ACCEPTABLE USE OF INFORMATION RESOURCES

ISSP-01-0410

1. **SUBJECT:** Individuals using information resources belonging to the Federal government must act in a legal, ethical, responsible, and secure manner, with respect for the rights of others.

2. **SCOPE:** This policy applies to all users of OPIC information resources.

3. **DESCRIPTION:** Inappropriate use of information resources exposes OPIC to risks including compromise of systems and services, legal issues, financial loss, and damage to reputation. The purpose of this policy is not to impose restrictions that are contrary to OPIC's established culture of openness, trust and integrity, but to protect OPIC's employees and the government from illegal or damaging actions by individuals, either knowingly or unknowingly.

   Access to computers, computing systems and networks owned by the government is a privilege which imposes certain responsibilities and obligations, and which is granted subject to OPIC policies and guidelines, and governing laws. This policy sets forth the principles that govern appropriate use of information resources, and is intended to promote the efficient, ethical and lawful use of these resources. Individuals using information resources belonging to the government must act in a responsible manner, and with respect for the rights of others.

4. **PROCEDURES & GUIDELINES:**

   (a) Employees shall use OPIC-provided information resources for OPIC-related business in accordance with their job functions and responsibilities, except as otherwise provided by management directives or other OPIC policies.

   (b) As set forth in OPIC Directive 94-04, employees are permitted limited personal use of information resources if the use does not result in a loss of employee productivity, interfere with official duties or business, and involves minimal additional expense to the government. Unauthorized or improper use of information resources may result in loss of use or limitations on use of those resources.

   (c) When using government information resources, employees are expected to:

      (1) Act responsibly so as to ensure the ethical use of OPIC information resources in compliance with the Standards of Ethical Conduct for Federal Employees.

      (2) Acknowledge the right of OPIC to restrict or rescind computing privileges at any time.

      (3) Use security measures to protect the confidentiality, integrity, and availability of information, data, and systems.

      (4) Conduct themselves professionally in the workplace and to refrain from using government information resources for activities that are inappropriate.

(5) Respect all pertinent licenses, copyrights, contracts, and other restricted or proprietary information.

(6) Use good judgment in accessing the Internet. Each use of the Internet should be able to withstand public scrutiny without embarrassment to OPIC or the federal government.

(7) Safeguard their user IDs and passwords, and use them only as authorized. Any actions taken under an assigned identification (*e.g.*, userid) are the responsibility of the user.

(8) Respect government property.

(9) Make only appropriate use of data to which they have access.

(10) Exercise good judgment regarding the reasonableness of personal use.

(11) Use information resources efficiently.

(d) The following activities are strictly prohibited:

(1) Intentionally corrupting, misusing, or stealing software or any other computing resource.

(2) Accessing OPIC systems that are not necessary for the performance of the employee's duties.

(3) Performing functions that are not related to the employee's job responsibilities on systems that they are otherwise authorized to access.

(4) Making unauthorized changes to OPIC computer resources, including installation of unapproved software or interfering with security measures (such as audit trail logs and antivirus software).

(5) Copying OPIC proprietary software or business data for personal or other non-government use.

(6) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which OPIC or the end user does not have an active license.

(7) Disseminating trade secrets or business sensitive information, except as permitted by law or regulation.

(8) Transmitting, storing, or processing classified data except as authorized and in accordance with OPIC Directive 94-14, *OPIC Security Program*.

(9) Unauthorized access to other computer systems using OPIC information resources.

(10) Accessing information resources, data, equipment, or facilities in violation of any restriction on use.

(11) Using government computing resources for personal or private financial gain.

(12) Using another person's computer account, with or without their permission.

(13) Implementing any computer systems without authorization from IRM.

(14) Knowingly, without written authorization, executing a program that may hamper normal OPIC computing activities.

(15) Adding components or devices (e.g., PDAs, thumb drives, cameras, etc) to OPIC desktops without explicit approval from the Director of Technical Services.

(16) Introducing malicious programs into the network or server (*e.g.*, viruses, worms, Trojan horses, e-mail bombs, etc.).

(17) Revealing account passwords to others or allowing the use of one's account by others, including family and other household members when work is being done at home.

(18) Revealing system passwords (e.g. FPPS passwords, database passwords, etc) to anyone who is not specifically authorized to use them.

(19) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.

(20) Effecting security breaches or disruptions of network communication.

(21) Unauthorized security scanning, network monitoring, or data interception that is not part of the employee's regular job duties.

(22) Circumventing any OPIC information security measures.

