



MS 542

Peace Corps IT Security Policies and Procedures

Effective Date: 05/21/02

Supersedes: MS 542: 6/16/88

Responsible Office: Office of Management/ CIO and IRM

Table of Contents: Subsections

Subsection A	General Policies and Procedures	2
Subsection B	External Connections Policy	16
Subsection C	User Accounts Management Policy	19
Subsection D	Password Policy	24
Subsection E	Remote Access Policy	30
Subsection F	Computer Incident Response Capability	33
Subsection G	Electronic Mail Policy	38
Subsection H	Malicious Code: Prevention and Corrective Action	42
Subsection I	Web-based Services Policy	46
Subsection J	IT Security Awareness, Training, and Education	55
Subsection K	Certification and Accreditation Policy	59
Subsection L	Personnel Investigation Policy	66
Subsection M	Peace Corps Data Center Policy	72

Subsection A: General Policies and Procedures

1.0	Authorities	3
2.0	Purpose	4
3.0	Applicability	4
4.0	General Definitions	4
4.1	“Acceptable risk”	4
4.2	“Availability protection”	4
4.3	“Computer security”	5
4.4	“Computer system”	5
4.5	“Confidentiality protection”	5
4.6	“General support system”	5
4.7	“Individual accountability”	5
4.8	“IT”	5
4.9	“Major application”	5
4.10	“Media”	5
4.11	“Networks”	5
4.12	“Office”	6
4.13	“Operational controls”	6
4.14	“Rules of behavior”	6
4.15	“Sensitive information” and “Sensitive But Unclassified Information” (“SBU Information”)	6
4.16	“Sensitive system”	6
4.17	“Sensitivity”	6
4.18	“Server”	6
4.19	“Technical controls”	6
4.20	“Users,” “system users,” and “privileged users”	6
5.0	General IT Security Policy and Goals	7
5.1	Policies	7
5.1.1	General Policy	7
5.1.2	Waivers	7
5.1.3	Classified Information	7
5.1.4	Penalties for Noncompliance	7
5.1.5	Attachments: Approval Authority	7
5.2	Goals	8
6.0	IT Security Principles of Behavior	8

7.0	Rules of Behavior	9
7.1	Rules Applicable to All Users.	9
7.1.1	Rules on Access	9
7.1.2	Rules on System Integrity	10
7.1.3	Rules on Availability	11
7.1.4	Rules on Hardware and Software	11
7.1.5	Rules on Disposal	12
7.1.6	Rules on Unattended Equipment	12
7.1.7	Rules on Encryption of Sensitive Information	12
7.1.8	Rules on Reporting	12
7.2	Additional Rules for Specialized Users	13
7.2.1	Rules for Privileged Users and Administrators	13
7.2.2	Rules for Privileged Users of Public Access Systems	13
7.2.3	Rules for Program Managers and Country Directors	14
7.2.4	Policies for Volunteers	14
7.2.5	Rules for Departmental Point of Contact	15
8.0	Inspector General Audits and Reviews	15

1.0 Authorities

Statutes and Regulations

The Information Technology Management Reform Act (Clinger-Cohen Act) of 1996, 40 U.S.C. 1401 et seq; The Paperwork Reduction Act, 44 U.S.C. 3506; The Computer Security Act of 1987 (Pub. L. 100-235); The Government Information Security Reform Act (GISRA), Pub. L. 106-398 (2000); and The Federal Property Management Regulations, 101 CFR Part 35.

Presidential Directives and OMB Circulars and Memoranda

OMB Circular A-130 Appendix III (Management of Information Resources); OMB Memorandum 99-05 (Instructions on Complying with President’s Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records, July 1, 1999); OMB Memorandum 99-18 (Privacy Policies on Federal Web Sites, June 2, 1999); OMB Memorandum 00-13 (Policies and Data Collection on Federal Web Sites, June 22, 2000); Presidential Decision Directive 63, Protecting America’s Critical Infrastructures, May 22, 1998; Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.

Federal Standards

Federal Information Processing Standard Publications (FIPS Pub) 31, Guidelines for Automated Data Processing Physical Security and Risk Management; FIPS Pub 41, Computer Security Guidelines for Implementing the Privacy Act of 1974; FIPS Pub 73, Guidelines for Security of Computer Applications; FIPS Pub 83, Guidelines on User Authentication Techniques for Computer Network Access Control; FIPS Pub 87, Guidelines for ADP Contingency Planning; FIPS Pub 102, Guidelines for Computer Security Certification and Accreditation; FIPS Pub 112, Standard on Password Usage; National Bureau of Standards Special Publication 500-137, Security for Dial-Up Lines.

2.0 Purpose

This manual section sets out the minimum policies and practices governing the security of the Peace Corps' computer systems with the goal of preserving the integrity, availability, and confidentiality of the agency's computer information systems.

3.0 Applicability

3.1 This manual section applies to all Peace Corps employees, contract personnel, and Volunteer Leaders/Coordinators, both in the United States or overseas. Guidelines and policies governing Volunteer use of computers shall be separately issued by the Office of Information Resource Management (IRM). Country Directors may issue additional country-specific IT security policies and procedures, provided they are consistent with this manual section.

3.2 Overseas posts are subject to the policies and requirements of this manual section to the extent they have been provided with the appropriate equipment and have the technical capacity to do so. Posts that are still transitioning to the new electronic systems shall confer with their Regional Directors and the IT Security Program Manager for guidance on methods for securing their systems.

4.0 General Definitions

4.1 "Acceptable risk" is the level of risk responsible management is willing to accept based on its evaluation of the cost of implementing security controls.

4.2 "Availability protection" is the protection required to ensure the availability of the agency's IT systems. Such protection requires the backup of the system and its information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, and time and attendance, financial, procurement, or life-critical information.

4.3 “Computer security” is the protection afforded an automated information system in order to preserve the integrity, reliability, availability, and confidentiality of the system’s information resources, including its hardware, software, firmware (software stored on an ROM chip), information data, and telecommunications. The term applies to the entire spectrum of computer information technology, including its applications and support systems.

4.4 “Computer system” is any interconnected equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information. The term includes computers; ancillary equipment; software, firmware, and similar programs; services, including support services; and related resources.

4.5 “Confidentiality protection” is the protection required to protect the agency’s sensitive information. Such protection requires access controls such as user IDs/passwords, terminal identifiers, and restrictions on actions like read, write, and delete. Examples of information requiring protection include personnel, financial, proprietary, and certain internal agency information; and information related to investigations, other federal agencies, national resources, and high or new technology protected under an Executive Order or Act of Congress.

4.6 “General support system” is an interconnected technology resource that automates routine office functions. It normally includes hardware, software, information, data, applications, and communications, and provides support for a variety of users and applications. Individual applications support different mission-related functions. Users may be from the same or different offices.

4.7 “Individual accountability” is a requirement that individual users be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

4.8 “IT” is information technology.

4.9 “Major application” is an IT application that requires special attention to security due to the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might affect many individual application programs, including hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware and software where the only purpose of the system is to support a specific mission-related function.

4.10 “Media” means the magnetic materials used to store data.

4.11 “Networks” include communication capabilities that allow one user or system to connect to another user or system. Networks can facilitate communication between

computers within a system, or between computers in different systems. Examples of networks include local area network (LAN) or wide area networks (WAN), including public networks such as the Internet.

4.12 “Office,” for the purpose of this manual section only, includes any officially recognized Peace Corps program unit, regardless of whether it is formally designated as an office.

4.13 “Operational controls” are security methods that are implemented and executed by people. (*See* the definition of “technical controls” below.)

4.14 “Rules of behavior” constitute the requirements, practices, and controls (do’s and don’ts) governing the use, security, and acceptable level of risk of an IT system.

4.15 “Sensitive information” or **“Sensitive But Unclassified Information” (“SBU Information”)** is information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes: (1) information the improper use or disclosure of which could adversely affect the ability of an agency to accomplish its mission, (2) proprietary information, (3) information requiring protection under the Privacy Act, and (4) information protected from disclosure under the Freedom of Information Act. The term does not include classified information.

