International Travel Policy for Mobile Computing Devices

Policy Number:	**OCTO – 7005.1**	**Creation Date:**	4/18/17
		Approval Date:	4/18/17
Effective Date:	4/18/17	**Revised Date:**	4/18/17

1. **Scope/Applicability:** This policy applies to all District of Columbia Government (the "District") issued mobile computing devices (e.g., laptops, tablets, smartphones) or other mobile electronic communication equipment that store, process, transmit, or receive District information.
2. **Authority:** DC Official Code § 1-1401 et seq.
3. **Purpose:** This policy provides procedures for safeguarding District information and systems for all employees, contractors, and other users while on travel outside of the continental United States, Alaska and Hawaii.
4. **Policy:** This policy establishes procedures for safeguarding District information and systems when used on personal and/or business travel.

   4.1. **Transport of mobile computing devices via Air Travel:**

      4.1.1. In most cases, employees shall follow the Transportation Safety Administration (TSA) recommendation and carry mobile electronic communication equipment (laptops/tablets/phones/mobile) devices on to 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. As of March 2017, the U.S. Department of Homeland Security placed restrictions on US-bound flights originating from specific airports (Queen Alia International Airport (AMM), Cairo International Airport (CAI), Ataturk International Airport (IST), King Abdul-Aziz International Airport (JED), King Khalid International Airport (RUH), Kuwait International Airport (KWI), Mohammed V Airport (CMN), Hamad International Airport (DOH), Dubai International Airport (DXB), and Abu Dhabi International Airport (AUH)). Employees travelling from these locations may not transport devices larger than a mobile phone (e.g., Laptops, Tablets, E-Readers, Cameras, Portable DVD players, Electronic game units larger than a smartphone) in the plane cabin; devices must be transported in the cargo hold. Prior to travel, Employees must submit a request to their respective Agency Director. Agency CIOs are responsible for forwarding the request to the OCTO CTO, via the OCTO CISO. Agency CIOS shall implement a process to ensure employee compliance with paragraph 4.4.

   4.2. **VPN usage:** VPN connections and devices are an extension of the DC Enterprise Network (DCEN) 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 continental United States, Alaska and Hawaii are blocked by policy. Employees wishing to establish a communication outside of the continental United States, Alaska and Hawaii must submit a request to the City-Wide Information Technology Security (CWITS) VPN Team (vpn.octo.dl@dc.gov), via their Agency Chief Information Officer (CIO).

      4.2.2. Requests are limited to the duration of each trip.

   4.3. **Personal travel:** When travelling on personal leave, travel with and use of government-issued equipment (laptops, tablets, or smartphones) is not recommended. If absolutely 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:** When travelling for business, employees will travel with government-issued equipment required for the business purpose. All devices must be reviewed for sensitive data (e.g., Personal Identifiable Information (PII) or sensitive government business data); this data shall 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).** When connecting to the DC Enterprise network, VPN use is required for all devices (i.e., laptop, tablet, smartphone). Users shall utilize the VPN at all times, even when not accessing the DC Enterprise Network, to reduce the risk of intercepted connections.

4.4.2. **Smartphones.**

4.4.2.1. Prior to departure, review device to ensure removal of Agency or District sensitive data (e.g., Personal Identifiable Information (PII) or sensitive government business data).

4.4.2.2. Prior to departure, ensure District Mobile Device Management software (e.g, AIRWATCH) is installed and configured.

4.4.2.3. While on travel, use only Wi-Fi connections in known safe areas (e.g., hotel, business centers), avoid using Wi-Fi in areas of unknown security.

4.4.2.4. While on travel, if accessing DC Enterprise Network, utilize the DC Enterprise VPN Client (e.g., PulseSecure).

4.4.3. **Laptops / Tablets.**

4.4.3.1. Prior to departure, review device to ensure removal of Agency or District sensitive data (e.g., Personal Identifiable Information (PII) or sensitive government business data).

4.4.3.2. Prior to departure, ensure the device has been encrypted using Full Disk Encryption (FDE) technology.

4.4.3.3. Prior to departure, ensure the device has the latest OCTO/Agency Management and Anti-Virus software (e.g., LANDESK, McAfee ePO) and device updates and anti-virus have been applied.

4.4.3.4. Prior to departure, employees must ensure their password meets District guidelines for length and security.

4.4.3.5. While on travel, use only Wi-Fi connections in known safe areas (e.g., hotel, business centers), avoid using Wi-Fi in areas of unknown security.

4.4.3.6. While on travel, if accessing DC Enterprise Network, utilize the DC Enterprise VPN Client (e.g., PulseSecure).

4.4.3.7. Ensure that the laptop is always locked up when not under employee direct control (e.g., hotel safe).

4.5. Cybersecurity and counter-intelligence threats are higher in the following countries and require higher level security precautions: Russia, China (including Hong Kong), North Korea, Iran, Iraq, Afghanistan, Syria.

4.5.1. **Personal travel:** When travelling on personal leave, travel with and use of government-issued equipment (laptops, tablets, or smartphones) is not permitted.