INDIAN AFFAIRS
DIRECTIVES TRANSMITTAL SHEET

(modified DI-416)

DOCUMENT IDENTIFICATION NUMBER	SUBJECT	RELEASE NUMBER
65 IAM 4	Portable Device Use Policy	07-45
FOR FURTHER INFORMATION Office of Chief Information Officer		DATE

EXPLANATION OF MATERIAL TRANSMITTED:

This policy sets the guidelines for managing user privileges and the secure use of handheld devices issued. The use of portable devices such as Personal Digital Assistants (PDAs), laptops, and portable USB drives within the workplace is expanding rapidly. While providing productivity benefits, the ability of these devices to store and transmit corporate information through both wired and wireless networks poses potential risks to an organization's security.

Debbie L. Clark
Deputy Assistant Secretary – Indian Affairs (Management)

FILING INSTRUCTIONS:

Remove: None

Insert: 65 IAM 4

1.1 Purpose. This chapter establishes policy for managing user privileges and the secure use of handheld devices issued. The use of portable devices such as Personal Digital Assistants (PDAs), laptops, and portable USB drives within the workplace is expanding rapidly. While providing productivity benefits, the ability of these devices to store and transmit corporate information through both wired and wireless networks poses potential risks to an organization's security.

1.2 Scope. This policy applies to all Indian Affairs (IA) employees and contractors who use portable devices and the technical staff responsible for managing and maintaining those portable devices.

1.3 Policy.

A. General

a. Portable devices (laptops and PDA) shall not be used for IA business information unless the device has been configured with the necessary security controls as defined by the Division of Information Security and Privacy (DISP). Security controls include but are not limited to: password protection, encryption, and antivirus software.

b. The approving authority shall ensure that the procurement of a portable device supports the individual's responsibilities, and related productivity and responsiveness requirements such as:
   i. Telecommuting or traveling
   ii. Providing technical assistance
   iii. Accessing staff and managers who are not present at the worksite

c. Users shall refrain from sending or storing non-encrypted sensitive data on portable devices. Sensitive data requires protection due to potential harm resulting from inadvertent or deliberate disclosure, alteration, or destruction of the data.

d. IA shall maintain an inventory of all portable devices that are in use to include:
   i. Make, model, and serial number of each device
   ii. Name, location and telephone number of the person to whom the device has been issued
   iii. Description of the authorized use
   iv. Installed software applications

e. All documents related to portable device purchases, replacements, maintenance, service cancellation, property, and payment of monthly service fee (for PDA and cell phones) shall be periodically reviewed and maintained.

f. Users are required to setup the "owner information" screen on PDAs so that the device can be returned if found.

g. Users shall immediately report damage to, loss, or theft of a portable device to immediate supervisors and the IA IT Help Desk. The Help Desk staff will initiate the necessary actions to disable service to the PDA unit.
h. Sensitive information on the portable devices shall be purged on a regular basis in case it is stolen or misplaced.
i. IA management shall ensure that all portable device users receive training for the proper and secure use of portable devices, specifically PDAs and laptops. The training shall include:
    i. Familiarity with the basic operations of the device, including setting up password protection
    ii. Physical security of the device
    iii. Information that may be stored on the device
    iv. The procedure to follow if the device is lost or stolen
j. Users are not allowed to install any unauthorized software on portable devices. The device shall only be used for work-related activities.
k. The authentication mechanism of the portable device shall be in compliance with IA Identification and Authentication Policy. All devices shall require an authentication at startup, after a period of inactivity, and at regular intervals while active.
l. IA technical staff shall ensure that the portable device's network connections that are not in use shall either be disabled or protected. The network connections to verify are Bluetooth, Infrared, 802.11, CDMA and GPRS.

B. Prohibitions

a. Portable devices may not be used to enter or store passwords, safe/door combinations, personally identifiable information (PII), or classified, sensitive, or proprietary information unless that information is encrypted on the device with approved encryption methods.
b. PDAs and USB drives shall not be left unattended when attached to a computer.
c. Non-government owned portable devices shall not be connected to BIA systems.
d. IA information shall not be stored on non-government portable devices.

1.4 Authority.

A. Department of the Interior (DOI) Computer Security Handbook V1.0

B. Federal Financial Management Improvement Act of 1996 (FFMIA)

C. Federal Information Processing Standards (FIPS)

a. 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003

b. 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006

D. Federal Information Security Management Act of 2002 (FISMA)

E. National Institute of Standards and Technology (NIST)

a. Special Publication 800-53, **Recommended Security Controls for Federal Information Systems**

b. Special Publication 800-36, **Guide to Selecting Information Technology Security Products**

F. Office of Management and Budget (OMB)

a. **Circular A-130, Management of Federal Information Resources**, Appendix III, Security of Federal Information Resources, November 2000

b. M06-16, Protection of Sensitive Agency Information, June 23, 2006

1.5 Responsibilities.

A. Chief Information Officer and OCIO Staff are responsible for creating and/or revising information technology policies and ensuring that the information in the IAM for the programs and functions within their authority, including references and citations, is accurate and up-to-date.

B. Bureau Information Technology Security Manager (BITSM) shall ensure that the policy and processes in the IAM conform to applicable statutes, regulations, Federal standards, and policies.

C. Authorized IA Users, defined as IA employees, contractors, and other individuals who have been granted explicit authorization to access, modify, delete, or utilize IA information, shall adhere to this policy.

1.6 Sanction of Misuse. In accordance with 370 DM 752, personnel are individually responsible for protecting the confidentiality, availability, and integrity of data and information accessed, stored, processed, and transmitted. Individuals are accountable for actions taken on and with IA and BIA IT information resources. Failure to comply with this policy may lead to disciplinary action. Unauthorized disclosure of sensitive information may result in criminal or civil penalties.