DATABASE SECURITY

ISSP-30-0410

1. **SUBJECT:** Securing information, so that it remains consistent, complete, and accurate, is essential to OPIC's reputation, mission, and critical business objectives.

2. **SCOPE:** This policy applies to all OPIC databases.

3. **DESCRIPTION:** OPIC has been entrusted with a variety of sensitive data to accomplish its goals. The success of agency programs depends on the availability, integrity and confidentiality of this data. In order to protect this data, OPIC must implement data security measures, such as data validation and verification controls. These controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets the expectations about its quality and that it has not been altered.

4. **PROCEDURES & GUIDELINES:**

(a) Data will be secured commensurate with its level of sensitivity and criticality.

(b) Databases, and applications that interface with databases, will be configured in accordance with security best practices:

(1) Integrity verification programs, such as consistency and reasonableness checks, shall be used to look for evidence of data tampering, errors, and omissions.

(2) Reconciliation routines (checksums, hash totals, record counts) shall be used to ensure software and data have not been modified.

(3) If users are allowed to make updates to a database via a web page, these updates should be validated to ensure that they are warranted and safe.

(4) For databases containing sensitive information, table access controls should be applied. Access to specific information within the database should be limited to only those personnel who need access to that information, and access should be limited to only those functions (e.g., read, write, modify, etc.) required for the person to perform his or her duties.

(5) Database servers should be configured to only allow connections from authorized, trusted sources (such as the specific web servers to which they supply information).

(6) For sensitive data, audit trails should be created and maintained within the database to track transactions and provide accountability.

(7) Securing sensitive information by selectively encrypting data within the database is encouraged.

(c) Programs or utilities that may be used to maintain and/or modify sensitive databases and other software modules that could affect or compromise the confidentiality, integrity, or availability of the data, must be carefully controlled.

(d) Databases containing non-public information should never be on the same physical machine as a web server.

(e) Databases (and database servers) that store public information cannot be used to also store non-public (e.g., private, proprietary, sensitive) information.

(f) Integrity errors and unauthorized or inappropriate duplications, omissions, and intentional alterations will be reported to the Information Owner.

(g) Database servers and database software must adhere to all OPIC information security policies and procedures pertaining to servers and systems, including patching, hardening, change control, authentication, etc.

(h) OPIC will follow NIST guidance regarding database security.

5. ROLES & RESPONSIBILITIES:

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

(1) Ensuring the confidentiality, integrity, and availability of the data.

(2) Ensuring that data integrity and validation controls are installed, operated and maintained.

(3) Authorizing and limiting access to data they own.

(4) Reporting database security incidents to the ISSO.

(b) Information Custodians are responsible for:

(1) Assisting Information Owners with maintaining the confidentiality, integrity, and availability of their data.

(2) Assisting Information Owners with implementing the prescribed database security controls.

(3) Immediately reporting breaches of database security to the Information Owner and the ISSO.

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

(1) Providing guidance to Information Owners and Custodians regarding database security.

(2) Auditing OPIC databases, servers, and applications to ensure compliance with this policy.

(d) Information Users are responsible for:

(1) Not accessing data that they are not authorized to access and/or for which they do not have a legitimate business need to know.

(2) Exercising due diligence to prevent accidental misentry, modification or deletion of data.

(3) Immediately reporting any security incidents to the Information Owner or Custodian.

(e) Supervisors are responsible for:

(1) Ensuring that their employees understand and comply with this policy.

(2) Reporting any suspected incidents to the ISSO and the Information Owner.

6. DEFINITIONS:

(a) Availability - Assuring information and communications services will be ready for use when expected

(b) Confidentiality - Assuring information will be kept secret, with access limited to appropriate persons.

(c) Data - A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.

(d) Database - An organized collection of logically related information stored together in one or more computerized files.

(e) Integrity - Assuring information will not be accidentally or maliciously altered or destroyed. Information has integrity when it is timely, accurate, complete, and consistent.

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

(g) Validation - The checking of data for correctness and/or for compliance with applicable standards, rules, and conventions.

(h) Verification - The process of ensuring that information has not been changed in transit or in storage, either intentionally or accidentally.

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) NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook." October 1995.

(e) NIST Special Publication 800-53, Recommended Security Controls for Federal Information 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.