“Highly sensitive information” is a subset of a sensitive information that is defined/determined by the owner of the system, in this case, by the Peace Corps. This term includes information, the loss, inaccuracy, or unauthorized alteration of which could reasonably be expected to cause significant harm to a person or an organization, including death, injury, legal liability, or financial loss. Typically this information is personnel, investigative, or medical information.

4.16 “Sensitive system” is a system that processes, stores, or transmits sensitive information.

4.17 “Sensitivity” in an information technology environment, is the degree of confidentiality, integrity, and availability requirements of a system.

4.18 “Server” is a machine whose sole purpose is to store and supply data, so that other machines can use it. A server machine also responds to client processes or programs locally, or across a network.

4.19 “Technical controls” consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

4.20 “Users” or **“system users”** are all Peace Corps employees, contract personnel, and Volunteers Leaders or Coordinators, who use, manage, operate, or supply

services to the agency's computer systems. **"Privileged users"** are users who have special IT privileges, including the privilege to manage, control, provide services for, maintain, administer, and access or control access to the agency's IT systems.

5.0 General IT Security Policy and Goals

5.1 Policies

5.1.1 General Policy

It is the policy of the Peace Corps to ensure the security of the agency's computer systems, including the systems' physical components and the information stored within each system. The security requirements and procedures in this manual section are intended to establish measures that will eliminate or reduce the risk of security threats to the agency's systems to an acceptable level and protect against the financial and program costs that result when information is lost, compromised, or unavailable when needed.

5.1.2 Waivers

Unless otherwise provided, waivers from the requirements of this manual section may be approved and issued by the Director of the Office of Information Resources Management (IRM). Before issuing a waiver of any provision of this Manual Section, the Director of IRM shall ensure that appropriate substitute measures will be taken for a specified time period. The Director of IRM may issue a waiver for unusual circumstances when there is a business need to do so. Waivers must be in writing and shall be issued only for the time period deemed necessary by the Director of IRM. Other waiver provisions are found in Subsections K and L.

5.1.3 Classified Information

Classified information shall NOT be processed or stored on the agency's IT systems. *See* MS 833, which provides procedures for the handling of classified information.

5.1.4 Penalties for non-compliance

The policies in this manual section are based on and implement federal laws and regulations. As such, there are administrative, civil, and criminal consequences for non-compliance. Disciplinary action may be taken at the discretion of management for violations by IT users of the policies and procedures in this manual section.

5.1.5 Attachments: Approval Authority

Due to the rapid and ongoing changes to federal security procedures and technology capabilities, new or revised attachments to this manual section may be approved by the Chief Information Office in consultation with and after legal clearance by the Office of the General Counsel.

5.2 Goals

The IT security policies and procedures in this manual section are intended to help achieve three goals: the availability, integrity and confidentiality of the agency's systems.

Availability

Computer systems must be available for use in a timely fashion. Any denial of a system's use or substantial delay in a system's processing could adversely affect the ability of an individual, office, or program to conduct business. Accordingly, protections from physical destruction, theft, or virus outbreaks, for example, should be in place.

Integrity

The integrity of the information in the agency's computer systems must be maintained. To achieve its statutory purpose, the agency must be able to rely on the authenticity of the information maintained in its computer systems, such as financial records, e-mails, and program and administrative data. Integrity can be compromised by human error when entering data; when transmitting data from one computer to another; by software bugs or viruses; by hardware malfunctions, such as disk crashes; or by natural disasters, such as fires or floods. The integrity of the agency's systems should be protected by appropriate handling by the user and by utilizing a system architecture designed to protect data from corruption and recover lost or corrupted information.

Confidentiality

Sensitive information must be protected against unauthorized access or disclosure. Sensitive information is often included in legal, financial, national policy, budget, personnel, contractual, procurement, proprietary, or agency-critical information.

6.0 IT Security Principles of Behavior

The following eight principles of reflect federal laws and regulations, underlie the security policies and rules of behavior set out in this manual section, and apply to all Peace Corps system users.

- (a) **Accountability:** All system users are accountable for the appropriate use of the information resources entrusted to them and for complying with the policies and procedures set out in this manual section.
- (b) **Confidentiality of Sensitive Information:** Sensitive information shall be collected, maintained, disseminated and protected from disclosure to unauthorized individuals or groups, as required by law and the requirements of this manual section.
- (c) **Passwords and User Identification:** All system users must protect sensitive information through appropriate use of user identification (ID) and passwords.
- (d) **Hardware:** System users shall make reasonable efforts to protect computer hardware equipment for which they are responsible from damage, abuse, and unauthorized use. Computer hardware equipment includes Peace Corps-owned or leased hardware wherever located, including the user's place of residence or travel location.
- (e) **Reporting:** System users must promptly report all security violations, incidents, and vulnerabilities, in accordance with the procedures in this manual section.
- (f) **Privileged Users:** Privileged users shall exercise their special positions and computer use privileges in a responsible, professional, and ethical manner.
- (g) **Remote Users:** Remote users (those who operate computer systems in an alternate workplace) must take reasonable precautions at their alternate workplace to protect the systems' hardware, software, and information.
- (h) **Software:** Software, including shareware, public domain software, or similar programs, must be authorized prior to its use on Peace Corps computer systems. ALL authorized software must be from reputable sources. Licensing agreements are required for all non-standard software.

7.0 Rules of Behavior: The rules of behavior constitute the requirements, practices, and controls (do's and don'ts) governing the use, security, and acceptable level of risk of an IT system.

7.1 Rules applicable to all users

7.1.1 Rules on Access

The rules on access require users to:

- (a) Work only with data they have been authorized to use;
- (b) Limit the number of persons who can access their files or data;

- (c) NOT retrieve information from a system for someone who is not authorized to access the information;
- (d) Give information only to persons who have access authority and who need the information to perform their job;
- (e) NOT attempt to gain access to information they are not authorized to access;
- (f) NOT give their password to any person, including supervisors or the Help Desk staff;
- (g) NOT divulge Dial-up or Dial-back modem phone numbers to any person outside of Peace Corps (Dial-back modem lines are not normally allowed outside of the data center without approval); and
- (h) NOT download, install or run security programs or utilities that reveal weaknesses in the security of the system, such as password cracking programs, on Peace Corps computing systems. Security vulnerability tools are to be used by approved personnel ONLY and use must be limited to a pre-approved period of time.

7.1.2 Rules on System Integrity

The rules on system integrity require users to:

- (a) Immediately discontinue use of any PC or LAN system or software that shows any indication of being infected with a virus;
- (b) Protect against viruses and similar malicious programs by using only authorized software and ensuring that ALL incoming software comes from reputable sources.
- (c) NOT use shareware, public domain software, or similar programs without authorization;
- (d) NOT change the configuration of or attempt to modify or disable any of the security programs set up on their personal computers, including virus protection software and the password-protection function on screen savers;
- (e) Ensure that their software is enabled to scan all CDs and diskettes for viruses upon use; and
- (f) Check incoming e-mail attachments for viruses, especially attachments with .com, .bat, .zip, .exe, or .vbs extensions.

7.1.3 Rules on Availability

The rules on availability require users to:

- (a) Always store files on an approved network storage location. When the user is not connected to a server, the user shall make backups of locally-stored files until a connection to a server is made;
- (b) Write-protect backups;
- (c) Store backups away from originals;
- (d) Keep storage media away from devices that produce magnetic fields; and
- (e) Protect disks from spills.

