



District of Columbia Government – Office of the Chief Technology Officer

## Network Access Policy

<b>Policy Number:</b>	<b>OCTO – 4001.3</b>	<b>Creation Date:</b>	10/26/2016
		<b>Approval Date:</b>	10/26/2016
<b>Effective Date:</b>	10/26/2016	<b>Revised Date:</b>	Not applicable

1. **Scope/Applicability:** This Network Access Policy (“Policy”) applies to all District of Columbia Government (the “District”) DC Workforce Members, including “DC Agencies,” “Workforce Members,” and “Hosts,” as defined in Section 12 below (collectively “DC Workforce Members”). These DC Workforce Members represent the District of Columbia “Information and Communications Technology (ICT) Ecosystem,” as the term is defined in Section 12 below.
2. **Authority:** DC Official Code § 1-1401 et seq.
3. **Purpose:** This Policy is designed to safeguard the District IT and communications ecosystem, data assets, DC Workforce Members, District constituents and stakeholders. The District is highly dependent on the use of information technology, communications systems and other cloud-based resources to effectively manage District programs and services. As such, with increasing risks, threats and vulnerabilities the District must respond with the availability and continued modernization of security policies and technology which provide for information confidentiality, integrity, and availability.
4. **Policy:** DC Agencies must strictly control access to the District’s Network (“DC networks”) and the asset resources that reside on the network by enforcing this Policy. Agencies that are unable to immediately comply with these requirements must submit a plan of action and milestones to OCTO outlining the date of compliance.
  - 4.1. **On Network:**
    - 4.1.1. Only DC Agency authorized endpoints shall be used to access DC networks.
    - 4.1.2. DC Workforce Members that access DC networks must be granted the most restrictive set of privileges required to perform authorized tasks.
    - 4.1.3. DC Workforce Members that access DC networks must be connected using enterprise active directory credentials.
    - 4.1.4. DC Workforce Members that need to perform IT administrator tasks on DC networks must use a separate privileged account to perform authorized tasks.
    - 4.1.5. DC Agency authorized endpoints must implement an OCTO Operating System image. The following OCTO security and management tools must not be disabled or removed: an endpoint management agent (e.g. ePO, LANDESK, or SCCM), Anti-Virus Software (McAfee), and Full Disk Encryption (for laptops). These requirements are further described in “OCTO Enterprise Endpoint Device Standards.” Remote administration by any DC Agency must only be performed using the OCTO approved tools.
    - 4.1.6. Remote administrative access to enterprise resources within DC Data Centers must use a privilege access management solution (e.g. Jump Host). Direct administrative access from an endpoint to enterprise resources in DC Data Centers is strictly prohibited.
    - 4.1.7. All non-DC agencies must sign an MOU, Interconnection Security Agreement (ISA) and external rules of behavior document to gain access to DC ICT Resources.



