Physical Access Security Policy

Policy Number:	**OCTO – 2030.0**	**Creation Date:**	Novem ber 23rd 2011
		Approval Date:	September 30th 2011
Effective Date:	September 30th, 2011	**Revised Date:**	September 16th 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 the establishment and implementation of physical access security controls to protect DC information systems and facilities from unauthorized physical access, tampering, theft, and physical damage (in accordance with OCTO Access Control Policy 1014.0).
4. **Policy:** Each DC Agency must implement measures for the protection of physical environments to prevent unauthorized exposure, tampering, and/or theft to DC information systems and resources that include at a minimum the following security controls:

   4.1. **Facility Access Controls** Agencies who operate computing facilities must ensure that physical access to information systems are limited to authorized workforce members. Measures include:

   4.1.1. Develop and implement a Continuity of Operations Plan (COOP).
   4.1.2. Develop and implement a Facility Security Plan.
   4.1.3. Implement physical security to critical areas of facilities housing information systems.
   4.1.4. Secure doors, windows, cabinets, desks, egresses, and all access ways.
   4.1.5. Validate workforce member facility access based on role and function.
   4.1.6. Control visitor accessibility; and maintain visitor logs.
   4.1.7. Maintain maintenance record logs of repairs and modifications to physical components of a facility related to security or the operating environment.

   4.2. **IT Equipment Security Controls.** Agencies must ensure that all IT equipment, and their immediate surrounding environment, is physically protected from unauthorized access.

   4.3. **Device and Media Controls.** Agencies must ensure the proper disposition of all electronic media to include receipt, removal, backup, storage, reuse, disposal, and accountability.
5. **Procedures:** Each DC Agency must implement physical access security 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 Access Control Policy 4001.0.
    10.2. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA)
    10.3. Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579
    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 800-116, *"A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS"*.
    11.6. NIST FIPS 201-1, *"Personal Identity Verification of Federal Employees and Contractors"*.

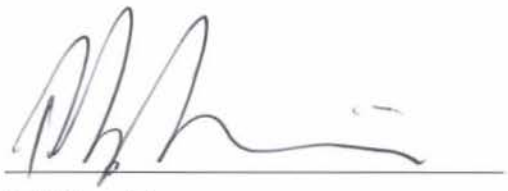
12. **Definitions:** Definitions for OCTO policies can also be found in the Glossary Section of the OCTO website.

Information System	An integrated set of components (e.g. hardware, software, processes) for collecting, storing, processing, and communicating information.
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:**

Physical Access Security Policy

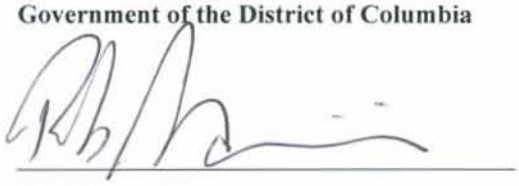
Effective September 30th, 2011



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