7.1.4 Rules on Hardware and Software

The rules on hardware and software require users to:

- (a) Take reasonable steps to safeguard computer equipment against waste, loss, abuse, unauthorized use, and misappropriation;
- (b) Use only that equipment they have been authorized to use;
- (c) NOT eat, drink, or smoke near computer equipment or media in a manner that would endanger the equipment or media;
- (d) NOT store highly combustible materials near a computer;
- (e) NOT move or remove a PC, laptop, or other computer hardware without proper permission.
- (f) NOT allow a hard drive with any Peace Corps data to be removed from Peace Corps premises without the proper data destruction;
- (g) Take computer equipment from Peace Corps premises only for official purposes;
- (h) Promptly report missing computer property;
- (i) NOT allow anyone to perform maintenance on computer equipment without proper identification and authorization;
- (j) Only use software they have been licensed to use and only for authorized purposes; and

(k) For approved non-standard software, file the software licensing agreements with the vendor within five days of receipt. Such agreements must be signed, and include the software registration number, and a copy of all licensing agreements shall be kept by the purchasing office.

7.1.5 Rules on Disposal

In regard to the disposal of IT property, users shall give the following items to the Computer Security Coordinator for proper disposition:

- (a) Diskettes and/or tapes containing sensitive information that are no longer in use;
- (b) Damaged diskettes and/or tapes containing sensitive information; and
- (c) Computer systems with hard drives which contain sensitive information.

7.1.6 Rules on Unattended Equipment

The rules on unattended equipment require users to ensure that the equipment is properly secured when left unattended. Diskettes, printouts, and other material containing sensitive information must be placed in an appropriate storage container equipped with a lock. At the end of each work day, users must logout from their computers. Users are also prohibited by Section 7.1.2 (d), from changing the configuration of or attempting to modify or disable any security programs, such as screen saver and login passwords **requirements**, on their personal computers.

7.1.7 Rules on Encryption of Sensitive Information

In regard to sensitive information transmitted across any public communications system, such as the Internet, including information sent over the e-mail system, users shall ensure that an encryption package, approved by the National Institute of Standards and Technology (NIST), is used to encrypt the information.

7.1.8 Rules on Reporting

The rules on reporting require users to:

Report all security violations, incidents, and vulnerabilities to the Peace Corps Information Technology Security Program Manager (IT Security Program Manager) and notify their supervisors, as set out in the incident response procedures in Subsection F. If they are unable to contact the IT Security Program Manager, they shall call the Help Desk to record the incident.

7.2 Additional Rules for Specialized Users

7.2.1 Rules for Privileged Users and Administrators

Privileged Users and Administrators shall:

- (a) Protect “privileged accounts passwords” at the highest level demanded by the sensitivity level of the system (privileged accounts passwords include the supervisor, root, and administrator or equivalent, passwords);
- (b) Develop or run programs for work purposes only;
- (c) Help train users on the appropriate use and security of the system;
- (d) Watch for unscheduled or unauthorized programs;
- (e) Track and notify appropriate staff of all security incidents occurring within their area of responsibility;
- (f) Take action to reduce damage caused by security incidents, such as, locking up property, logging out of a terminal, and disconnecting a PC with a virus; and
- (g) Establish virus protection for servers that are available to the public (Internet servers), when possible.

7.2.2 Rules for Privileged Users of Public Access Systems

Privileged users of public access systems, such as the Internet, shall:

- (a) Transmit, store, or post sensitive information across public access systems ONLY if the information is encrypted or the user is using an encrypted, or otherwise trusted path;
- (b) Use virus protection software when receiving information from a public access system;
- (c) Get official approval for any Web pages placed on the Internet;
- (d) Ensure that information placed on a public access system is approved in accordance with Peace Corps’ policies regarding content and security;
- (e) Ensure that information placed on a public access system is up-to-date, accurate, and true;

- (f) Ensure that information placed on a public access system reflects the policies of the agency; and
- (g) Ensure that any distribution or receipt of documents via public access systems does not violate any applicable copyright laws.

7.2.3 Rules for Program Managers and Country Directors

Program Managers and Country Directors shall:

- (a) Notify security personnel and the Departmental Point-of-Contact whenever the status of a system user terminates or changes;
- (b) Ensure continued availability of data when a system user terminates by obtaining the user's password, ID, keys to encrypted files, and the user's documentation of tasks;
- (c) Advise a terminating user of the responsibility to keep sensitive information confidential;
- (d) Terminate the user's access to information and computer systems immediately, in the event the system user is separated;
- (e) Report the threat or likelihood of sabotage, as the result of, for example, an unfriendly termination or separation;
- (f) Ensure that system users are given adequate and appropriate training in the Peace Corps IT Security Awareness, Training, and Education Program;
- (g) Ensure that IT security is and remains a highly visible aspect of day-to-day operations;
- (h) Appoint a computer security coordinator;
- (i) Assign responsibility for the security of each IT system to the computer security coordinator; and
- (j) Assure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the development or acquisition of IT equipment and software.

7.2.4 Policies for Volunteers

The only Peace Corps-provided computer resources Volunteers may use are those specifically designated for Volunteer use. Guidelines and policies regarding

Volunteer use of computers can be found in other documents, including “Mandatory Guidelines for Volunteer Computers.”

7.2.5 Rules for Departmental Point-of-Contact

The Departmental Point-of-Contact shall notify appropriate account management staff and IRM System Administrators by utilizing the Personnel Tracking System (PTS) whenever a system user terminates or changes status.

8.0 Inspector General Audits and Reviews

The Inspector General shall conduct periodic audits or reviews that test the adequacy of the agency’s security safeguards of its sensitive systems, and shall advise the applicable program manager of any problems concerning the application or efficacy of the safeguards.

Subsection B: External Connections Policy

11.0	Purpose	16
12.0	Applicability	16
13.0	Policy	16
14.0	Requirements	16

11.0 Purpose

This policy sets out the Peace Corps' minimum security standards for connecting any Peace Corps computer or network to a non-Peace Corps organization. Peace Corps-to-Peace Corps connections using NON-dial-up methods, i.e., wireless, DSL, cable, and other similar methods, are also included in this policy.

12.0 Applicability

This policy is applicable to all Peace Corps owned, leased, and operated computers and networks, including stand-alone and laptop computers.

13.0 Policy

Peace Corps computer or network connections to non-Peace Corps organizations shall generally be made through the Peace Corps Local Area Network/Wide Area Network (LAN/WAN), which is administered by the Office of Information Resources Management (IRM).

14.0 Requirements

14.1 Peace Corps offices that have, or wish to establish, a computer or network connection with a non-Peace Corps organization must submit a request for approval to the Director of IRM. The request shall include information on the type of connection to be established and the business purpose for the connection, and shall certify that the minimum security standards identified in Section 14.2 are met.

14.2 No Peace Corps computer or network shall be connected to, or have the capacity to be directly connected to, any non-Peace Corps organization, unless the organization has the following security measures in place:

- (a) Fire walls;
- (b) Anti-virus software, if applicable;

- (c) The means to ensure that anti-virus software is kept up to date, if applicable;
- (d) A memorandum of understanding (MOU) that sets out the terms, configurations and dates when the connections and the security safeguards will be in place as outlined in Section 14.4 of this policy; and
- (e) A security plan that is certified by the connecting organization.

14.3 Once a year, all Peace Corps offices that have established external connections with non-Peace Corps organizations shall conduct an inventory of external connections and then provide a report of the inventory to the IT Security Program Manager. The report shall include the type of connection and the business purpose for that connection, and shall certify that the minimum security measures identified in Section 14.2 are in place.

14.4 Memorandum of Understanding

The MOU between the Peace Corps and a non-Peace Corps organization shall include:

- (a) A list of interconnected computer systems, including the Internet;
- (b) A list of unique system identifiers, if appropriate;
- (c) The name of each system;
- (d) The name of the organization owning each non-Peace Corps system;
- (e) The type of interconnection (e.g., TCP/IP, Dial, SNA);
- (f) A short summary of major concerns or considerations in determining the interconnection;
- (g) The name and title of authorizing management officials for both Peace Corps and the non-Peace Corps organization;
- (h) The signature of authorizing management officials for both Peace Corps and the non-Peace Corps organization;
- (i) The date the MOU was authorized and approved;
- (j) A list of any Privacy Act systems of records, if applicable;
- (k) The sensitivity level of each system;
- (l) A description of the interaction among systems; and

(m) Rules of behavior and any security concerns.

