# PHYSICAL AND ENVIRONMENTAL SECURITY

ISSP-17-0410

1. **SUBJECT:** Information resources require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation.
2. **SCOPE:** This policy prescribes the procedures, guidelines, and standards that govern the implementation of physical security measures designed to protect OPIC information resources. It does not govern protection of personnel, facilities, and property not directly associated with information technology, which are covered by OPIC Directive 94-14.
3. **DESCRIPTION:** It is crucial that OPIC implement physical security safeguards to protect its information resources. These safeguards must be applied in all administrative, physical, and technical areas and can include the use of locks, guards, administrative controls, and measures to protect against damage from intentional acts, accidents, fires, and environmental hazards.
4. **PROCEDURES & GUIDELINES:**

(a) Physical access to information resources is to be controlled commensurate with the classification of the resource and the level of risk.

(b) Areas containing sensitive information resources require special restrictions to limit access to these resources:

(1) Admittance to these areas is to be limited to personnel assigned to the area and persons who have been specifically authorized access to the area.

(2) Personnel assigned to the area must escort personnel without an appropriate security clearance.

(3) When uncleared personnel are present in these areas, sensitive information must be protected from observation, disclosure, or removal. This includes storing away documents and positioning all computer monitors to prevent viewing by unauthorized persons.

(4) Each person within a sensitive area, regardless of position, shall be subject to challenge by another OPIC employee, facility security personnel, or any law enforcement officer, and shall display appropriate identification when challenged. Failure to do so may result in removal from the facility or other administrative action.

(5) Areas containing sensitive information must be physically secured in accordance with OPIC facility security policies and OPIC Directive 94-14.

(c) Areas containing critical information resources require special protections to safeguard the availability of these resources:

(1) Protection must be implemented against fire, flood, humidity, electromagnetic disturbance, and other environmental factors that could damage the resources.

(2) Automated systems should monitor for environmental problems and alert specified personnel as appropriate.

(3) Smoke and fire detection systems with alarms must be installed in accordance with OPIC facility security policies and OPIC Directive 94-14.

(d) Specific requirements for the Computer Room (*i.e.*, "Data Center"):

(1) Comply with all requirements listed above.

(2) Install fire suppression equipment.

(3) Provide emergency power shutdown controls. Cover controls to prevent accidental activation.

(4) Equipment is to be located on a raised floor

(5) Provide an uninterruptible power supply

(6) Vendors and visitors are to be escorted at all times.

(7) All physical access to the room must be tracked.

(8) Annual testing will be performed on all fire, utility, and environmental alarms and protective systems.

(e) Backups and other media, both originals and copies, containing data and programs must be kept in good condition and protected from theft. It is important to keep backups in a separate location from the originals, not only for damage considerations, but also to guard against thefts.

(f) Other areas where physical access should be restricted are wiring closets and computer storage areas.

**5. ROLES & RESPONSIBILITIES:**

(a) Information Users are responsible for:

(1) Understanding and adhering to the security requirements prescribed in this policy

(2) Physically protecting the OPIC information resources entrusted into their possession.

(3) Reporting any incident or condition contrary to the specified requirements to the ISSO or OPIC Security Officer.

(b) Supervisors are responsible for:

(1) Ensuring that their personnel understand OPIC policy regarding physical and environmental security.

(2) Monitoring their employees' compliance with this policy.

(c) Information Owners are responsible for implementing measures to protect their resources against physical and environmental threats, as well as unauthorized physical access.

(d) Information Custodians are responsible for assisting information owners with implementing physical and environmental security measures.

(b) The Information Systems Security Officer (ISSO) is responsible for performing auditing to ensure compliance with these policies and guidelines.

(c) The OPIC Security Officer is responsible for ensuring the physical and environmental security of the OPIC facilities.

**6. DEFINITIONS:**

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

**7. ENFORCEMENT:** Anyone who violates this policy is subject to disciplinary action, up to and including termination of employment.

8. **POINT OF CONTACT:** OPIC Information Systems Security Officer (ISSO)

**9. ATTACHMENTS:** None

(a) **AUTHORITY:** 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 800-26, Security Self-Assessment Guide for Information Technology Systems.

**10. LOCATION**: TBD

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

**12. REVISION HISTORY:** None

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