

Access Control Policy

Policy Number:	OCTO – 1014.0	Creation Date:	August 22, 2009
		Approval Date:	September 30 th 2011
Effective Date:	September 30 th , 2011	Revised Date:	September 16 th 2011

1. **Scope/Applicability:** This policy applies to all DC workforce members and those using DC Government information systems and technologies on the internal DC Wide Area Network.
2. **Authority:** DC Official Code § 1-1402 et seq.
3. **Purpose:** This policy ensures appropriate access control to include but not limited to all DC computer networks, facilities, resources, equipment, applications, information systems, and data at rest or in transmission.
4. **Policy:** Each DC Agency must implement security access control measures to ensure appropriate access for all DC workforce members based upon each workforce members' job requirements; and must establish procedures that document, review, and modify a user's right of access to assigned equipment, transactions, programs, networks, data, work areas, or processes that include at a minimum the following security controls:
 - 4.1. An appropriate process for granting and prohibiting access of DC controlled IT resources to workforce members based only on requirements set forth by the workforce member's title, duties, and responsibilities.
 - 4.2. Measures to lock out unauthorized access to potential threat agents.
 - 4.3. Establish procedures to workforce members as it relates to disaster recovery, incident response, and continuity planning.
5. **Procedures:** Each DC agency must implement access control measures in accordance with this policy.
6. **Sanctions:** Non-compliance with the provisions of this policy may result in referral of the responsible individual for disciplinary action up to and including termination of employment, in accordance with District Personnel Manual Chapter 16.
7. **Exemptions:** None
8. **Policy Maintenance:** The Office of the Chief Technology Officer must review and update this policy at least annually to ensure that the policy is up-to-date with the latest developments in DC technology consistent with applicable law.
9. **Policy Enforcement:** The Office of the Chief Technology Officer is responsible for the enforcement of this policy. Agencies will actively participate in the audit and enforcement of these policies when requested by the Office of the Chief Technology Officer.
10. **Supporting Regulations and Policies:**
 - 10.1. OCTO Information Security Program Policy 1013.0.
 - 10.2. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA)

District of Columbia Government – Office of the Chief Technology Officer

- 10.4. HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C.
- 10.5. ARRA, Health Information Technology for Economic and Clinical Health Act (HITECH)

11. Reference Documents:

- 11.1. 42 U.S.C. § 1320d-5.
- 11.2. NIST Special Publication 800-30, “*Risk Management Guide for Information Technology Systems*”.
- 11.3. NIST Special Publication 800-53 Revision 3, “*Recommended Security Controls for Federal Information Systems and Organizations*”.
- 11.4. NIST Special Publication 800-66 Revision 1, “*An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*”.
- 11.5. NIST Special Publication 800-92, “*Guide to Computer Security Log Management*”.
- 11.6. NIST FIPS 200, “*Minimum Security Requirements for Federal Information and Information Systems*”.

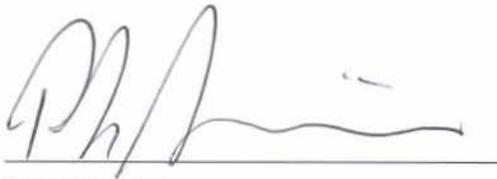
12. Definitions: Definitions for OCTO policies can also be found in the Glossary Section of the OCTO website.

Information System	An integrated set of components (e.g. hardware, software, processes) for collecting, storing, processing, and communicating information.
Risk	The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome).
Security Controls	Safeguards or countermeasures to avoid, counteract, or minimize security risks.
Workforce Member	Employees, 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.

13. Policy Acceptance:

Access Control Policy

Effective September 30th, 2011



Rob Mancini
Chief Technology Officer
Government of the District of Columbia

9/30/11
Date



Rob Mancini
Interim Chief Security Officer
Government of the District of Columbia

9/30/11
Date