Subsection C: User Accounts Management Policy

17.0	Purpose	19
18.0	Definitions	19
18.1	“Account Manager”	19
18.2	“Personnel Tracking System”	19
18.3	“Departmental Point-of-Contact”	19
19.0	Policy	20
20.0	User Account Management: General	20
20.1	Authentication of Identity	20
20.2	Standard Operating Procedures	20
20.3	Operating Procedures for Specialized Systems	21
21.0	Roles and Responsibilities	22
21.1	Account Holders (users who have accounts)	22
21.2	Account Managers	23
21.3	Program Managers	23
21.4	IT Security Program Manager	23

17.0 Purpose. The user accounts management policy sets out minimum security standards for user accounts and user access to sensitive information.

18.0 Definitions

18.1 “Account manager” means a technical user who grants or restricts access to a given computer system.

18.2 “Personnel Tracking System” is an agency-maintained database consisting of a series of records that contain contact information about each employee. These records control changes to the staff telephone directory and facilitate payroll from the National Finance Center.

18.3 “Departmental Point-of-Contact” is the person(s) for each office who is designated to make necessary changes in the agency’s personnel tracking system and submit Help Desk tickets for services required when, for example, an employee begins or terminates employment or is transferred.

19.0 Policy

Before a potential user may access any agency computer system that contains sensitive information, the identity (ID) of the user must be authenticated, and the user must be approved for access and be assigned an initial password for access to the system. A “user account” that tracks, regulates, and secures a user’s identity and passwords is established for each user. A separate account is established for each system accessed by a user.

20.0 User Account Management: General.

20.1 Authentication of Identity

Authentication of a user’s identity is the first step in setting up a user account and is commonly accomplished with such methods as the use of physical keys, account names, passwords, and biometric checks. Acceptable security mechanisms that could be used to identify and authenticate a user’s identity include:

- (a) Password based mechanisms;
- (b) Smartcards/smart tokens based mechanisms;
- (c) Biometrics based mechanisms;
- (d) Password generators;
- (e) Password locking;
- (f) PC or workstation locking;
- (g) Termination of connection after multiple failed logins; and
- (h) Cryptography with unique user keys.

20.2 Standard Operating Procedures

Account Managers shall draft standard operating procedures for each sensitive computer system they manage. The procedures shall describe the method used to verify the identity of the potential user and the method used to periodically review and verify the accounts on the system for appropriate access rights and account status. They shall also describe how the process will be implemented and who is responsible for the implementation. For a system without the technical capacity to perform the function required under this section (20.2) a manual procedure may be implemented.

Standard operating procedures shall include:

- (a) Creating a new account**

A description of the process used to initiate, verify and create a new user account. Users shall be required to change initial passwords before login will be allowed. All users must have a valid username and password. All usernames must be assigned to a specific user. Generally, only individual accounts for users will be allowed. Requests for shared accounts shall be directed to the Help Desk and must be approved by the IRM Director;

(b) Selecting user names

A description of each account's naming convention, that is, how user names are selected (Each system's naming convention shall be documented);

(c) Changing accounts

A description of the process for changing names or access privileges of an existing account. This is sometimes necessary, for example, when a user changes positions within the agency. Before a user account may be changed, the user's access approval must be independently verified;

(d) Disabling/suspending accounts

A description of the process for disabling or suspending a user account, including the method used to periodically review and verify the accounts on the system for appropriate access rights and account status; and

(e) Suspension dates

Each system account shall have a suspension date set when it is created, unless the system lacks the technical capacity to do so.

20.3 Operating Procedures for Specialized Systems

In addition to the standard operating procedures described in Section 20.2, additional procedures are required for certain systems, as set out below:

(a) Network systems

Network systems, which includes file and print sharing, electronic mail and mainframe, shall have the following additional standard operating procedures:

- (1) New users of network systems are required to read Sections 5.0 through 7.2.4 which set out the agency's basic security guidelines, and sign a verification that they have done so before they may have access to the network (*See Attachment A for the agency's verification form*); and

(2) All network accounts shall be given a suspension date when they are created that shall correspond to the expected term of the user's employment. User accounts are required to be disabled or suspended when a user will be absent from work for more than 60 days. Verification of the extension of a user's term of employment is required before an account may be re-enabled. Account managers must remove accounts left in suspension for more than 90 days.

(b) Web-based systems

Web-based systems, which includes accounts created on Extranet servers, shall have the following additional standard operating procedure:

The suspension date of Web accounts shall be set for one year from creation of the account. The suspension date shall be changed only when the account user is re-verified as requiring access. Account managers shall remove accounts left in suspension for more than 90 days.

(c) Application Systems

Application systems, which reside in various locations within the agency's computer system, including the mainframe, Web server, and personal computers, shall have the following additional standard operating procedures:

(1) The suspension date of an application account shall be the date in the particular application's standard operating procedures. The date may be changed only when the user assigned to the account has been re-verified as requiring access. Application accounts shall be disabled or suspended when a user will be away for more than 60 days. Account managers shall remove accounts left in suspension for more than 90 days.

(2) A signed agreement shall be obtained from potential users of *highly*-sensitive application systems that they will abide by the principles and rules of behavior for the particular system before gaining approval for access.

21.0 Roles and Responsibilities

21.1 Account Holders (users who have accounts)

Account holders shall:

(a) Protect their individual account IDs and passwords. It is a violation of Peace Corps policy for users to share their IDs or passwords;

(b) Notify their system manager when they need a change in their account status, such as, a name change or extended absence; and

(c) When appropriate, notify the IT Security Program Manager in accordance with the Computer Incident Response Capability Policy and Procedures in Subsection F of this manual section.

21.2 Account Managers

Account Managers are responsible for:

- (a) Drafting and adhering to their standard account management operating procedures and keeping the procedures up-to-date; and
- (b) Expeditiously removing or disabling accounts, when necessary. When appropriate, they shall notify the IT Security Program Manager in accordance with the Computer Incident Response Capability Policy and Procedures in Subsection F of this manual section.

21.3 Program Managers

Program Managers are responsible for:

- (a) Notifying their account managers or departmental point-of-contact of the need for new accounts to be created and the appropriate permissions or rights to be assigned to new accounts;
- (b) Notifying their account manager or departmental point-of-contact of a change in an existing account status for a supervised employee or contractor, such as name changes or extended absences; and
- (c) Expeditiously notifying account managers of the need for accounts to be removed or disabled. When appropriate, program managers shall notify the IT Security Program Manager in accordance with the procedures set out in Subsection F of this manual section, *Computer Incident Response Capability*.

21.4 IT Security Program Manager

The IT Security Program Manager:

- (a) Is responsible for periodically reviewing the standard operating procedures and the controls and processes used by the account managers to manage user accounts; and
- (b) Will prepare a Computer Security Incident Report in accordance with the Computer Incident Response Capability policy and procedures in Subsection F of this manual section.

Subsection D: Password Policy

25.0	Purpose	24
26.0	Applicability	24
27.0	General Policies	24
28.0	Policies for Sensitive Systems	25
29.0	Types of Passwords: Technical Requirements	25
29.1	Operating System Passwords	25
29.2	Mainframe Passwords	26
29.3	Privileged Account Passwords	27
29.4	Service Account Passwords	27
29.5	Application Passwords	28

25.0 Purpose. The purpose of the password policy is to provide agency security standards for passwords used to authenticate a user's access to sensitive information in the agency's computer systems as required by the Federal Information Processing Standard 112, *Password Usage*.

26.0 Applicability

This policy applies to all users of the agency's sensitive computer systems.

