Person or Entity Authentication Policy

Policy Number:	**OCTO – 2013.0**	**Creation Date:**	April 15, 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 Agencies 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 that adequate measures are in place to validate the authenticity of a person or entity attempting to gain access to DC information systems prior to granting access to the resource.
4. **Policy:** Each DC Agency must implement appropriate information system authentication measures to confirm that access to information systems (in accordance with OCTO Information System Access Management Policy 2000.0) will include, at a minimum, the following security controls:

   4.1. Access to information systems will contain access methods that include two or more of the following:
   - 4.1.1. Unique User Identifiers [userid]
   - 4.1.2. Security Identifier [SID]
   - 4.1.3. Password Systems
   - 4.1.4. Personal Identification Number (PIN) Systems
   - 4.1.5. Multiple factor authentication for remote access
   - 4.1.6. Biometric Identification Systems
   - 4.1.7. Digital Signatures

   4.2. Agencies must support or implement appropriate authentication processes to include:
   - 4.2.1. Documented procedures for granting persons or entities authentication credentials, or for changing an existing authentication method of a person or entity.
   - 4.2.2. Documented procedures for removing or disabling authentication credentials for persons or entities that no longer require access.
   - 4.2.3. Periodic validation that security credentials are current and verifiable.
   - 4.2.4. Protection of authentication credentials (e.g., passwords, PINs) with appropriate security controls to prevent unauthorized access in accordance with OCTO – 2003.0 Password Management Policy.
   - 4.2.5. Measures for masking, suppressing, or otherwise obscuring the passwords and PINs (when feasible) for workforce password privacy.

   4.3. Prohibit the use of login scripts for authenticating access to sensitive information without the review and approval of the OCTO Chief Information Security Officer (CISO), Deputy CTO and/or CTO prior to deployment.

   4.4. Ensure that authentication attempts, within a specified time limit, not exceed the number of reasonable attempts specified in OCTO policy. Failed login attempts must result in the following:
   - 4.4.1. Disable the associated account for an appropriate period of time
   - 4.4.2. Log the event as a failed access attempt.
   - 4.4.3. Notify the appropriate system administrator.

5. **Procedures:** Each DC Agency must implement personnel or entity authentication procedures 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 System Access Management Policy 2000.0.
    - 10.2. OCTO Password Management Policy 2003.0.
    - 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)
11. **Reference Documents:**
    - 11.1. NIST Special Publication 800-53 Revision 3, *"Recommended Security Controls for Federal Information Systems and Organizations"*.
    - 11.2. NIST Special Publication 800-63, "*Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology"*.
    - 11.3. NIST Special Publication 800-66 Revision 1, *"An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule"*.
    - 11.4. NIST Special Publication 800-300, *"Risk Management Guide for Information Technology Systems"*.
    - 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.

Biometric Identification Systems	A security and access control system of authentication capable of identifying measurable physical characteristics of a person.
Digital Signature	A digital signature is a method to ensure data authenticity. A digital signature is created by generating a hash (message digest) against the data and then encrypting this digest using the cryptography (public or private) key. This signature is then appended to the data. Once the recipient has received the data and signature, they generate a hash against the data, as well as decrypting the signature using their cryptography (public or private) key. These digests are then compared to ensure data authenticity.
Information System	An integrated set of components (e.g. hardware, software, processes) for collecting, storing, processing, and communicating information.
Password System	A subsystem of the operating system that manages user accounts, confirms user authentication, and enables system access according to policy.
Security Controls	Safeguards or countermeasures to avoid, counteract, or minimize security risks.
Security Token	A two-factor authentication methodology used to electronically validate authorized users. The user is issued a device and a personal identification number (PIN), which authorizes them as the owner of that particular device; the device then displays a frequently changed access code, which uniquely identifies the user to the service, allowing them to log in.

13. **Policy Acceptance:**

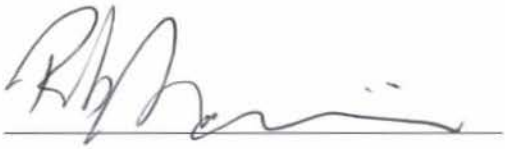
Person or Entity Authentication Policy

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