



## IT Remote Access Policy

<b>Policy Number:</b>	<b>OCTO – 4060.2</b>	<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 Government Agencies.
2. **Authority:** DC Official Code 1-1401 et seq.
3. **Purpose:** This policy establishes requirements for all District of Columbia Agencies to track, record, and report computer system access and usage throughout the District of Columbia's computer network. This policy is intended to ensure that system access and data use controls are sufficient to ensure proper systems functionality, District system user accountability, adequate support for investigations of improper transactions and monitoring District agency compliance with applicable regulatory requirements.
4. **Policy:** Each agency must strictly control remote access to the District of Columbia government network to prevent unauthorized access, illegal use or damage to the information technology (IT) network and its content.
  - 4.1. **Procedures:** Each District of Columbia agency Chief Information Officer (CIO) or his/her designee must implement procedures in written or electronic form that meet the following standards:
    - 4.1.1. Only District of Columbia Agency authorized devices may be used to access District of Columbia Government systems from any remote location. District of Columbia Agency authorized devices that the District Agency Director has authorized in writing for District of Columbia workforce users. District of Columbia agency approved equipment includes laptops, tablets, blackberries, PDAs, smart phones or other devices.
    - 4.1.2. Network connections used from remote locations must be District of Columbia Agency authorized network technologies such as, DC Webmail/Google Mail applications, VPN (IPSec, SSL, and SSH) via wired broadband internet, encrypted VoIP or wireless 3/4G and secure Wi-Fi connections.
    - 4.1.3. Remote access connections established outside of the intercontinental United States without the express written permission of the DC Chief Technology Officer (CTO), the DC Chief Information Security Officer, and the requesting District of Columbia Agency Program Manager are strictly prohibited.
    - 4.1.4. Direct internet access to any system containing Federal Tax Information is prohibited.
    - 4.1.5. Each District of Columbia Agency Chief Information Officer (CIO) or his/her designee must verify IT remote access by monitoring network traffic and/or checking traffic logs.
    - 4.1.6. All remote access security breaches must be reported immediately to the Office of the Chief Technology Officer Network Operations Center at 202.724.2028 or [noc-eng@dc.gov](mailto:noc-eng@dc.gov).



---

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

---

5. **Policy Maintenance:** The Office of the Chief Technology Officer (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.
6. **Policy Enforcement:** OCTO is responsible for the enforcement of this policy. Agencies must actively participate in the audit of this policy when requested by the OCTO.
7. **Exemptions:** None.
8. **Sanctions:** If OCTO discovers non-compliance with this policy, OCTO will:
  - 8.1. 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.
  - 8.2. 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.
  - 8.3. 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.
9. **Supporting Laws and Regulations:**
  - 9.1. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA).
  - 9.2. Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579.
  - 9.3. HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C.
10. **Reference Documents:**
  - 10.1. NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems (moderate confidentiality impact)", February 2004.
  - 10.2. NIST FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems", March 2006.
  - 10.3. NIST IR 7298 Revision 2, "Glossary of Key Information Security Terms", May 2013.
  - 10.4. NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations", April 2013.
  - 10.5. NIST SP 800-66 Revision 1, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule", October 2008.





12. Policy Acceptance:

**IT Remote Access Policy**

Effective April 22, 2016

Archana Vemulapalli

4/22/16

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

**Date**