



## Virtual Private Network Policy

<b>Policy Number:</b>	OCTO – 2060.2	<b>Creation Date:</b>	4/22/2016
		<b>Approval Date:</b>	4/22/2016
<b>Effective Date:</b>	4/22/2016	<b>Revised Date:</b>	

1. **Scope/Applicability:** This policy applies to all District of Columbia (DC) Government agencies.
2. **Authority:** DC Official Code § 1-1401 et seq.
3. **Purpose:** This policy establishes the requirements for remote access via a Virtual Private Network (VPN) connection from an external device to DC Government networks.
4. **Policy:** The Office of the Chief Technology Officer (OCTO) and agencies must ensure that the following VPN controls are implemented for each agency VPN connection:
  - 4.1. **Business purpose:** No person or entity may access DC Government information or networks via a VPN connection, or disclose or use any information so accessed, except for DC Government business purposes.
  - 4.2. **Applicability of other policies:** VPN connections and devices are a *de facto* extension of the DC government network, and as such are subject to the same rules and regulations that apply to DC Government-owned equipment.
  - 4.3. **Access by approval only:** No person or entity may access the DC Government network or information via a VPN connection except upon the written approval of OCTO.
  - 4.4. **Only OCTO approved solutions permitted:** Only OCTO approved-VPN solutions may be used for VPN access to DC Government information or networks.
  - 4.5. **Data integrity:** Any person or entity accessing DC government information via a VPN connection must preserve the confidentiality, availability, and integrity of DC government networks and information.
5. **Responsibilities**
  - 5.1. **Responsibilities of OCTO and agencies:**
    - 5.1.1. OCTO and agencies may provide VPN connections only to persons who submit a request to, and are approved by, OCTO for such access.
    - 5.1.2. OCTO and agencies must immediately terminate VPN access upon the departure of any VPN user from employment or engagement with a DC Government agency.
    - 5.1.3. OCTO and agencies must configure and administer VPN gateways in accordance with approved OCTO network operations and network security operating procedures.
    - 5.1.4. OCTO and agencies must control VPN access using a multi-factor VPN user authentication procedure, integrating the use of a security token with a strong passphrase provided to the user by OCTO.
    - 5.1.5. OCTO and agencies must limit VPN concentrators to an absolute continuous connection time of twelve (12) hours.
    - 5.1.6. OCTO and agencies must ensure that VPN users are automatically disconnected from DC Government networks after no more than thirty (30) minutes of inactivity. The user must then log on



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

---

again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

- 5.1.7. OCTO and agencies must monitor VPN sessions and must record and periodically audit time of access, date of access, access duration, and accessing individuals' user-IDs.
- 5.1.8. OCTO and agencies must ensure that all computers connected to DC Government networks via a VPN connection use the most up-to-date anti-virus software.
- 5.1.9. OCTO and agencies must provide training for all VPN users that explains VPN policies, procedures, and guidelines for accessing DC government network resources via an OCTO approved VPN connection.

### 5.2. Responsibilities of VPN users:

- 5.2.1. Users must preserve the security, availability, integrity and confidentiality of the information accessed using DC government networks.
- 5.2.2. Users must prevent access to DC government networks by unauthorized users.
- 5.2.3. Users must immediately notify the Agency Information Security Officer (ISO) of any data integrity errors.
- 5.2.4. Users must immediately notify OCTO of all security related VPN violations.
- 5.2.5. Users must configure all non-DC government computers to comply with OCTO VPN and network policies and standards.
- 5.2.6. Users must select an Internet Service Provider (ISP), install and activate any required software, and pay associated ISP-related network connectivity fees.

- 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 currency and compliance with applicable law.
- 7. **Policy Enforcement:** OCTO is responsible for the enforcement of this policy. Agencies must actively participate in the audit of this policy when requested by OCTO.
- 8. **Exemptions:** None.
- 9. **Sanctions:** If OCTO discovers non-compliance with this policy, OCTO will:
  - 9.1. 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 DC Agency CIO does not implement the corrective action plan within the stated timeframe, OCTO will escalate the matter to the DC Agency Director for immediate action and 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 immediate action and resolution.



District of Columbia Government – Office of the Chief Technology Officer

---

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

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

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

**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 800-77, "*Guide to IPsec VPNs*", December 2005.

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





13. Policy Acceptance:

**Virtual Private Network Policy**

Effective April 22, 2016

Archana Vemulapalli

4/22/16

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

**Date**