Password Management Policy

Policy Number:	OCTO-PM-P101.01	Effective Date:	December 31, 2013

1. **Purpose:** This policy provides directives on the secure and effective use, development and maintenance of user account passwords, password-based authentication systems and applications.

2. **Authority:** DC Official Code §§ 1-1401 et seq.

3. **Scope:** This policy applies to all DC workforce members and all users granted access to any DC Government information systems and or technology on the internal DC Wide Area Network.

4. **Policy:** Each Agency must implement system and application account management procedures for all passwords and must, at a minimum:
   - 4.1. Create strong passwords using the following standard:
     - 4.1.1. The password is at least eight (8) characters long.
     - 4.1.2. The password contains characters from at least three of the following four categories:
       - 4.1.2.1. English uppercase characters (A - Z)
       - 4.1.2.2. English lowercase characters (a - z)
       - 4.1.2.3. Base 10 digits (0 - 9)
       - 4.1.2.4. Special or Punctuation Characters (*Example:* !, $, #, or %)
   - 4.2. Disable account or delay account access for at least five (5) minutes after a minimum of at least five (5) failed password attempts.
   - 4.3. Require user passwords to be changed at least every 180-360 days
   - 4.4. Exemption to the requirement contained in 4.3 of this document can be granted by review and approval of CTO on a case by case basis.
   - 4.5. Restrict the use of at least the previous six (6) passwords.
   - 4.6. Provide awareness education on password policy, usage and protection.
   - 4.7. Provide ability for user to change user's own password.
   - 4.8. Implement procedures to validate a user's identity for password reset requests.
   - 4.9. Implement procedures for secure password provisioning, reset and protection.
   - 4.10. Implement procedures to audit and respond to password usage activity including failed password attempts.
   - 4.11. Apply strong passwords to accounts used by services or processes.
   - 4.12. Implement procedures to require service account passwords and application passwords be changed at least annually or changed immediately upon notification of unauthorized password disclosure.
   - 4.13. Implement procedures to restrict passwords from being transmitted or sent in the same email as the corresponding user name or access credential.
   - 4.14. Change vendor default passwords on all systems and applications prior to use in production.
   - 4.15. Prohibit passwords from being shared or disclosed to unauthorized personnel.

5. **Policy Maintenance:** The Office of the Chief Technology Officer is responsible for the maintenance and administration of this policy and must periodically review and, when necessary, update this policy to ensure technical relevance and regulatory compliance.

6. **Policy Enforcement:** The Office of the Chief Technology Officer is responsible for the enforcement of this policy and may audit agencies to determine compliance with this policy.

7. **Exemptions:** No workforce member or user is exempt from this policy except for members identified in DC Official Code DC ST § 1-1406 Applicability.

8. **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.

9. **Applicable Policies and Regulations:**

   9.1 E-Government Act, (P.L. 107-347), Title III, Federal Information Security Management Act
   9.2 Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-379
   9.3 HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C
   9.4 The Federal Information Security Management Act (FISMA) of 2002 44 U.S.C. § 3541
   9.5 ARRA, Health Information Technology for Economic and Clinical Health Act (HITECH)

10. **Reference Documents:**
    10.1. NIST Special Publication 800-30, *"Risk Management Guide for Information Technology Systems"*.
    10.2. NIST Special Publication 800-53 Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"*.
    10.3. NIST Special Publication 800-66 Revision 1, *"An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule"*.
    10.4. ISO/IEC 27002:2005, *"Information technology - Security techniques - Code of practice for information security management"*

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

12. **Document History:**

Date	Action	Effective Date	Next Review Date
September 1, 2004	Initial Release		
May 9, 2011	Revised	June 1, 2011	
May 21, 2012	Revised	August 31, 2012	July 31, 2013
October 9, 2013	Content Revised	December 31, 2013	August 15, 2014

13. **Contact Information:** Questions concerning this policy may be directed to the Office of the Chief Technology Officer at 202-727-2277 or infosecpolicy@dc.gov.

14. **Authorization and Approval:**

Password Management Policy
Effective December 31, 2013

Rob Mancini
Chief Technology Officer
Government of the District of Columbia

12/18/13
Date

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

12/18/13
Date