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.

4.5.1.1. **Business travel:** When travelling for business to the aforementioned countries, District issued equipment (laptop, tablet, or phone) may not be taken or utilized without Agency Director and OCTO CTO approval. Agency CIOs shall be responsible for forwarding the request to OCTO CTO, via the OCTO CISO, and shall implement a process to ensure employee compliance with requirements outlined in Sections 4.5.1.2 -4.5.1.6. Historic reports indicate that users should not expect that devices outside of their direct control are secure, even when stored in hotel safes.

4.5.1.2. Employees will utilize 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 or sensitive information will not be installed on this device. Upon return, this device will be returned the OCTO or Agency IT Staff to be reimaged using secure erase techniques.

4.5.1.3. Prior to travel, employees shall ensure their password has been changed to meet District policy. Upon return from travel, employee password shall be changed. Use of Multi-Factor Authentication for personal accounts is advised.

4.5.1.4. While on travel, connection to the DC Enterprise Network or VPN is specifically disallowed.

4.5.1.5. Connection to District email clients (via OWA or Office 365) is allowed when using Multi-Factor Authentication (MFA) (e.g., phone text with one-time access code).

4.5.1.6. Connections to other District online resources not hosted within the DC Enterprise Network (e.g., PeopleSoft, PASS, etc.) that do not use MFA are specifically disallowed.

5. **Loss of Device:** Employees who experience a loss of District issued mobile computing devices (e.g., laptops, tablets, smartphones) or other mobile electronic communication equipment shall immediately report the loss to their Agency CIO and Director. The Agency CIO shall contact the OCTO CISO. The Agency CIO will work with the OCTO CISO and General Counsel to determine if there was a loss of District sensitive data (e.g., Personal Identifiable Information (PII) or sensitive government business data).

6. **Policy Maintenance:** OCTO is responsible for the maintenance, administration, and publication of this Policy. OCTO must annually review this policy and update as needed to ensure the policy's technical relevance and regulatory compliance.

7. **Policy Enforcement:** OCTO is responsible for the governance and enforcement of this Policy. DC Agencies must actively participate in the enforcement and audit of this policy when requested by the OCTO.

8. **Exemptions:** None.

9. **Sanctions:** When OCTO discovers non-compliance with this Policy, OCTO will advise the Agency CIO and Director of the non-compliance, and will notify the City Administrator, depending on the severity of the issue. Non-compliance with these guidelines implies tacit acceptance of the risk of District sensitive data (e.g., Personal Identifiable Information (PII) or sensitive government business data) by the Agency Director and Agency CIO. Employees may be subject to further disciplinary proceedings.

10. **Supporting Laws and Regulations:**

10.1. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA).

10.2. Privacy Act of 1974, 5 U.S.C. § 552a, P.L. 93-579.

10.3. HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C.

11. **Reference Documents:**

11.1. Department of Homeland Security, Press Release DTD April 7th 2017 – Aviation Security Enhancements for Select Last Point of Departure Airports with Commercial Flights to the United States

11.2. OCTO 7006.1, Landline Telephone and Mobile Electronic Communications Device Usage Policy

11.3. OCTO 2060.2, Virtual Private Network Policy

11.4. OCTO 2003.2,

11.5. Password Management Policy

11.6. OCTO 1072.0, Telecommunications Service Acquisition Policy

11.7. NIST IR 7298 Revision 2, "*Glossary of Key Information Security Terms*", May 2013.

11.8. NIST SP 800-30 Revision 1, *"Guide for Conducting Risk Assessments"*, September 2012.

11.9. NIST SP 800-46 Revision 1, *"Guide to Enterprise Telework and Remote Access Security"*, June 2009.

11.10. NIST SP 800-53 Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"*, April 2013.

11.11. NIST SP 800-66 Revision 1, *"An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule"*, October 2008.

11.12. NIST SP 800-77, *"Guide to IPSec VPNs"*, December 2005.

11.13. NIST SP 800-113, *"Guide to SSL VPNs"*, July 2008.

11.14. Fact Sheet: Aviation Security Enhancements for Select Last Point of Departure Airports with Commercial Flights to the United States. https://www.dhs.gov/news/2017/03/21/fact-sheet-aviation-security-enhancements-select-last-point-departure-airports

12. **Definitions:** Definitions for OCTO policies can be found in the Policy Glossary Section.

Availability	The property requiring that information system components, data or information will be accessible and available to authorized parties when needed. This is a fundamental security principle. (NIST IR 7298)
BYOD	Bring Your Own Device – Includes any information or communications system generally laptops or mobile phones, owned by a DC Workforce Member or contracted service provider with approved access to 1 or more DC ICT Hosts. (OCTO)
Confidentiality	The property ensuring that information assets are accessible only for reading by authorized parties. This is a fundamental security principle. (NIST IR 7298)
DC Agencies	Includes all District of Columbia Government organizations accessing the DC ICT Ecosystem. (OCTO)
DC Assets	All DC Government devices, security devices, hosts and data.
DC ICT Ecosystem	The DC Information and Communications Technology Ecosystem includes the patchwork of DC Agencies, Workforce Members, Hosts and ICT Policies for On-Network, Off-Network / Cloud and BYOD. (OCTO)
DC Networks	All DC Government computer and communications networks including the "Secure" wireless access point.
Hosts	All information and communications systems hardware and software which are part of the DC ICT Ecosystem (on-network, off network, BYOD and accessed by the DC Workforce Members. A host is a type of node that are devices attached to the network, which include but are not limited to desktops, laptops, servers, applications, phones, printers, fax machines. (OTCO)
Integrity	The property ensuring that only authorized parties can modify data or information disclosed in an electronic document. This is a fundamental security principle. (NIST IR 7298)
On-Network (DC Network)	All DC Government computer and communications networks which are part of the DC ICT Ecosystem (ex. Wired, Wireless, VPN)
Off-Network	All DC Government IT Systems and Hosts accessed by DC Workforce Members which are not directly connected to a DC Network (ex. Cloud, SaaS, ASP Service Providers) which are part of the DC ICT Ecosystem.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence. (NIST IR 7298)
Security Team	The OCTO Security Team, formerly City-Wide IT Security (CWITS)
Workforce Members (DC)	Employees, contractors, interns, volunteers, trainees, contracted service providers, and other persons whose conduct, in the performance of work for an organization, is under the direct control of such entity, whether they are paid by the organization. (OCTO)

