PERSONNEL SECURITY

ISSP-16-0410

1. **SUBJECT:** Access to OPIC information resources is to be limited to only those persons who have been appropriately screened and authorized.
2. **SCOPE:** This policy applies all information owners, users and custodians.
3. **DESCRIPTION:** The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. Users, designers, implementers, administrators, and managers are involved in many important issues in securing information. It is important to ensure that the personnel who have access to OPIC's information resources can be trusted, to institute controls over the access provided to those personnel, and to implement procedures that minimize the personnel-related risks to OPIC's resources.
4. **PROCEDURES & GUIDELINES:**

(a) Any access granted to OPIC information resources will be based on the principles of separation of duties and least privilege, and in compliance with OPIC access control policies and procedures.

(b) Information users must have appropriate clearance for the sensitivity level of the resources which they are given access.

(1) Prior to being granted access to sensitive information resources, information users with no previous investigation and/or no recent, documented positive suitability determination must initiate and submit a Request for Background Investigation through the OPIC Human Resource Department (for employees) or the OPIC Security Officer (for contractors).

(c) Employees must be trained in the information security responsibilities and duties associated with their jobs.

(d) A detailed process will be implemented to manage user accounts, including processing requests for new accounts, establishing accounts, and closing accounts, as well as tracking accounts and user access authorizations.

(e) Procedures will be implemented for outgoing or transferring employees. These shall include, but are not limited to, the following:

(1) The removal of access privileges, computer accounts, and authentication tokens.

(2) The return of any OPIC information resources (property or data).

(3) Procedures for unfriendly termination that include the prompt removal of system access.

(f) Contractors must sign a non-disclosure agreement protecting any sensitive data to which the contractor requires access.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for the following for the resources they own:

(1) Determining who should have access their resources.

(2) Determining the level of screening required for access.

(3) Ensuring that personnel security policies and procedures are being followed.

(b) Information Custodians

(1) Follow OPIC procedures for adding and removing access for personnel to the resources they manage, including promptly deleting or disabling accounts when users terminate employment.

(2) Implementing least privilege and separation of duties for resources they manage.

(3) Verifying that employees have appropriate clearance for the resources to which they are being granted access, in accordance with clearance requirements set by information owners.

(c) Supervisors shall:

(1) Communicate to their personnel the security requirements outlined in this policy.

(2) Ensure all personnel are trained in the computer security responsibilities and duties associated with their jobs.

(3) Adhere to OPIC policies and procedures for adding and removing access for their employees.

(4) Ensure their contractors undergo the appropriate level of background screening

(d) Information Users shall:

(1) Understand their personnel security responsibilities and duties.

(2) Follow OPIC procedures for obtaining access to information resources.

(3) Promptly notify the information owner, information custodian, or their own supervisor when they no longer need access to a resource.

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

(1) Implement procedures to ensure that access to unclassified information via OPIC information systems is controlled pursuant to OPIC's security policies and procedures.

(2) Monitor the adherence to the personnel security policy.

(f) Human Resources Management is responsible for designating both the risk level and the sensitivity level for all competitive and excepted civil service positions, and for notifying the ISSO when background investigations have been completed.

(g) The OPIC Security Officer is responsible for designating both the risk level and the sensitivity level for all contractor positions, and for notifying the ISSO when background investigations have been completed.

6. **DEFINITIONS:**

(a) Access Privilege –An authorized ability to perform a certain action on a computer, such as read a specific computer file.

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

(c) Authentication Token – A hardware device, the possession of which can be verified, and which helps to confirm identity as part of the authentication process (*e.g.,* smartcard, SecureID)

(d) Least Privilege – A concept that means granting users only the minimum level of access they need to perform their official duties.

(e) Sensitive Data – Any data that is categorized as "sensitive" under OPIC's information resource classification policy and framework.

(f) Separation of Duties – Refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process or bypass security controls. Where feasible, the responsibilities of programmers, system administrators, database administrators, and system auditors should not overlap.

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) OPIC Directive 94-14, OPIC Security Program

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

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

(e) 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.