27.0 General Policies

27.1 It is the policy of the Peace Corps to limit access to the agency's computer systems to authorized users. To control access to its systems, the agency shall issue passwords to all system users and shall use access control methods contained within and controlled by the operating systems, security subsystems, or database management systems (e.g., file attributes, access control lists, security rules, object-oriented security labels, and database schemes). Stored passwords shall be encrypted using a NIST- approved secure encryption method and systems will be programmed so that passwords will not be displayed on the monitor. In addition, each operating system shall be programmed to automatically require re-authentication of the user's ID after a specified period of inactivity has been detected.

27.2 Each system user will be issued a password and a user ID for accessing the agency's computer systems. Users shall take reasonable precautions to protect their passwords and IDs and shall not share them with any person and shall never display their passwords on the monitor.

27.3 The agency reserves the right to monitor compliance with its password policy by installing or running security programs or utilities which have the capacity to reveal misuse of a password by individual users. If technically feasible, each operating system and application control shall be programmed to monitor compliance with this policy.

28.0 Policies for Sensitive Systems

28.1 Peace Corps contractors with Peace Corps IT responsibilities must ensure that all Peace Corps multi-user sensitive information systems, desktops, and laptops under their purview have and use a password mechanism that authenticates the identity of each person who accesses any of the sensitive systems for which they are responsible. This does not apply to personal digital assistants (palm pilots) or those information systems intended for unrestricted public access, such as Web servers.

28.2 Each office within the agency with a computer system that includes sensitive information:

- (a) Shall designate an individual to be responsible for implementation of the password policy;
- (b) Is restricted from using clear-text reusable passwords; and
- (c) Is responsible for documenting a procedure that verifies the identity of a new user before issuing the user's initial password.

29.0 Types of Passwords: Technical Requirements

29.1 Operating System Passwords

- (a) An initial password for accessing the network will be issued to each user by a system administrator. The system administrator shall verify the user's identity according to the Accounts Management Policy in Subsection C of this manual section before issuing the initial password. After accessing the system with the initial password, the user shall select a new password. New passwords may contain some non-alpha/numeric characters.
- (b) A user operating system password:
 - (1) Shall have a minimum length;
 - (2) Shall have a preset lifetime (Systems shall have an automated mechanism to ensure that users change their passwords at a pre-set interval. For systems without the technical capacity to do so, a manual process must be used to ensure compliance with this requirement.);

(3) Shall be changed as soon as possible, but within one business day after a password has been or is suspected of being compromised, or in response to a management directive; and

(4) Shall be suspended after a pre-determined number of invalid password attempts.

(c) Password Reuse

For systems without the technical capacity to do so, the system shall be protected against reuse of a network password by a given user. The system will store used passwords for a given user. *See* § 3.2 for exemptions for overseas posts.

29.2 Mainframe Passwords

29.2.1 An initial password for accessing the mainframe will be issued to each user by the system administrator (Peace Corps' mainframe includes two operating systems: VM and VSE. Each operating system includes various application systems.). The system administrator shall verify the user's identity before issuing the password.

29.2.2 A user must first enter a valid network password. Then the user shall enter the initial mainframe password provided by the system administrator. Users will then be required to select a new mainframe password after signing on with the initial password.

29.2.3 To access applications within the two operating systems in the mainframe (VM and VSE), a user also needs an application password for each application. *See* Section 29.5 in this subsection.

29.2.4 For systems with the technical capacity to do so, application passwords shall be at least six characters in length. For systems without the technical capacity to do so, the mainframe passwords shall be at least four characters in length.

29.2.5 All mainframe application passwords shall have a maximum password lifetime of 90 days. Systems with the technical capacity to do so shall have an automated mechanism to ensure that users change their passwords at an interval not greater than 90 days. In addition, passwords shall be changed:

(a) As soon as possible, but within one business day after a password has been or is suspected of having been compromised; or

(b) In response to a management directive.

29.2.6 Unless they lack the technical capacity to do so, all systems with password access shall be set to suspend password log-ins after five invalid attempts.

29.2.7 Unless they lack the technical capacity to do so, mainframe systems shall be protected against reuse of a password by a given user. The mainframe systems shall be set to store five previously used passwords for a given user.

29.3 Privileged Account Passwords

29.3.1 Access to a privileged account by a system administrator must first be approved by the Director of IRM. (A higher level of authentication is required for access to a privileged account due to the extraordinary capabilities and powers inherent in this level of access.) System administrators may then issue their own passwords.

29.3.2 Password Selection

The general process for selecting an account password is set out in Section 29.1. In addition, a privileged account password shall:

- (a) Be at least twelve characters in length; and
- (b) Have a maximum lifetime of 90 days (Systems shall have an automated mechanism to ensure that users change their passwords at an interval not greater than 90 days. If automated mechanisms are not technically possible, a manual process must be used to ensure compliance with this requirement); and
- (c) Be protected against reuse of a password by a given user. The system will store up to five previous passwords.

29.4 Service Account Passwords

29.4.1 Service account passwords are passwords already programmed into a computer system to permit the automatic transfer of information from one computer server to another without the assistance of a user.

29.4.2 The process for selecting a password is set out in Section 29.1.

29.4.3 All service account passwords shall also have:

- (a) At least 12 characters; and
- (b) A maximum lifetime of one year.

29.4.4 Unless the system lacks the technical capacity to do so, it shall be protected against the reuse of a service account password. Service account passwords shall not be reused within a five-year period.

29.4.5 Auto-logout features shall not be used where a user's ID and passwords are maintained on the system in script form (clear text executable instructions or parameter values) or where the system does not require the user to enter the information for identification and authentication purposes.

29.4.6 No service account shall be configured to log on interactively to a network device, unless the system lacks the technical capacity to comply.

29.4.7 All vendor-supplied or developer-supplied default passwords (passwords provided for initial entry to a system) shall be changed before any product is put into use.

29.5 Application Passwords

29.5.1 Applications reside in various locations within the agency's computer system, including the mainframe, Web server, and personal computers. To gain access to an application that contains sensitive information, a user must enter a valid application password.

29.5.2 An initial application password will be issued to the user by a system administrator after the administrator verifies the user's identity in compliance with the agency's User Accounts Management Policy in Subsection C. To access an application, the user must first enter a valid network password and then enter the initial application password provided by the system administrator. The user must then select a new application password.

29.5.3 Passwords for existing applications shall be at least four characters in length. When existing applications are revised or new applications are added to the system, passwords for the revised or new applications must be at least six characters in length.

29.5.4 All application passwords shall have a maximum lifetime of 90 days. When possible, systems shall have an automated mechanism to ensure that users change their passwords on time. If the system lacks the technical capacity to have an automated mechanism, a manual process shall be used. Passwords shall also be changed:

- (a) As soon as possible, but within one business day after a password has been or is suspected of having been compromised; or
- (b) In response to a management directive.

29.5.5 Unless the system lacks the technical capacity to do so, the computer system shall be protected against reuse of an application password by a given user. To protect against reuse, the system shall store up to five previous passwords.

Subsection E: Remote Access Policy

34.0	Purpose	30
35.0	Definition/Applicability	30
36.0	Policies	30
36.1	General Policies	30
36.2	Access From Overseas Locations	31
36.3	Technical Support	31

34.0 Purpose

The purpose of the remote access policy is:

- (a) To ensure the security of the agency’s computer systems when the systems are accessed by users from a location other than their official work sites; and
- (b) To provide reasonable access to the agency’s computer systems for dial-up remote access users.

35.0 Definition/Applicability

“**Remote access**” is used in this policy to mean the establishment of a dial-up computer communications connection by a Peace Corps user through or to Peace Corps offices from anywhere other than the user’s official work location. Peace Corps-to-Peace Corps connections using NON-dial-up methods, i.e., wireless, DSL, cable, and other similar methods, are included in the External Connections policy. This remote access policy is applicable to all Peace Corps owned, leased, and operated computers and networks, including stand-alone and laptop computers.

36.0 Policies.

36.1 General Policies

36.1.1 Remote access is available only to authorized users, as approved by their office head and either the Chief Information Officer (CIO) or the IRM Director. Approved use of remote access is for business use only. Approval to use remote access does not, in itself, constitute approval for extension of regular working hours or overtime approval. Non-business hour use of remote access must not conflict with authorities and procedures contained in MS 630.

