



Security Sensitive Information Policy

Policy Number: Approved By:	OCTO – 2011.0	Creation Date:	January 1, 2011
		Approval Date:	April 7, 2011
Effective Date:	March 29, 2011	Revised Date:	March 29, 2011

1. **Scope/Applicability:** This policy applies to all DC workforce members.
2. **Authority:** DC Official Code § 1-1402 et seq.
3. **Purpose:** This policy ensures uniformity and consistency in how sensitive information that resides within all DC Agency information systems is properly used and stored by DC workforce members.
4. **Policy:** All data that resides on any DC information system and (in accordance with OCTO Data Classification Policy 2010.0) is classified by any DC Agency as sensitive information must be treated in the following manner:
 - 4.1. The usage of sensitive information for other than approved official District of Columbia Government business is prohibited.
 - 4.2. The access to sensitive information by an unauthorized person or entity is prohibited.
 - 4.3. The storage of sensitive information on mobile storage devices without written approval from the Agency Information Security Officer (ISO) or an officially approved designee is prohibited.
 - 4.4. The storage of sensitive information on employee owned personal computers is prohibited.
 - 4.5. Sensitive information copied to mobile storage devices shall be removed/deleted from the device after the sensitive information is no longer required for business purposes.
 - 4.6. Any lost or stolen Agency mobile storage device that contains sensitive information must be reported to the Agency’s ISO. The Office of the Chief Technology Officer, Chief Security Officer must be notified of all incidents involving the lost or theft of sensitive information as soon as such loss or theft is discovered.
5. **Procedures:** The Agency ISO must define, document, and implement security standards, and related procedures in accordance with this policy.
6. **Sanctions:** Non-compliance with the provisions of this policy may result in disciplinary actions 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 technological currency and compliance with applicable law.
9. **Policy Enforcement:** The Agency ISO is responsible for the enforcement of this policy.
10. **Supporting Regulations and Policies:**
 - 10.1. OCTO Information Access Management Policy 2000.0
 - 10.2. OCTO Data Classification Policy 2010.0
 - 10.3. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA)
 - 10.4. Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579
 - 10.5. HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C.
 - 10.6. ARRA, Health Information Technology for Economic and Clinical Health Act (HITECH)



District of Columbia Government – Office of the Chief Technology Officer

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 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.
Sensitive Information	Information is considered sensitive if the loss of confidentiality, integrity, or availability can be expected to have a serious, severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals directly affected by the information.
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.



OFFICE OF THE CHIEF TECHNOLOGY OFFICER

District of Columbia Government – Office of the Chief Technology Officer

13. Policy Acceptance:

Security Sensitive Information Policy

Effective March 29, 2011

A handwritten signature in black ink, appearing to read "Rob Mancini", written over a horizontal line.

Rob Mancini
Chief Technology Officer
Government of the District of Columbia

A handwritten date "9/7/11" in black ink, written over a horizontal line.

Date

A handwritten signature in black ink, appearing to read "Rob Mancini", written over a horizontal line.

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

A handwritten date "9/7/11" in black ink, written over a horizontal line.

Date