MS 545 Mobile Information Technology Device Policy

Effective Date: January 7, 2013
Responsible Office: Office of the Chief Information Officer
Supersedes: 11/22/11

Issuance Memo 11/22/11
Issuance Memo 01/07/13

Table of Contents

1.0 Purpose

This Manual Section sets forth the security control standards for the issuance, administration, use, and security of mobile information technology (IT) devices that are used to conduct Peace Corps business. These standards are established to protect Peace Corps information on mobile IT devices, which consist of any non-stationary electronic apparatus with capabilities of recording, storing, and/or transmitting data, voice, video, or photo images and include laptops, personal digital assistants (PDAs), cellular phones, satellite phones, digital tablets, secure tokens, and any related storage media or peripheral devices (e.g. CDs, flash memory, Internet Air Cards, etc.).

2.0 Authorities

OMB Circular A-130, Clinger-Cohen Act, Federal Information Security Management Act, NIST SP 800-124, and NIST SP 800-53.

3.0 Policy

It is the policy of the Peace Corps to develop and maintain security control standards for all Peace Corps mobile IT devices and the information created, collected, and processed on behalf of Peace Corps on these devices. These standards are part of the overall Peace Corps Information Security Program authorized by MS 542 *Peace Corps Information Technology Security* and must be followed by all Peace Corps employees, including personal services contractors, contractor personnel, Volunteers, and Trainees. The Chief Information Officer (CIO) directs and oversees compliance with the security control standards for mobile IT devices.

4.0 Roles and Responsibilities

4.1 The Chief Information Officer

The CIO has overall responsibility for establishing the security standards for mobile IT devices and must:

(a) Procure all mobile IT devices for Peace Corps issuance.

(b) Assure that mobile IT devices are available for staff members with job functions that are mission critical to Peace Corps operations, or that protect the safety and security of Peace Corps staff or Volunteers.

(c) Provide for the distribution, operation, and administrative support of mobile IT devices.

(d) Maintain an inventory of IT devices issued by serial number, user's office, user's name, and service start/end dates.

(e) Configure all issued mobile IT devices in accordance with the Peace Corps Remote Access and Mobile Information Technology Guide.

(f) Establish and maintain security configurations for all issued devices, to include patching and upgrading of software/firmware.

(g) Log and monitor the activity on all the devices for compliance with the Rules of Behavior for General Users.

4.2 Supervisors

Supervisors of Peace Corps staff who have applied for, or have been issued, mobile IT devices must:

(a) Ensure compliance with managerial requirements as described in the Peace Corps Remote Access and Mobile Information Technology Guide.

(b) Sign and approve the Mobile IT Device User Agreement Form for each user that they supervise.

(c) Report the loss of any IT device containing Personally Identifiable Information to the Service Desk.

4.3 Users

Users who conduct official Peace Corps business on a mobile IT device must:

(a) Sign the Mobile IT Device User Agreement Form.

(b) Operate the device in compliance with this policy, all applicable federal requirements, and the Peace Corps' Remote Access and Mobile Information Technology Guide.

(c) Not process Classified information on the device.

(d) Use only approved and authorized Peace Corps owned devices on Peace Corps IT systems.

(e) Store only the minimum amount, if any, of Personally Identifiable Information (PII) and electronic Protected Health Information (ePHI) necessary to do one's work, and immediately delete the PII or ePHI when no longer needed. Notify Peace Corps supervisor or Service Desk of the loss or theft of an IT device containing such information.

(f) Exercise extra care to preclude loss, theft, or compromise of the device, especially during travel.

(g) Abide by all federal and local laws for using the device while operating a motor vehicle (e.g. users are banned from text messaging while driving federally owned vehicles, and text messaging to conduct Peace Corps business while driving non-government vehicles).

Users who are issued a mobile IT device by the Peace Corps must:

(a) Not disable or alter security features on the device.

(b) Use the device only for official government use and limited personal use.

(c) Contact the Peace Corps' Service Desk immediately if the device is lost, stolen, compromised, or non-functional.

(d) Reimburse the OCIO for any personal charges incurred that are above the established fixed cost for the Agency's use of the device.

5.0 Effective Date

The effective date is the date of issuance.