36.1.2 Only Peace Corps computers, communications equipment, and software systems may be used for permissible dial-up remote access. The use of

personally-owned computers or communications equipment or software is specifically prohibited.

36.1.3 Individual user IDs and passwords are required for remote access. The selection and use of user IDs and passwords is governed by the Peace Corps Password Policy in Subsection D of this manual section.

36.1.4 Any approval granted for remote access shall be made to a specific individual for specific purposes. Approval shall not be transferred under any circumstances or used for any purpose other than those specifically stated in the approval.

36.1.5 Total log-on/connect time is governed by the Laptop Dial-Out Procedures For Domestic Users (Dial-Out Procedures). The user's connection will be automatically terminated if any call lasts past the time credited to the user under the Dial-Out Procedures.

36.1.6 After a specific period of idle time, (*See* the Dial-Out Procedures), the user's current session will be automatically terminated. Idle time is defined as no keyboard or mouse use.

36.1.7 Remote access to Peace Corps information resources may be revoked for cause without prior notification at any time.

36.1.8 Unless the system lacks the technical capacity to do so, the remote user's access will be restricted to network resources and services approved via the Peace Corps Laptop Checkout Form.

36.1.9 Notwithstanding *MS 643, Limited Personal Use of Government Office Equipment*, use of remote access for personal use or gain is prohibited.

36.2 Access From Overseas Locations

36.2.1 The policies and procedures governing access to the domestic data center resources by domestic users traveling overseas are set out in the agency's Laptop Dial-Out Procedures For Domestic Users.

36.2.2 The policies and procedures governing access to the domestic data center resources with laptops issued by overseas posts to sub-regional users (Rovers) who have obtained prior approval for a Headquarters Exchange account are set out in the agency's Overseas Information Technology (IT) Manual.

36.3 Technical Support

36.3.1 Users shall be provided with appropriate agency equipment and technical support for remote access work they have been assigned by their supervisors.

36.3.2 Technical support is not available to employees in connection with their use of personally-owned computers, communications systems and equipment, or software systems, under any circumstances.

Subsection F: Computer Security Incident Response Capability (CIRC)

39.0	Purpose and Applicability	33
40.0	Definitions	33
40.1	“Computer Security Incident”	33
40.2	“Threat”	33
40.3	“Vulnerability”	33
41.0	Incident Categories	34
42.0	Incident Response Priorities	34
43.0	Order of Incident Responses	35
44.0	Roles and Responsibilities	35
45.0	Security Incident Response Procedures	36

39.0 Purpose and Applicability

The purpose of the Computer Security Incident Response Capability (CIRC) program is to set out policies and procedures for reporting and responding to computer security incidents on the agency’s computer network. The policy applies to all users of the agency’s computer systems.

40.0 Definitions

40.1 “Computer Security Incident” means an unexpected, unplanned event that has or could have a negative impact on information technology resources in the agency’s computer systems, requires immediate action to prevent further negative impact, and violates security policies or circumvents security mechanisms. *Also see* Subsection H for the reporting requirements for malicious code or computer virus incidents.

40.2 “Threat” means any activity, intentional or unintentional, with the potential for causing harm to an automated information system or activity.

40.3 “Vulnerability” means a flaw or weakness in a computer system, such as in the security procedures, hardware, design, or internal controls, that may allow harm to the system.

41.0 Incident Categories

A computer security incident includes any denial of service caused by, but is not limited to, the following incident categories:

- (a) System Compromise (System privileges are acquired by an unauthorized user);
- (b) Information Compromise (Unauthorized access to password files, protected or restricted data or system resources, and/or software or code);
- (c) Misuse (An authorized user violates federal laws or regulations and/or agency policies regarding the proper use of computer resources, installs unauthorized or unlicensed software, causes physical destruction, or accesses resources and/or uses privileges that have not been assigned to the user);
- (d) Denial of Service (Resources are unavailable for use by the authorized user);
- (e) Hostile Probes (The act of using one or more systems to scan targeted systems or networks with the intent to conduct or to gather information for unauthorized or illegal activities);
- (f) Intrusion (Access by unauthorized individuals to agency systems that bypass authentication mechanisms or exploit system vulnerabilities); and
- (g) Theft (The unauthorized removal of information, computer equipment or other computer system property).

42.0 Incident Response Priorities

A user's response to a security incident shall be governed by the following priorities:

- (a) Priority one: protect human life and safety;
- (b) Priority two: protect classified and extremely sensitive data; prevent exploitation of classified or sensitive systems, networks or sites;
- (c) Priority three: protect computer property and data, including Privacy Act, scientific, managerial, and other data;
- (d) Priority four: prevent damage to the systems (e.g., loss or alteration of system files, damage to disk drives); and
- (e) Priority five: minimize disruption of computer resources (including processes). It is better in many cases to shut a system down or disconnect the system from the network than to risk additional damage to other data or systems.

43.0 Order of Incident Responses

Under the CIRC program, the preferred order of responses to a security incident is as follows:

- (a) Isolate the incident;
- (b) Determine the who, what, where, when, how, and why of the incident;
- (c) Assure the integrity of critical systems;
- (d) Maintain and restore data;
- (e) Maintain and restore service;
- (f) Avoid recurrence; and
- (g) Identify the source of the incident and report the source to the proper authorities.

44.0 Roles and Responsibilities

44.1 The IT Security Program Manager is responsible for:

- (a) Implementing and maintaining the CIRC program;
- (b) Serving as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins and other security related material;
- (c) Ensuring additional CIRC program resources for all security incidents, as needed;
- (d) Disseminating to all IT system managers prompt advisories of system threats, operating system vulnerabilities, and tracking all reported security incidents, trends, and impacts;
- (e) Monitoring the resolution of all incidents;
- (f) Assisting system administrators with security incident identification, handling and resolution;
- (g) Serving on the agency's Computer Emergency Response Team ("CERT" or "Response Team");
- (h) Serving as the agency's emergency contact person for IT incidents; and

- (i) Ensuring that general and privileged users are aware of their duties and responsibilities as outlined in this policy.

44.2 System Administrators are responsible for the following:

- (a) Identifying individuals who are responsible for reporting incidents to the IT Security Program Manager;
- (b) Providing timely reports to the IT Security Program Manager on a security incident in the following order: (1) a verbal report as soon as possible after detection of a security incident; (2) a written preliminary report containing as much information as possible, within two working days of the security incident; (3) a status report every 10 days when a security incident is expected to take more than 30 days to resolve; and (4) a written final report within 5 working days of the resolution of a security incident;
- (c) Developing, implementing and maintaining internal incident response procedures and coordinating those procedures with the IT Security Program Manager;
- (d) Identifying individuals to serve on the CERT; and
- (e) Reviewing, at least on a quarterly basis, the agency's security incident policies and procedures.

44.3 All users are responsible for the following:

- (a) Reporting any suspected security incidents, threats, or vulnerabilities to the agency's Help Desk;
- (b) Reporting any suspected security incidents, threats, or vulnerabilities to their immediate supervisor; and
- (c) Reviewing the IT security policies on a regular basis, and staying up-to-date on the procedures for reporting security incidents.

45.0 Security Incident Response Procedures

45.1 Procedures for Initial Response

The initial response to a domestic and overseas security incident shall include:

- (a) Investigating the incident to determine the cause of the security incident;
- (b) Determining a way to prevent additional harm to the agency's computer systems;

- (c) Assessing the impact and damage of the security incident;
- (d) Implementing solutions for recovering from the incident and preventing additional harm;
- (e) Following all applicable security incident response procedures.

