ELECTRONIC MAIL

ISSP-29-0410

1. **SUBJECT:** Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.
2. **SCOPE:** This policy applies to the use of any OPIC information resource to transmit, receive or store electronic mail, as well as use of any non-OPIC email systems to transfer OPIC data.
3. **DESCRIPTION:** Electronic mail is an essential tool used by OPIC to conduct its business. Email is a vital method of exchanging messages and data files over computer networks.

   However, email is inherently insecure and presents many risks to OPIC information security. Email can be read, altered, or deleted by unknown parties without the permission of the person who sent or received the message. Email can also be used to distribute viruses and other harmful code that pose a threat to OPIC resources. Information users might also send inappropriate, proprietary, or other sensitive information via email, thus exposing OPIC to legal action or damage to its reputation. After web servers, an organization's mail servers are typically the most frequent targets of attack. Therefore, it is crucial to take prudent security precautions in administering and using email.
4. **PROCEDURES & GUIDELINES:**

   (a) Information Users must understand that email can be intercepted or altered without the knowledge of the sender or recipient when it is transferred over the Internet.

   (b) Sensitive information may not be sent over the Internet (via email or other means) without being encrypted. Sensitive information should be encrypted when transferred outside of OPICNET.

   (c) To ensure data is adequately protected, OPIC personnel may only send OPIC data via OPIC owned or operated email systems.

   (1) Permission may be granted by Management to use an alternate system in the case of an emergency.

   (2) OPIC information users are not permitted to forward OPIC email or attachments to personal accounts managed by public email or Internet service providers where the information might be compromised.

   (d) Information users are prohibited from using any OPIC email systems (or any other email systems accessed from OPIC computers) for prohibited purposes, as outlined in OPIC's Acceptable Use of Information Resources policy and Management Directive 94-04.

   (e) Information users may not direct unauthorized or personal messages to the All OPIC distribution group or other large groups of users.

(f) Emails should be deleted once no longer needed. Old emails that must be retained should be archived from the email server on a periodic basis.

(g) The following procedures should be used to avoid potential damage caused by email-borne computer viruses:

(1) All incoming emails should be scanned for viruses in accordance with the OPIC Antivirus policy.

(2) Information users should not open attachments or click on links in messages from senders they do not know.

(3) Information users should report all suspicious emails to the ISSO or the CSC.

(4) Emails containing executable attachments should be filtered and quarantined from entering the OPIC network.

(h) To minimize spam and avoid waste of OPIC resources, information users must avoid using their OPIC email addresses for personal correspondence on the Internet, particularly if they do not know or have a trust relationship with the other party. This especially includes giving out one's official email address to Internet shopping sites, bulletin boards, and mailing lists.

(i) Information users shall have no expectation of privacy while using OPIC's email system.

(j) OPIC will adhere to NIST guidance as set forth in Special Publication 800-45, Guidelines on Electronic Mail Security, and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that any email system they own, and the data they own which is transmitted via email, adhere to this policy and its associated procedures and guidelines.

(b) Information Custodians are responsible for assisting information owners in implementing the procedures and guidelines specified in this document.

(c) Information Users are responsible for adhering to the procedures and guidelines provided in this document.

(d) Supervisors are responsible for ensuring that their employees understand and adhere to the procedures and guidelines provided in this document.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing email systems and usage to ensure compliance with the procedures and guidelines provided in this document.

6. **DEFINITIONS:**

(a) 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.

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

(c) Spam – Unauthorized and unsolicited electronic mass mailings.

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) 5 U.S.C. 552A, Records Maintained on Individuals and The Privacy Act of 1974, as amended

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

(f) NIST Special Publication 800-45, Guidelines on Electronic Mail Security.

11. **LOCATION:** TBD

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

13. **REVISION HISTORY:** None

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