# MOBILE COMPUTING

ISSP-22-0410

1. **SUBJECT:** Laptops and other mobile computing devices require additional security controls to mitigate the risks posed by using them outside the OPIC office environment.
2. **SCOPE:** This policy applies to all laptops and other mobile computing devices that are used to store or process OPIC data.
3. **DESCRIPTION:** The use of laptop computers and mobile devices (such as PDAs) provide flexibility and enhanced communications that allow OPIC personnel to be more productive. However, the use of these devices outside of the OPIC office poses risks to those devices and the information they contain. These devices may also present a hazard to other OPIC resources upon their return to the OPIC office (for example, by spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the Internet or other networks outside of OPICNET which lack the protections afforded by OPIC's corporate firewall and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing.
4. **PROCEDURES & GUIDELINES:**

   (a) Laptops and other mobile computing devices must be inventoried and tracked.

   (b) Laptops must use antivirus and personal firewall software when connected to any network other than OPICNET.

   (c) Access to mobile devices which store or transmit sensitive data, or which can be used to connect to other sensitive OPIC systems, must be authenticated.

   (d) All security policies applied in the OPIC office environment must also be applied when using or connecting to OPIC resources outside the OPIC office environment.

   (e) Mobile computer users are responsible for backing up their data that is stored on the mobile computer on a regular basis.

   (f) OPIC sensitive data stored on laptops or other mobile devices is to be protected against unauthorized access via encryption or other appropriate measures.

   (g) OPIC will adhere to NIST guidance as set forth in Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, and subsequent publications.
5. **ROLES & RESPONSIBILITIES:**

   (a) Information Owners are responsible for ensuring that any mobile computing resources they own are being managed and used in accordance with the procedures and guidelines set forth in this policy.

(b) Information Custodians are responsible for assisting information owners with managing and protecting their mobile computing devices, including inventorying and tracking them, as well as defining security countermeasures that will be applied.

(c) Information Users are responsible for:

(1) Complying with the procedures and guidelines set forth in this policy.

(2) Taking all reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.

(3) Immediately reporting to the Customer Service Center the loss, theft, tampering, unauthorized access, or damage of any mobile device covered by this policy.

(d) Supervisors are responsible for ensuring that their employees understand and comply with these policies and guidelines.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing the use of mobile computing devices to ensure compliance with the procedures and guidelines set forth in this policy.

**6. DEFINITIONS:**

(a) Mobile Computing Device – A laptop, PDA, or other *portable* device that can store or process data.

(b) Personal Firewall – Software installed on a computer or device which helps protect that system against unauthorized access.

(c) Antivirus Software – Software that searches for evidence of computer virus infection and attempts to remove the malicious code and repair any damage the virus caused.

(d) Authentication – The process of verifying that a user is who he or she purports to be, via password, token or other credential.

**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) OPIC Directive 03-01, Telecommuting Program

(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) NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices

(f) 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.