(23) Interfering with or denying service to other information resource users.

(24) Providing information about, or lists of, OPIC employees to parties outside of the government that are not required for OPIC business.

(25) Sending unsolicited email messages (spam).

(26) Any form of harassment via email, telephone, pager, IRC, SMS, or other communication method, whether through language, frequency, or size of messages.

(27) Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.

(28) Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity without specific permission from OPIC.

(29) Posting agency information to external news groups, bulletin boards or other public forums without authority, or conducting any activity that could create the perception that communication was made in one's official capacity as a Federal government employee, unless appropriate Agency approval has been obtained.

(30) Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment.

(31) Using government office equipment or information resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. This includes, but is not limited to, materials related to:

- Sexually explicit or sexually oriented content
- Ethnic, racial, sexist, or other offensive comments
- Anything that is in violation of sexual harassment or hostile workplace laws
- Making fraudulent offers of products, items, or services.
- Gambling
- Illegal weapons or terrorist activities
- Planning or commission of any crime

(32) Forging or misrepresenting one's identity.

(e) Auditing and Privacy:

(1) All use of OPIC information resources may be monitored by OPIC.

(2) Employees do not have an expectation of privacy or anonymity while using any government information resource at any time, including accessing the Internet and email.

(3) Users agree to be governed by acceptable usage policies and to have their usage audited. By using government office equipment, employees imply their consent to disclosing the contents of any files or information maintained or passed-through government office equipment.

(4) To the extent that employees wish that their private activities remain private, they should avoid using agency office equipment such as their computer, the Internet, or E-mail, for those activities.

(5) Auditing procedures will be implemented to ensure compliance with OPIC security policies.

(6) System administrators have the ability to audit network logs, employ monitoring tools, and perform periodic checks for misuse.

(f) Employees agree to be bound by the following conditions for continued use of OPIC information resources:

(1) Employees and contractors will sign an agreement to comply with OPIC information security policy.

(2) Personnel with administrative access or elevated privileges to any IT resources will sign an Elevated Privileges Usage Agreement.

(g) Usage of OPIC IT resources for illegal purposes will be reported to appropriate authorities.

5. ROLES & RESPONSIBILITIES:

(a) Information Users are responsible for:

(1) Using information resources responsibly and in compliance with all OPIC information security policies and guidelines.

(2) Reporting any suspected inappropriate use of information resources to either their manager or the ISSO.

(b) Supervisors are responsible for:

(1) Ensuring that their personnel understand OPIC policy regarding acceptable usage of information resources.

(2) Monitor their employees' use of information resources.

(c) Information Owners are responsible for implementing measures to protect their resources against inappropriate use.

(d) Information Custodians are responsible for assisting information owners with implementing measures to protect their resources against inappropriate use.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing usage of the OPIC information resources to ensure compliance with policies and guidelines.

6. DEFINITIONS:

(a) Access - The right to enter or make use of a computer system. To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

(b) Administrative Access – Enhanced privilege level that allows the user to perform administration of the system.

(c) Account - A set of privileges for authorization to system access, which are associated with a userid.

(d) Information Resources - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

(e) Audit Trail - In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

(f) Information Custodians - Individuals (*e.g.*, IT staff) who maintain or administer information resources on behalf of Information Owners. They are guardians or caretakers who are charged with the resource owner's requirements for processing, telecommunications, protection controls, and output distribution for the resource.

(g) Information Owners - The individuals ultimately responsible for information resources, and are generally Departmental Vice Presidents or designated senior managers. The initial owner is the individual who creates, or initiates the creation or storage of, information. Once information is created or stored, the individual's respective OPIC business unit becomes the Owner, with the Departmental Vice President of that unit taking official responsibility.

(h) Information Users - Individuals who use or have access to OPIC's information resources, including employees, vendors, and visitors.

(i) Password - Any secret string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).

(j) Personal Use - Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

(k) System Administrator - A designated individual who has special privileges to maintain the operation of a computer application or system.

7. **ENFORCEMENT:** Unauthorized or improper use of government information resources could result in loss or limitations of use of these 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) OPIC Directive 98-02, Use of the Internet and Electronic Mail

(c) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

(d) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

(e) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(f) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

(g) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

(h) 5 C.F.R. Part 735, Employee Responsibilities and Conduct

(i) 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch

(j) Part 1 of Executive Order 12674, Implementing Standards of Ethical Conduct for Employees of the Executive Branch

11. LOCATION: TBD

12. EFFECTIVE DATE: October 22, 2004

13. REVISION HISTORY: None

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