



## Data Classification Policy

|  |                |                       |                 |
|--|----------------|-----------------------|-----------------|
| <b>Policy Number:<br/>Approved By:</b> | OCTO – 2010.0  | <b>Creation Date:</b> | January 1, 2011 |
|  |                | <b>Approval Date:</b> | April 7, 2011   |
| <b>Effective Date:</b>                 | March 30, 2011 | <b>Revised Date:</b>  | March 30, 2011  |

1. **Scope/Applicability:** This policy applies to all DC Agency Directors, DC Agency Information Security Officers (ISOs), the DC Chief Technology Officer, and all DC workforce members.
2. **Authority:** DC Official Code § 1-1402 et seq.
3. **Purpose:** This policy requires all DC Agency information assets to be identified, classified, protected, and managed from creation to disposal in a manner that ensures protection commensurate with the sensitivity and value of the information asset.
4. **Policy:** Each Agency must identify and classify all information assets based on criticality, confidentiality, sensitivity, availability, value, and legal requirements; and must implement sufficient measures to protect each asset from use or disclosure that would be harmful or inappropriate in light of the classification of the asset.
5. **Procedures:** Each DC Agency Information Security Officer (ISO) must implement security procedures in accordance with this policy.
  - 5.1. **Asset Classification Responsibility:** Information Owners must implement a mechanism to identify information assets for the purpose of defining their criticality, confidentiality, sensitivity, availability, value, and legal implications.
  - 5.2. **Classification Schema:** Agencies must use the following classification schema to differentiate between various levels of sensitivity and value. Information that is not labeled and cannot be easily identifiable as Level 1, should be handled as described in this document for Level 2.
    - 5.2.1. **Level 1, “Public”** – Low-sensitivity information; information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of Agency workforce members, clients or partners. Level 1 includes information regularly made available to the public via electronic, verbal or hard copy media.
    - 5.2.2. **Level 2, “For Internal Use”** – Sensitive information that may not be protected from public disclosure but if made easily and readily available, may jeopardize the privacy or security of Agency workforce members, clients, or partners. While safeguards must be in place, the unauthorized disclosure, modification, or destruction of this information is not expected to seriously or adversely affect the Agency. Agency shall follow its customary disclosure policies and practices before providing this information to external parties.
    - 5.2.3. **Level 3, “Confidential”** – Sensitive information intended for limited personnel access and business use that may be exempt from public disclosure. The unauthorized disclosure of this information could adversely affect the Agency, its employees, and its key stakeholders. Information in this category may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized Agency business must be under contractual obligation of



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

---

confidentiality with the Agency (for example, confidentiality/non-disclosure agreement) before receiving it.

5.2.4. **Level 4, “Restricted Confidential”** – Information that is deemed extremely sensitive and is intended for use by named individual(s) only. The unauthorized disclosure of this information could adversely affect the Agency, its employees, clients, or partners. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to identified individual(s), Agency workforce members, clients, or partners, or cause major harm to the Agency.

5.3. **Information Asset Protection:** Each information asset classification must be associated with a set or range of controls designed to provide the appropriate level of protection of the information commensurate with the sensitivity and value of the information in that classification.

5.3.1. Level 1 data does not require special handling or safeguards.

5.3.2. Level 2 data may be sent electronically or mailed without special security controls at the discretion of the information owner.

5.3.3. Level 3 data with PII must be secured via encryption or secured form of transport. Disclosure, transmission or dissemination of Level 3 data must be authorized by the information owner.

5.3.4. Level 4 data must be secured via encryption and such safeguards as digital certificates. Disclosure, transmission or dissemination of Level 4 data must be authorized and documented by the Agency’s ISO.

5.4. **Training:** All Agency workforce members must have training that explains the Agency’s classification of data as part of its regular security awareness training program (in accordance with OCTO IT Security Awareness and Training Policy 1090.0).

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 Office of the Chief Technology Officer is responsible for the enforcement of this policy.

10. **Supporting Regulations and Policies:**

10.1. OCTO IT Security Awareness and Training Policy 1090.0

10.2. E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act (FISMA).

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*.

District of Columbia Government – Office of the Chief Technology Officer

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

|                            |  |
|----------------------------|--|
| <b>Information Asset</b>   | Any electronic information that is used in the course of business activities.  |
| <b>Information Owner</b>   | The person or group responsible for applying security policies to an information asset.  |
| <b>Availability</b>        | The property requiring that information system components, data or information will be accessible and available to authorized parties when needed. This is a fundamental security principle.   |
| <b>Confidentiality</b>     | The property ensuring that information assets are accessible only for reading by authorized parties. This is a fundamental security principle.   |
| <b>Digital Certificate</b> | A digital certificate is an electronic token that establishes the credentials of a person or entity when doing business or other transactions on the Web. It is issued by a certification authority (CA) containing a person or entity's name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. |
| <b>Information System</b>  | An integrated set of components (e.g. hardware, software, processes) for collecting, storing, processing, and communicating information.   |
| <b>Integrity</b>           | The property ensuring that only authorized parties are able to modify data or information disclosed in an electronic document. This is a fundamental security principle.   |



District of Columbia Government – Office of the Chief Technology Officer

---

13. Policy Acceptance:

Data Classification Policy

Effective March 30, 2011

**Rob Mancini**  
Chief Technology Officer  
Government of the District of Columbia

4/7/11  
Date

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

4/7/11  
Date