ACCESS CONTROL

ISSP-11-0410

1. **SUBJECT:** Access to OPIC information resources will be limited to those that need those resources to perform their duties. The principles of separation of duties and least privilege will be applied to the allocation of access rights.
2. **SCOPE:** This policy applies to all OPIC information users, owners, and custodians, as well as access to any OPIC information resources.
3. **DESCRIPTION:** Users must have access to the information resources required to do their jobs. However, excessive or uncontrolled access can lead to the unauthorized or unintentional disclosure, modification, or destruction of those resources, as well as liability for negligence in protecting those resources. Therefore, access to specific resources is only to be granted to authorized personnel who have a legitimate need to use those resources, and their access privileges will be limited to those required to perform their duties.
4. **PROCEDURES & GUIDELINES:**

   (a) Users must be granted specific access privileges on each system, limited to those required to perform their job functions.

   (b) Users must be authorized by the information owner prior to being granted access to a particular resource.

   (c) Users will only access resources to which they have been authorized, regardless of actual system permissions.

   (d) Users will not circumvent the permissions granted to their accounts in order to gain access to unauthorized information resources.

   (e) Users will protect their own accounts:

      (1) Users will not allow anyone else to use their account, or use their computers while logged in under their account, except as required for system administration.

      (2) When leaving their computer unattended, users will either log out or invoke protection of their system (such as a password-protected screensaver).

      (3) Users are responsible for any activity initiated by their own userID (since only they should have access to their userID).

   (f) The level of access control will depend on the classification of the resource and the level of risk associated with the resource.

   (g) Criteria must be established for account eligibility, creation, maintenance, and expiration for each system.

(h) Information Custodians (i.e. system administrators) will periodically review user privileges and modify, revoke, or deactivate as appropriate, based on the above criteria.

(i) Inactivity timeouts will be implemented, where technically feasible, for access to sensitive information.

(j) Employee access to OPIC information systems will be limited to standard OPIC business hours, unless otherwise permitted by IRM for legitimate business purposes. Employees will not be permitted access to OPICNET during nightly scheduled backup periods.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for:

(1) Determining who should have access to their resources.

(2) Ensuring that their resources are protected against unauthorized access.

(3) Periodically reviewing access permissions.

(4) Ensuring that information users have undergone appropriate background checks and security training.

(b) Information Custodians are responsible for:

(1) Assisting information owners with controlling access to their resources.

(2) Promptly removing access from a system when requested.

(3) Reporting any unauthorized accesses that they discover.

(c) Information Users are responsible for:

(1) Understanding OPIC information resource access policies and procedures.

(2) Adhering to OPIC procedures for obtaining and removing access to information resources for themselves.

(3) Safeguarding their access credentials.

(4) Accessing only those resources for which they are authorized and using information in accordance with job function and agency policy.

(5) Immediately reporting suspected violations of this policy to their supervisor or the ISSO.

(6) Understanding the consequences of their failure to adhere to this policy.

(d) Supervisors are responsible for:

(1) Adhering to OPIC procedures for obtaining and removing access to information resources for their employees, contractors, and interns.

(2) Ensuring that their employees are authorized to access the resources needed to perform their duties.

(3) Notifying the ISSO when access privileges or accounts are to be removed.

(4) Immediately reporting suspected violations of this policy.

(e) The Information Systems Security Officer (ISSO) is responsible for:

(1) Auditing to ensure compliance with the procedures and guidelines specified in this policy.

(2) Ensuring that all personnel are trained on their computer security responsibilities.

(f) The OPIC Security Officer is responsible for ensuring that IT staff and IT contractors have undergone the appropriate background checks and security training.

6. **DEFINITIONS:**

(a) Access – The right to enter, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of specific information resources.

(b) Access Control – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

(c) Access Privilege (Privilege) – A specific activity that a user has been granted access to perform on an information resource (e.g. view or modify)

(d) Account – A set of privileges for authorization to system access, which are associated with a UserID.

(e) Authorization – The formal granting of access to an individual to perform certain activities.

(f) Least Privilege – Granting users only the minimum privileges required to provide the level of access needed to perform their official duties.

(g) Separation of Duties – Concept that provides the necessary checks and balances to mitigate against fraud, errors and omissions by ensuring that no individual or function has control of the entire process.

(h) System Permissions – The technical configuration that provides an individual the ability to perform certain actions on information resources.

(i) UserID – Character string (i.e. logon name) that uniquely identifies a computer user.

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) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

(d) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

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

(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.