13. **Policy Review:**

Document History

Policy Number	Action	Effective Date	Next Review Date
OCTO – 70005.1	Published	4/18/2017	4/18/2018

14. **Policy Acceptance:**

International Travel Policy for Mobile Computing Devices

Effective April 18, 2017

Archana Vemulapalli 4/18/17

Archana Vemulapalli
Chief Technology Officer
Government of the District of Columbia

Date

TO: Archana Vemulapalli
Chief Technology Officer
District of Columbia Government

FROM : [Director Name]
Director [Or other title for the Director]
[Agency Name]

DATE: [Date]

SUBJECT: Approval for Employee use of District issued mobile computing devices (e.g., laptops, tablets, smartphones) or other mobile electronic communication equipment that store, process, transmit, or receive District information, while on travel outside of the continental United States, Alaska and Hawaii

Employee [Name, Position, Agency] has a requirement to travel to one of these two categories of countries:

☐ A country that the U.S. Department of Homeland Security has placed restrictions on US-bound flights originating from specific airports (see 4.1.2 of OCTO Policy 7005.1).

☐ A country with elevated Cybersecurity and counter-intelligence threats, necessitating higher level security precautions (see section 4.5 of OCTO Policy 7005.1).

I have specifically authorized my employee to utilize District issued mobile computing devices in support of the District of Columbia government and the agency requirements and performance of their duties. My Agency CIO has ensured compliance with section 4.4 or 4.5 of OCTO Policy 7005.1. My Agency CIO has reviewed and removed sensitive data (e.g., Personal Identifiable Information (PII) or sensitive government business data) from all devices to be used during travel.

Thank you,
[Agency Director Signature]

Archana Vemulapalli
Chief Technology Officer

Date

☐ **Approved**
☐ **Disapproved**

CIO Checklist for District issued mobile computing devices (e.g., laptops, tablets, smartphones) when used on Business travel

1.1. **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). The following requirements must be met when using government-issued devices when on travel:

1.1.1. **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.

1.1.2. **Smartphones.**

- ☐ Prior to departure, review device to ensure removal of unnecessary Agency or District sensitive data (e.g., Personal Identifiable Information (PII) or sensitive government business data).
- ☐ Prior to departure, ensure District Mobile Device Management software (e.g, AIRWATCH) is installed and configured.
- ☐ 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.
- ☐ While on travel, if accessing DC Enterprise Network, utilize the DC Enterprise VPN Client (e.g., PulseSecure).

1.1.3. **Laptops / Tablets.**

- ☐ Prior to departure, review device to ensure removal of unnecessary Agency or District sensitive data (e.g., Personal Identifiable Information (PII) or sensitive government business data).
- ☐ Prior to departure, ensure the device has been encrypted using Full Disk Encryption (FDE) technology.
- ☐ 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.
- ☐ Prior to departure, employees must ensure their password meets District guidelines for length and security.
- ☐ 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.
- ☐ While on travel, if accessing DC Enterprise Network, utilize the DC Enterprise VPN Client (e.g., PulseSecure).
- ☐ Ensure that the laptop is always locked up when not under employee direct control (e.g., hotel safe).

1.2. 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.

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

1.2.2. **Business travel:** When travelling for business to the aforementioned countries, District issued equipment (laptop, tablet, or phone) may not be taken or utilized without Agency Director and OCTO CTO approval. Historic reports indicate that users should not expect that devices outside of their direct control are secure, even when stored in hotel safes.

- ☐ Employees will utilize 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 or sensitive information will not be installed on this device. Upon return, this device will be returned the OCTO or Agency IT Staff to be reimaged using secure erase techniques.
- ☐ Prior to travel, employees shall ensure their password has been changed to meet District policy. Upon return from travel, employee password shall be changed. Use of Multi-Factor Authentication for personal accounts is advised.
- ☐ Prior to travel, DC Employees shall complete a "Safe Computing Brief" with the District Chief Information Security Officer (CISO).
- ☐ While on travel, connection to the DC Enterprise Network or VPN is specifically disallowed.
- ☐ Connection to District email clients (via OWA or Office 365) is allowed when using Multi-Factor Authentication (MFA) (e.g., phone text with one-time access code).
- ☐ Connections to other District online resources not hosted within the DC Enterprise Network (e.g., PeopleSoft, PASS, etc.) that do not use MFA are specifically disallowed.

As Agency CIO I hereby acknowledge and ensure that the Employee's District issued mobile devices are in compliance with section 4.4 or 4.5 of OCTO Policy 7005.1. As Agency CIO, I hereby acknowledge that I have reviewed and removed sensitive data (e.g., Personal Identifiable Information (PII) or sensitive government business data) from all devices the Employee will use during travel.

[Insert Name of Agency CIO
Chief Information Officer
[Insert Name of Agency]

Date