SYSTEMS DEVELOPMENT

ISSP-28-0410

1. **SUBJECT:** Security must be integrated into all phases of the System Development Life Cycle (SDLC).
2. **SCOPE:** This policy covers all systems at OPIC, whether purchased or developed internally.
3. **DESCRIPTION:** Each information system passes through multiple phases during its lifetime (SDLC), as it is planned. developed, deployed, operated, and retired. Specific security-related activities must occur in each phase to assure that the system is secure.

   It is usually more cost-effective to include preventive security measures from the start rather than to deal with security breaches later on. By considering security early in the information SDLC, OPIC will be able to avoid higher costs later on while also developing a more secure system from the start.
4. **PROCEDURES & GUIDELINES:**

   (a) Security must be considered in all phases of the SDLC and treated as an integral part of any system development or implementation project, including system modifications.

   (b) In each phase of the SDLC there are specific information security requirements that need to be met:

   (1) Initiation Phase:

   - Conduct sensitivity assessment (information, potential damage, laws and regulations, threats, environmental concerns, security characteristics, OPIC policy and guidance). The assessment shall consider which laws, regulations or policies establish specific requirements for the availability, integrity, and confidentiality of the system. The environmental (e.g., hazardous location) and public threats to the system or information should also be considered.
   - Perform preliminary Risk Assessment and incorporate the results into the decision-making process regarding the development/acquisition of the system.

   (2) Development/Acquisition Phase:

   - Security requirements shall be developed at the same time system planners define the other requirements of the system.
   - The security requirements shall be incorporated into design specifications along with assurances that the security features acquired can and do work correctly and effectively. The system's security design will be documented.

- Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified.
- A System Security Plan (SSP) is to be developed in accordance with OPIC System Secur ity Plan policy and procedures.
- Operational practices will be developed, including standard operational procedures and system-specific security policies (e.g., account management, backups, user training, etc.). A system handbook reflecting these practices should be developed.

(3) Implementation Phase:

- The system's security features will be configured and enabled.
- The system’s security management procedures will be implemented.
- The system will be tested and authorized for processing via OPIC’s Certification and Accreditation (C&A) process.

(4) Operation/Maintenance Phase:

- Perform the security activities outlined in the system security plan (e.g., performing backups, holding training classes, managing accounts.)
- Any changes made, or maintenance performed, on the system are to comply with OPIC’s Change Control and Patch Management policies and processes.
- Periodic security audits and vulnerability tests will be performed in accordance with OPIC Audit and Vulnerability Testing policies.

(5) Disposal Phase:

- Information may be moved to another system, archived, discarded or destroyed in accordance with OPIC data retention policies.
- Any storage media must be disposed of in accordance with OPIC’s Media Management policies.
- The disposition of software needs to be in keeping with its license or other agreements

(c) Each application must be categorized in accordance with OPIC’s Information Resource Classification policy, and provided protection appropriate to its level of sensitivity and criticality.

(d) System Testing:

(1) All systems will be thoroughly tested prior to being placed in the OPIC production operating environment.

(2) Sensitive data will not be used to test applications software until software integrity has been reasonably assured by testing with non-sensitive data or files.

(e) Documentation of sensitive systems must be provided the same degree of protection as that provided for the software.

(f) Application software used at OPIC must be obtained through authorized procurement channels and must comply with all licensing requirements.

(g) Systems must comply with all OPIC information security policies and procedures (e.g., system hardening, access control, backup and recovery, etc.)

(h) OPIC will adhere to NIST guidance as set forth in Special Publications 800-64, Security Considerations in the Information System Development Life Cycle, 800-12, An Introduction to Computer Security: The NIST Handbook, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for:

(1) Understanding the security requirements for each system life cycle phase.

(2) Implementing the life cycle security requirements for their systems.

(3) Documenting the security controls in the System Security Plan.

(4) Ensuring that security controls are incorporated in the design, development, and testing of contractor-developed software.

(5) Accrediting systems in accordance with OPIC C&A policy.

(b) Information Custodians are responsible for:

(1) Assisting Information Owners with the development and implementation of security controls.

(2) Ensuring that system security controls are implemented properly and operating as intended.

(3) Maintaining the system in accordance with all standard operating procedures and other approved security management processes.

(4) Assisting the ISSO with testing and auditing of the system.

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

(1) Assisting System Owners in addressing the security issues present in each life cycle phase.

(2) Providing baseline security requirements to be used for OPIC systems.

(3) Auditing to ensure that all systems are in compliance with this policy.

(4) Performing certification of systems in accordance with OPIC C&A policy.

6. DEFINITIONS:

(a) Media – Physical objects on which data can be stored, such as hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives, and tapes.

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

(c) System Development Life Cycle – The system development life cycle (SDLC) starts with the initiation of the system planning process, and continues through system acquisition/development, implementation, operations and maintenance, and ends with disposition of the system.

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

7. **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) Office of Management and Budget (OMB) Circular No. A-130, "Management of Federal Information Resources."

(d) Office of Management and Budget Memorandum M-00-07, "Incorporating and Funding Security in Information Systems Investments," February 28, 2000.

(e) Computer Security Act of 1987, P.L. 100-235 (1988).

(f) Federal Information Processing Standards (FIPS) Publication 73, Guidelines for Security of Computer Applications, June 1980.

(g) NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle.

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

(i) NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook.

(j) NIST Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach.

10. **LOCATION:** TBD

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

12. **REVISION HISTORY:** None

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