45.2 Specific procedures to be used for domestic security incidents are set out in Attachment B to this manual section.

Subsection G: Electronic Mail Policy

48.0	Purpose	38
49.0	Policies	38
49.1	Standard Use of E-mail	38
49.2	E-mail and Privacy	38
49.3	E-mail Records Management	39
49.4	General Use Requirements	39
49.5	Rules of Behavior	40
49.5.1	Prohibitions	40
49.5.2	Safety Requirements	41

48.0 Purpose

The purpose of this policy is to establish standards and guidelines for the use of the agency's electronic mail (E-mail) system to help employees use the system properly, reduce the risk of intentional or inadvertent misuse, and ensure that official records transferred via E-mail are properly handled.

49.0 Policies

49.1 Standard Use of E-mail

Agency employees shall use the Peace Corps E-mail system for official and authorized purposes only, except as permitted under MS 643 *Limited Personal Use of Government Office Equipment*. Employees are expected to use common sense, good judgment, and propriety in their use of the system.

49.2 E-mail and Privacy

Agency employees should have no expectation of privacy when using the Peace Corps E-mail system. Although certain employees with special access privileges are expressly prohibited from reading others' E-mail, they may do so if authorized by appropriate senior management officials or if technical or administrative problems create a situation in which it is necessary for such employees to read message text. In addition, E-mail messages are government property and agency officials may have access to those messages whenever there is a legitimate governmental purpose for doing so.

49.3 E-mail Records Management

The National Archives and Record Administration (NARA) has issued standards for the management of federal records created or received on E-mail. Specifically, the National Archives and Records Administration Management Guide Series (1995) states that electronic record keeping systems must be designed to ensure the security and integrity of records, preservation of records for the time they are needed, and migration of data to other agency systems or subsequent systems. If messages that are made or received through E-mail do not show the complete names of senders, addressees, and the date of transmission, users should take reasonable steps to preserve the mail envelope information sheet, distribution list, or other screen that contains any of that information that is not on the message itself. In addition, E-mail receipts should be maintained.

Agency offices shall establish the standard requirements for retention of electronic messages based on their individual policies. Offices are responsible for ensuring that employees are familiar with the legal requirements for creation, maintenance, and disposition of records on E-mail systems. Records management officers and records custodians should emphasize to users that E-mail messages are generally considered to be public records subject to retention.

49.4 General Use Requirements

49.4.1 All users of the Peace Corps electronic resources are expected to utilize such resources in a responsible, ethical and legal manner consistent with applicable federal laws.

49.4.2 Each user shall be provided an E-mail account for conducting official agency business. This account shall be the only account the employee or contractor may use to conduct official agency business.

49.4.3 All E-mail messages created and stored on agency computers or networks are the property of the agency and may be accessed by the agency.

49.4.4 The content and maintenance of an E-mail mailbox is the responsibility of the person to whom the E-mail account is assigned.

49.4.5 All employees shall use E-mail as they would any other type of official agency communications tool. This means that when E-mail is created and sent, the sender should ensure that the communications comply with the agency's E-mail guidelines and manual sections.

49.4.6 The agency shall provide access to E-mail to non-Peace Corps personnel, such as contractors, temporary employees, or other government agencies.

49.4.7 The agency reserves the right to review and monitor all employee E-mail communications. Electronic mail messages may be retrieved by the agency even though they have been deleted by the sender and the reader. Inappropriate messages may be grounds for disciplinary action.

49.4.8 Only authorized E-mail software may be used for conducting agency business.

49.4.9 All E-mail messages must contain the name and E-mail address of the sender and a subject heading that reflects the content of the message without divulging highly-sensitive information.

49.4.10 Shared/Office E-mail boxes may only be used to receive E-mail. Senders must be identified as an individual, whenever possible.

49.4.11 Broadcast messages (messages to multiple offices) may only be sent by pre-approved designees.

49.5 Rules of Behavior

49.5.1 Prohibitions

The following uses of E-mail systems are prohibited:

- (a) Use of the Agency's E-mail system that could cause congestion, delay, or disruption of service to any government system (for example, video, sound or other large file attachments can degrade the performance of the entire network);
- (b) Using non-agency issued E-mail accounts for official agency business;
- (c) Using the agency E-mail system for business purposes other than agency business, including using the system for private commercial activities;
- (d) Using or sending anonymous E-mail for any purpose (E-mail communications must accurately identify the sender);
- (e) Using the E-mail system to intentionally misrepresent oneself or the agency;
- (f) Using the E-mail system to participate in any non-work related "chat room;"
- (g) Using the E-mail system to send or forward any information that can be interpreted as sexually implicit or explicit, or derogatory toward any racial, religious, or ethnic group. Harassing or obscene material shall also not be

sent, printed, requested, displayed, or stored. Also, the system shall not be used for any mass mailing, such as, SPAM, chain letters, and/or JUNK MAIL.

(h) Using E-mail to improperly disclose sensitive information, or to communicate unethical information or information that could be perceived to be a conflict of interest;

(i) Using E-mail for unlawful activities, including any communication that violates security policies, federal laws, or regulations;

(j) Using E-mail to send classified or agency proprietary information;

(k) Using E-mail for malicious activities, such as, knowingly activating and/or propagating computer viruses, or other malicious codes, or purposefully disguising the true content of an E-mail message with a subject or title that is not reflective of the message content; and

(l) Joining electronic discussion groups, e.g., listservs or Usenet newsgroups, that are not related to agency business.

(m) Permitting others (supervisors, secretaries, assistants, or any other subordinate) to use your E-mail accounts as their own.

49.5.2 Safety Requirements

Every user of the agency's E-mail system is expected to help protect the E-mail services by:

(a) Allowing virus scanning software to check incoming E-mail attachments for viruses using the desktop Anti-virus software (Users shall not disable or re-configure the desktop Anti-virus software); and

(b) Checking his electronic mail often and properly disposing of messages that are no longer needed.

Subsection H: Malicious Code (Computer Virus): Prevention and Corrective Action

54.0	Purpose	42
55.0	Definitions	42
	55.1 “Malicious Code”	42
	55.2 “Media”	42
	55.3 “Write Protect”	42
56.0	Applicability	42
57.0	Policies	43
58.0	Roles and Responsibilities	43
	58.1 Users	43
	58.2 System Administrator	43
	58.3 IT Security Program Manager	45

54.0 Purpose

The purpose of the malicious code policy is to set out the corrective actions to be taken should any type of malicious code be detected on the Peace Corps network or computer systems.

55.0 Definitions

55.1 “Malicious code” is any computer program code or software which intentionally hides its full intent and purpose with the effect of harming or degrading computer and/or network resources or performance. Although “malicious code” is an umbrella term which includes viruses, worms, Trojans, and macros, it is used interchangeably throughout this manual section with “computer virus” and “virus.”

55.2 “Media” means the magnetic materials used to store data.

55.3 “Write-protect” means to mark a computer file or disc so that its contents cannot be modified or deleted. Write-protected files and media can only be read; a user cannot edit, append data to, or delete such files.

56.0 Applicability

The POLICY in this subsection applies to all Peace Corps network users and system administrators, file servers, Web servers and e-mail servers, including those overseas.

The PROCEDURES, on the other hand, apply only to agency users located in the United States. Procedures for non-domestic users are in the Computer Support Manual for Macintosh users and the Technical Support Specialist Manual for PC users (users of personal computers).

57.0 Policies

57.1 All network users shall take reasonable precautions, according to their roles and responsibilities, to avoid the possibility of a malicious code being introduced into the agency's equipment and networks.

57.2 Only authorized software shall be installed and used on Peace Corps' equipment and networks.

58.0 Roles and Responsibilities

58.1 Users

Users shall:

- (a) NOT change the configuration of or attempt to modify or disable any of the security programs set up on their personal computers, including virus protection software and the password-protection function on screen savers;
- (b) Ensure that a computer that is infected or suspected of being infected is disconnected from networks to reduce the risk of spreading a virus; and
- (c) Notify the agency Help Desk immediately upon the detection or suspicion of any malicious code stored or transmitted on the agency's network and related computer equipment and media, and cooperate fully with efforts by technical support staff to address the problem.

