PASSWORD MANAGEMENT

ISSP-32-0410

1. **SUBJECT:** OPIC will protect access to its information resources by ensuring that any passwords used for authentication are properly assigned and protected.

2. **SCOPE:** This policy applies to all OPIC owned or operated information systems, both operational and in development.

3. **DESCRIPTION:** In order for passwords to be an effective tool for providing security, they must be selected, stored, and administered appropriately. If passwords are poorly chosen, they can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

4. **PROCEDURES & GUIDELINES:**

(a) In systems that use passwords as their authentication method, every account (including newly issued accounts) will have a password.

(b) Passwords must be changed:

(1) Immediately upon initial user logon.

(2) At least every 90 days.

- Individual systems may set a shorter expiration period for their users.
- Systems will have an automated mechanism to ensure that passwords are changed.

(3) If it is suspected that the password has been compromised.

(4) For administrator accounts, immediately upon the departure of personnel with access to those accounts, or upon suspected compromise of those passwords.

(c) The following guidelines apply to password storage and visibility:

(1) Passwords will not be visible on a screen, hardcopy or other output device.

(2) Passwords will never be stored in a clear text file. This includes storage of passwords in configuration files, database files, application code, and system directories. Any such passwords must be encrypted if they are required.

(3) Passwords will not be sent via unsecured (i.e., unencrypted and unauthenticated) email.

(4) Passwords will not be stored in written form (*e.g.* sticky notes) except if secured in an approved locked area.

(d) Passwords are never to be lent or divulged to other persons, including individuals purporting to be system administrators.

(e) A poorly chosen password could compromise the entire OPIC computer network. The object when choosing a password is to make it as difficult as possible for someone to guess what you have chosen. The following guidelines should be used to select strong, effective passwords:

(1) Users with multiple accounts on the same OPIC system (*e.g.* an administrative account and a regular user account) must use completely different passwords for each account. Generic or group passwords will not be used.

(2) Users are not to use the same password at OPIC that they use for any non-OPIC computer accounts (*e.g.* an account on an Internet website).

(3) Passwords should be at least 8 characters and contain a combination of letters, numbers, and special characters.

(4) Passwords cannot be reused for at least four changes.

(5) Never assign a login account a password that is the same string as the User ID or that contains the User ID (*e.g.,* "bob123" is not an appropriate password for user "bob").

(6) Never set any password equal to the null string (*i.e.,* a blank password), which is equivalent to no password at all.

(7) Passwords should not be a dictionary word in any language.

(8) Passwords should not contain any proper noun or the name of any person, pet, child, or fictional character.

(9) Passwords shall not contain any employee serial number, Social Security Number, birth date, telephone number, or any information that could be readily guessed about the creator of the password.

(10) Passwords should not contain any simple pattern of letters or numbers, such as "xyz123."

(11) Passwords should not share more than 3 sequential characters in common with a previous password (*i.e.,* do not simply increment the number on the same password, such as fido1, fido2, etc.).

(12) Use a password that is easy to remember (*e.g.,* a phrase, line from a song, or nonsense words) and that you can type quickly.

(f) The assignment of passwords for specific OPIC systems should adhere to the following:

(1) Each system should have its own password selection standard that adheres to the above guidelines while being commensurate with the level of security required by the level of sensitivity of the system.

(2) The system will be configured to enforce the password selection criteria specified in the system criteria.

(g) Users should avoid using the "remember password" feature on web sites and other applications.

(h) If SNMP is used, the community strings should follow the same selection guidance provided for passwords.

(i) OPIC will adhere to NIST guidance as set forth in Special Publication 800-63, Recommendations for Electronic Authentication, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners shall ensure that the resources they own comply with the guidelines set forth in this policy.

(b) Information Custodians shall:

(1) Assist Information Owners with implementing measures to enforce policy selection and management on their systems.

(2) Instruct users regarding system password policy.

(3) Assist the ISSO with auditing for compliance with this policy.

(4) Report any password compromises of OPIC information resources to the ISSO and the Information Owner.

(c) Employees shall understand their responsibilities for selecting and safeguarding their passwords, and immediately notify a supervisor or the Information Custodian if they suspect that a password has been compromised.

(d) Supervisors shall:

(1) Ensure that their personnel understand and comply with the guidelines contained in this policy.

(2) Report any suspected violations or password compromises to the ISSO and the Information Custodian.

(e) The Information Systems Security Officer (ISSO) shall:

(1) Provide advice to Information Owners and Custodians regarding system-specific password policies.

(2) Audit systems to ensure compliance with this policy

(f) System Developers must ensure that their systems support the procedures and guidelines specified in this policy document.

6. DEFINITIONS:

(a) Authentication – The process of verifying that a user is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or iris.

(b) Password – Any secret string of characters which serves as authentication of a person’s identity, and which may be used to grant or deny access.

(c) User ID - Character string that uniquely identifies a computer user or computer process.

7. **ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

8. **POINT OF CONTACT:** OPIC Information Systems Security Officer (ISSO)

9. **ATTACHMENTS:** None

10. **AUTHORITY:**

    (a) OPIC Directive 00-01, Information Systems Security Program.

    (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.

    (c) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers.

    (d) Homeland Security Presidential Directive / HSPD-7, December 17, 2003.

    (e) NIST Special Publication 800-63, Recommendations for Electronic Authentication.

    (f) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

11. **LOCATION:** TBD

12. **EFFECTIVE DATE:** October 22, 2004

13. **REVISION HISTORY:** None

14. **REVIEW SCHEDULE:** This policy should be reviewed and updated annually.