## District of Columbia Government – Office of the Chief Technology Officer

---

- 4.1.8. All inter-agency network communications must be authorized; DC agencies are prohibited from accessing other DC agency's non-public resources without an MOU.
- 4.2. **Off Network / Virtual Private Network (VPN) Access:** For specific VPN guidance, refer to the OCTO "Virtual Private Network Policy 2060.2," incorporated into this Policy by reference.
- 4.2.1. Government endpoints (laptop/desktop):
- 4.2.1.1. DC Agency approved endpoints must follow the same requirements for On Network endpoints.
  - 4.2.1.2. DC Agency approved endpoints must ONLY use an OCTO enterprise VPN.
- 4.2.2. Government mobile devices (phone, tablets, etc.):
- 4.2.2.1. DC Agency approved mobile devices must follow the same requirements for On Network devices.
  - 4.2.2.2. DC Agency approved mobile devices must implement an OCTO approved Mobile Device Management Solution (MDM)
- 4.2.3. Non-Government endpoints (e.g. BYOD):
- 4.2.3.1. Unless implementing all facets of 1.1.6, Non-government endpoints are prohibited from accessing the DC Intranet (DC network) via wired or wireless connections, unless connecting via Virtual Desktop Infrastructure (VDI). Agency help desks are not responsible for providing help desk support for these devices.
  - 4.2.3.2. Non-government endpoints must use an enterprise Layer 4 VPN connection to authorized network resources.
- 4.3. Access to the network not conforming to the above standards is expressly prohibited.
5. **Procedures:** Each DC Agency Chief Information Officer (CIO) must implement and enforce network access management procedures in accordance with this policy.
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 this policy's enforcement, and audit of this Policy when requested by the OCTO.
8. **Exemptions:** None.
9. **Sanctions:** If OCTO discovers non-compliance with this policy, OCTO will:
- 9.1. Block rogue devices from accessing the network and advise the DC Agency CIO of the non-compliance and assist the DC Agency CIO in developing a corrective action plan and a reasonable timeframe for its implementation.
  - 9.2. If the CIO does not implement the corrective action plan within the stated timeframe, OCTO will escalate the matter to the DC Agency Director for resolution.
  - 9.3. If the DC Agency Director does not resolve the policy non-compliance within his/her DC Agency, OCTO will refer the matter to the DC City Administrator for resolution.



## District of Columbia Government – Office of the Chief Technology Officer

---

### 10. Supporting Regulations and Policies:

- 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, Public Law No. 93-579.
- 10.3. HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C.
- 10.4. DC Code § 1-14, Authority and responsibility of the Office of the Chief Technology Officer.

### 11. Reference Documents:

- 11.1. NIST FIPS 200, “*Minimum Security Requirements for Federal Information and Information Systems*”, March 2006.
- 11.2. NIST IR 7298 Revision 2, “*Glossary of Key Information Security Terms*”, May 2013.
- 11.3. NIST SP 800-30 Revision 1, “*Guide for Conducting Risk Assessments*”, September 2012.
- 11.4. NIST SP 800-53 Revision 4, “*Security and Privacy Controls for Federal Information Systems and Organizations*”, April 2013.
- 11.5. NIST SP 800-66 Revision 1, “*An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*”, October 2008.
- 11.6. NIST SP 800-92, “*Guide to Computer Security Log Management*”, September 2006.



District of Columbia Government – Office of the Chief Technology Officer

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

<b>Availability</b>	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)
<b>Authorized endpoint</b>	An endpoint device is an Internet-capable computer hardware device on a TCP/IP network. In the context of this document, it refers to a user device, to include desktop computers, laptops, smart phones, tablets, or thin clients.
<b>BYOD</b>	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)
<b>Confidentiality</b>	The property ensuring that information assets are accessible only for reading by authorized parties. This is a fundamental security principle. (NIST IR 7298)
<b>DC Agencies</b>	Includes all District of Columbia Government organizations accessing the DC ICT Ecosystem. (OCTO)
<b>DC Assets</b>	All DC Government endpoints, security devices, hosts and data.
<b>DC ICT Ecosystem</b>	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)
<b>DC Networks</b>	All DC Government computer and communications networks including the “Secure” wireless access point.
<b>Hosts</b>	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)
<b>Integrity</b>	The property ensuring that only authorized parties are able to modify data or information disclosed in an electronic document. This is a fundamental security principle. (NIST IR 7298)
<b>On-Network (DC Network)</b>	All DC Government computer and communications networks which are part of the DC ICT Ecosystem (ex. Wired, Wireless, VPN)
<b>Off-Network</b>	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.
<b>Risk</b>	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)
<b>Security Team</b>	The OCTO Security Team formerly City-Wide IT Security (CWITS)
<b>Workforce Members (DC)</b>	Employees, contractor, intern, 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 or not they are paid by the organization. (OCTO)





OFFICE OF THE CHIEF TECHNOLOGY OFFICER

District of Columbia Government – Office of the Chief Technology Officer

---

14. Policy Acceptance:

**Network Access Policy**

Archana Vemulapalli

**Archana Vemulapalli**  
**Acting Chief Technology Officer**  
**Government of the District of Columbia**

10/26/2016

**Date**