement a process to ensure the device user's compliance with requirements outlined:

- The user may be issued a temporary device (laptop, tablet, phone; available through OCTOhelps or Agency IT Staff) with a tightly secured, minimally capable operating system baseline for the duration of their travel. Agency or District privacy, health, or other sensitive information will not be stored on this device. Upon return, this device will be returned to OCTO or the Agency IT staff to be reimaged using secure erase techniques.
- Before traveling, the user must ensure their password has been changed to meet District policy. Upon return from travel, the user's password must be changed again.
- While in transit to destination and back, connection to the network or VPN is not authorized.
- Connection to District email clients (via OWA or Office 365) is allowed when using MFA (e.g., phone text with one-time access code).
- Connections to other District online resources not hosted within the network (e.g., PeopleSoft, PASS, etc.) that do not use MFA are not authorized.

4.6. Loss of Device

Workforce members who experience a loss of a District-issued mobile computing device (e.g., laptops, tablets, smartphones) or other mobile electronic communication equipment, must immediately report the loss to the main OCTOhelps line via phone, as well as their immediate manager. The user will be provided the OCTOhelps contact information in the automated email to their work account once their travel request is approved so that they can keep it in a safe location while traveling. The Agency CIO will work with the CISO and Agency General Counsel in instances where loss of District sensitive data may have been lost (e.g., PII, PHI, etc).

5. Exemption

Exceptions to this policy must be requested in writing to the Agency's CIO and the request will be escalated to the Chief Information Security Officer (CISO) for approval.

6. Definitions

The definition of the terms used in this document can be found on the *Policy Definitions website*.