CONTINGENCY PLANNING

ISSP-10-TBD

1. **SUBJECT:** OPIC will establish a comprehensive and effective program to ensure continuity of essential agency functions during a broad spectrum of emergencies or situations that may disrupt normal operations.
2. **SCOPE:** This policy applies to all major information systems and mission-critical applications.
3. **DESCRIPTION:** In addition to being a legal mandate for federal agencies, contingency planning is simply a good business practice, and part of the fundamental mission of OPIC as a responsible and reliable public institution. For the success of OPIC's programs, the agency's information systems must be available in the event of disruptions.

   OPIC's information systems are vulnerable to a variety of disruptions, ranging from mild (*e.g.*, short-term power outage) to severe (*e.g.*, equipment destruction, fire), and from a variety of sources ranging from natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of OPIC's risk management program, it is virtually impossible to completely eliminate all risks. In many cases, critical resources reside outside OPIC's control (such as electric power or telecommunications), and the agency may be unable to ensure their availability. Thus effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.
4. **PROCEDURES & GUIDELINES:**

   (a) OPIC will develop and maintain a viable contingency planning program for its major information systems and mission-critical applications.

   (b) The program will support OPIC's agency-level Continuity of Operations (COOP) Planning.

   (c) The program will yield documented plans on how OPIC would continue its mission and provide continuity of data processing if service, use, or access was disrupted for an extended period of time.

   (d) Each major IT system will have its own Contingency Plan, Continuity of Support Plan, or Disaster Recovery Plan.

   (e) Contingency planning will be based on business impact analyses that will identify and rank major information systems and mission-critical applications according to priority and the maximum permissible outage for each.

   (f) Preventive measures will be identified to reduce the effects of system disruptions and increase system availability.

   (g) Recovery strategies and procedures will be developed to ensure that systems may be recovered quickly and effectively following a disruption.

(h) Contingency plan testing and training will be held to address deficiencies and to prepare Information Owners and Custodians for plan activation.

(1) Testing will occur annually or when a significant change occurs to OPIC's major information systems or mission-critical applications.

(i) Contingency plans will be reviewed regularly and updated as needed to remain current with OPIC information technology enhancements.

(j) OPIC will adhere to NIST guidance as set forth in Special Publication 800-34, Contingency Planning Guide for Information Technology Systems and subsequent publications.

5. ROLES & RESPONSIBILITIES:

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

(1) assisting in identifying major information systems and mission critical applications.

(2) reviewing contingency plans to ensure they align with the overall agency COOP plan and information security policies.

(3) providing training, support and coordination for Information Owners and Custodians as they develop and coordinate contingency plans.

(4) ensuring that contingency plans are updated and tested annually.

(5) monitoring the contingency planning process and reporting progress to management as required.

(6) maintaining current copies of all contingency plans, tests, evaluations, and subsequent follow-up actions and making this information available as required.

(7) activating and coordinating established contingency plans during an emergency.

(b) Information Owners are responsible for:

(1) developing, reviewing, and testing system and application contingency plans for the resources they own.

(2) developing a strategy for providing adequate alternate processing capability based on the prioritization of major systems or critical applications which they own.

(3) providing personnel for contingency plan testing

(4) maintaining a list of the personnel involved in the disaster planning/recovery process, including their functions, roles, and assigned tasks.

(c) Information Custodians are responsible for:

(1) working with Information Owners and the ISSO to develop contingency plans.

(2) participating in contingency plan testing.

6. **DEFINITIONS:**

(a) Contingency Plan – Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

(b) Continuity of Support Plan (COSP) – The documentation of a predetermined set of instructions or procedures mandated by Office of Management and Budget (OMB) A-130 that describe how to sustain major applications and general support systems in the event of a significant disruption.

(c) Continuity Of Operations Plan (COOP) – A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

(d) Disaster Recovery Plan (DRP) – A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

(e) Disruption – An unplanned event that causes the system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

(f) Major Information System – An information system that requires special management attention because of its importance to an agency mission (and in this case mission critical business processes).

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) Presidential Decision Directive 67, Continuity of Operations, October 21, 1998.

(e) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(f) NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

(g) 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.