BACKUP AND RECOVERY

ISSP-19-0410

1. **SUBJECT:** Backups of critical information resources must be performed, tested, and appropriately managed.
2. **SCOPE:** This policy applies to all OPIC information resources.
3. **DESCRIPTION:** There are many threats that exist which could cause the loss, corruption, or temporary unavailability of data. These include, but are not limited to, hardware failures, accidental deletion, incorrect modification, software corruption, and malicious activities. These threats are very common and it is inevitable that some of these events will occasionally occur at OPIC.

   It is therefore essential that OPIC maintain backup copies of all critical data and systems so that they can be used to provide the continued availability and viability of these resources when these events occur.

4. **PROCEDURES & GUIDELINES:**

   (a) All critical OPIC information resources will be backed up in a recoverable fashion.

   (b) Backups will be performed according to the following schedule:

      (1) All critical data and system configurations must be backed up on at least a daily basis.

      (2) Applications and licenses will be backed up whenever there are changes to them.

      (3) The backing up of non-critical data is at the discretion of the data owner.

   (c) Backups will be stored off-site in a secure, environmentally-controlled location at least 30 miles from the OPIC office.

   (d) Each system will have a defined backup retention schedule which complies with OPIC's data retention policies.

   (e) OPIC will periodically test the back up and restore procedures to ensure that data can be effectively restored from the backups.

   (f) OPIC will develop and implement detailed procedures for performing back ups restoring data, performing testing of backups, transferring tapes to/from the storage facility, and recycling or disposing of backups upon expiration of their retention period.

   (g) Backups will be treated with the same level of criticality and sensitivity as the data and applications stored on them.

   (h) Persons who have access to the backups, or who have access to perform back up or restore functions, must undergo appropriate background screening in accordance with OPIC Personnel Security policy prior to being given such access.

(i) Backup media (e.g., tapes) must be handled in accordance with OPIC Media Management policy.

(j) System custodians will back up data stored on their servers. However, information users are responsible for backing up any data stored on workstations and portable storage media (i.e., diskettes, flash drives, CDs, etc).

(1) Users may copy their data to servers to be backed up or may perform their own back ups of data not stored on OPIC servers.

(2) Backups made by users must be handled in accordance with OPIC Media Management policy.

(k) OPIC will follow NIST guidance regarding backups.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners will ensure that their resources are backed up in accordance with this policy.

(b) Information Custodians will assist Information Owners with backing up and restoring their resources.

(c) The Information Systems Security Officer (ISSO) will perform auditing to ensure compliance with this policy.

(d) Information Users will ensure that any critical data residing on their workstations or portable media are backed up in accordance with this policy.

6. DEFINITIONS:

(a) Back Up – The process of copying data to alternative or redundant media.

(b) Backup – A copy of data that is made in order to provide redundancy in case the original becomes corrupted or unavailable.

(c) Restore – The process of copying data from a previously-made backup to the original (or an alternate) system.

(d) Critical Data – Data which has been designated as "critical" under OPIC's Information Resource Classification policy.

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) 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.