IDENTIFICATION AND AUTHENTICATION

ISSP-12-TBD

1. **SUBJECT:** Access to OPIC information systems will only be granted to identified and authenticated users. OPIC will establish procedures and controls for granting, changing, and terminating access to information systems.

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

3. **DESCRIPTION:** In order to ensure that unauthorized persons do not have access to sensitive OPIC information resources, it is necessary to first establish the identity of the user who is attempting to access the resource. Access controls can then be used to allow or limit access based on the established user identity.

   The specific method(s) of authentication used for each system shall be commensurate with the level of sensitivity of the system to be accessed (*i.e.* more sensitive systems should use stronger authentication methods). Multiple authentication methods (*e.g.* use of both a password and a token) may be required for high-sensitivity or high-risk situations.

4. **PROCEDURES & GUIDELINES:**

   (a) Each OPIC system shall incorporate proper user authentication and identification to ensure that access is not granted to unauthorized persons. Users will not have access to OPIC information resources without identifying and authenticating themselves (*i.e.* "logging on").

   (b) OPIC will develop and follow detailed procedures for the creation, removal, and modification of user accounts and authentication credentials.

   (c) User accounts must adhere to the following guidelines:

      (1) Allow only one user per account; User IDs are never to be shared.

      (2) Never install a guest/guest account. Remove any guest accounts that are created by default by the system unless absolutely required approved by the system owner and the ISSO.

(3) No accounts will be named with easily guessed generic names (such as "anonymous", "guest", "admin", "ftp", "telnet", "www", "host", "user", "test", "bin", "nobody", etc.) unless absolutely technically required by the system.

(4) Default accounts that are present upon initial installation of the system should be removed or renamed unless absolutely technically required by the system.

(5) Accounts should be deactivated immediately upon termination of an employee or contractor.

(6) Unused accounts will be deactivated on at least a monthly basis.

(7) Accounts for contractors and temporary employees should expire on the final date of their contract.

(b) Administrator accounts must adhere to the following guidelines:

(1) The names of the administrator accounts should be renamed, if possible, to make it more difficult for attackers to guess the names of these accounts.

(2) Each person who has a legitimate need to use Administrator privileges should have their own administrative account that they will use to perform administrative functions. Usage of the main administrator account for each system should be limited to emergencies, and is to be limited to designated IRM staff. This will protect the main administrator account and also provide an audit trail of administrative activities.

(3) All accounts with administrator privileges should have strong passwords or other alternative strong authentication methods.

(d) If passwords are used for authentication, they must adhere to the OPIC Password Management policy.

(e) If authentication methods other than passwords other than passwords (e.g., biometrics, smartcards, tokens, etc), then:

(1) They must be approved by the ISSO.

(2) Additional policies and procedures will be developed to govern their usage.

(f) Account credential information (e.g., User IDs, passwords) that are stored on the devices (such as enable passwords in router configuration files) must be encrypted.

(c) To preclude brute force attacks, an intruder lockout feature should be implemented on each system to temporarily suspend the account after three invalid logon attempts. Manual action by a security system administrator is required to reactivate the ID.

(d) OPIC will restrict access to authentication data. Authentication data will be protected with access controls and encryption to prevent unauthorized individuals from obtaining the data.

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

5. ROLES & RESPONSIBILITIES:

(a) Employees shall understand their responsibilities for safeguarding User IDs and passwords, and immediately notify a supervisor or the Information Custodian (e.g., the IRM department) if they suspect that a password or other system credential has been compromised.

(b) Supervisors shall ensure that their personnel understand and comply with the guidelines contained in this policy, promptly notify Information Custodians of accounts that should be deactivated, and report any suspected violations or compromises of credentials to the ISSO and the Information Custodian.

(c) Information Custodians shall implement appropriate identification and authentication methods for the information resources in their care, instruct users as to their usage, and report any compromises of these resources to the ISSO and the Information Owner.

(d) Information Owners shall ensure that appropriate identification and authentication methods are implemented for the resources that they own, based on the classification and level of risk assigned to the resource.

(e) The Information Systems Security Officer (ISSO) shall prepare guidelines and standards for user credentials, perform compliance reviews, and approve issuance of administrator credentials.

(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) Brute Force Attack - attack where the attacker attempts to systematically "guess" a password or other secret by trying all possible values.

(c) Identification – The process of determining who a user claims to be; usually performed by presenting a user ID (*i.e.*, "jsmith").

(d) Information Resources – The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

(e) 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.

(f) Strong Authentication – An authentication process using techniques which would require a high level of effort to compromise. Strong authentication usually entails the use of multiple, integrated authentication techniques (factors), such as using both a token and a PIN number together.

(g) 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.