58.2 System Administrator

System Administrators shall:

- (a) Make regular backups of data on their systems as a precaution against data loss;
- (b) Ensure that an anti-virus report log from the servers is available to the IT security staff when requested;
- (c) Configure the anti-virus software to notify a user that a virus was detected or cleaned from data or e-mail belonging to the user;

- (d) Configure application or system logs to record and retain information regarding infections that are detected;
- (e) Keep anti-virus signature file updates and application programs up-to-date with vendor releases for servers and workstations;
- (f) Use all available tools and procedures compatible with a system's technical capacity to guard against the placement or storage of malicious codes on the agency's servers;
- (g) For file servers:
 - (1) Implement a regular schedule for virus signature file updates from the vendor to be loaded onto the servers and desktops;
 - (2) Configure distribution file server systems to do a virus signature "pushdown" when a new virus is identified by authorized personnel as requiring immediate action that cannot wait for the monthly update; and
 - (3) To initiate a regular schedule (daily or nightly) for scanning viruses, which shall require scanning at least once a day;
- (h) For desktops:
 - (1) Configure real-time automatic scan of removable media, e.g., floppy disks and CDs, upon use;
 - (2) Implement a regular, weekly schedule for virus scans of all hard drives on PCs and laptops; and
 - (3) If feasible, lock desktop anti-virus client settings so users cannot turn off the client protection;
- (i) For e-mail:
 - (1) Configure real-time automatic scan of e-mail attachments when received or opened by the user; and
 - (2) Configure e-mail servers to automatically strip off and quarantine e-mail attachments considered or known to be potentially harmful or threatening. E-mail administrators shall determine whether the attachment is appropriate to be forwarded to the user. If not, the attachment shall be deleted and the user shall be notified.

58.3 IT Security Program Manager

The IT Security Program Manager shall:

- (a) Report widespread infection levels that result in a major impact to the computer system or network availability to proper federal authorities;
- (b) Help coordinate resources in the event of a widespread virus “outbreak;” and
- (c) Advise network and system administrators of new virus threats.

Subsection I: Web-Based Services Policy: Internet/Intranet/Extranet

63.0	Purpose	46
64.0	Applicability	47
65.0	Definitions	47
65.1	“Broken link” and “dead link”	47
65.2	“Common Gateway Interface”	47
65.3	“Domain name”	47
65.4	“Editorial support”	47
65.5	“Extranet”	47
65.6	“Home page”	47
65.7	“Internet”	47
65.8	“Intranet”	48
65.9	“Internet service”	48
65.10	“Mobile Code”	48
65.11	“Publishing Guide”	48
65.12	“Web server”	48
66.0	Policies	49
67.0	Requirements	49
67.1	General Requirements.	49
67.2	Browser and Mobile Code Requirements	50
67.3	Web server requirements	50
68.0	Remote Administration/Development Security	51
69.0	Responsibilities	51
69.1	Chief Information Officer	51
69.2	Office Directors and Web Managers	52
69.3	Office Heads	52
69.4	Network Administrators	52
69.5	System designers/developers	53
69.6	IT Security Program Manager	53
69.7	Users	54

63.0 Purpose

This Web-based services policy sets out the guidelines and procedures for managing, maintaining, and establishing Web-based services, including the agency’s Internet,

Intranet, and Extranet Service Sites. The policy delineates who is responsible for planning, design, maintenance, support, and other services related to the agency's Web-based systems, and defines the appropriate uses of the agency's Internet services. Appropriate uses include, but are not limited to, the use of mobile code (i.e., Java and ActiveX), File Transfer Protocol (FTP), Hypertext Markup Language (HTML), Simple Mail Transfer Protocol (SMTP), Web pages, active server pages (ASP), e-mail forums, and list servers.

64.0 Applicability

This policy is applicable to:

- (a) Individuals who design and/or maintain the agency's web-based pages and sites, including contractors;
- (b) All agency domains and servers that utilize Peace Corps' remote resources, wherever they are located; and
- (c) Web-based services that are out-sourced to an external host.

65.0 Definitions

65.1 "Broken Link" or "dead link" means a hyperlink to a non-existent or non-operational page or server.

65.2 "Common Gateway Interface" (CGI) is the method that Web servers use to allow interaction between server programs and Web users. CGI enables the creation of dynamic and interactive Web pages and can easily become the most vulnerable part of the Web server.

65.3 "Domain name" means a meaningful and easy-to-remember name ("handle") for an Internet address.

65.4 "Editorial support" means editorial services provided by the Peace Corps program office with Web site responsibility.

65.5 "Extranet" is a computer network which provides various levels of access to outside users. A user's scope of access is determined by the user's identity.

65.6 "Home page" means the primary page or starting point reached through the Uniform Resource Locator (URL). A home page is described as a single document but can contain multiple screens. An "organizational home page" contains information about a definable organization such as a division of the agency.

65.7 "Internet" means a large computer network of information resources which interconnects innumerable smaller groups of linked computer networks worldwide.

This network of information resources relies on three mechanisms to make the information resources readily available to the public. The three mechanisms are:

- (a) A uniform naming convention for services located on the Web, e.g., URLs;
- (b) Protocols to access named resources on-line, e.g.; HTTP (HyperText Transfer Protocol); or FTP (File Transfer Protocol);
- (c) Hypertext to facilitate navigation among available resources, e.g., HTML (Hypertext Markup Language).

65.8 “Intranet” means a network of information resources fully comparable to and interoperable with the Internet, but which is generally accessible only to members of the same company or organization and is not readily available to the public.

65.9 “Internet service” (sometimes referred to as “public access system”) means a network-based information/service resource operated by an entity for the use of internal and/or external users. This includes, but is not limited to, FTP, HTML, SMTP, Web pages, active server pages, e-mail forums, chat rooms, and list servers.

65.10 “Mobile Code” means software obtained from a remote system, transferred across a network and then downloaded and executed on a local system without explicit installation or execution by the recipient, such as, Java and ActiveX.

65.11 “Publishing Guide” means a document written by an agency office supporting Web-based services that describes the controls, approval process and polices for publishing content on a Web server under its purview.

65.12 “Web server” means a computer program that provides HTML files requested by a browser. The web server provides access to one or more collections of documents using Web formats and protocols. Each Web server may have multiple main entry points and one home page, although numerous files or pages are usually directly addressable. The Peace Corps may use three types of Internet (Web) servers:

- (a) Development servers, which are used as platforms to develop and review Web pages before releasing them to the public;
- (b) Staging servers, which are used by technical support to house files for review and scanning before moving them to the production server; and
- (c) Production servers, which contain the current files accessed by Peace Corps Websites.

66.0 Policies

66.1 The Peace Corps promotes the secure and effective use of Web-based services to empower employees in their work and improve access to and delivery of information to staff, Volunteers, contractors, and the general public. Information available on the agency's Web-based systems includes information on the policies, programs, activities, and objectives of the agency, and information from public and private organizations.

66.2 Use of the agency's Web-based services shall reflect and support the Peace Corps' mission, goals and objectives, and be consistent with prudent operational, security, and privacy considerations.

66.3 The agency's Web-based service sites shall be designed to support the widest possible range of potential users and computing platforms and shall be consistent with Section 508 of the Rehabilitation Act of 1973, as amended.

67.0 Requirements

67.1 General Requirements

67.1.1 All software used to access the Web-based services shall be approved in accordance with the Peace Corps' agreement with Seat Management, Peace Corps' Concept of Operations Plan (CONOP), and shall incorporate all vendor-provided security patches.

67.1.2 Any files downloaded over the Internet shall be scanned for viruses, using approved virus detection software.

67.1.3 Peace Corps reserves the right to monitor Web usage by its employees and contractors. Any user suspected of misuse may have all transactions and material retained for further action. Internet addresses of offensive sites shall be forwarded to the IT Security Program Manager.

67.1.4 A notice of the agency's privacy policy shall be posted on all agency Web sites with public access.

67.1.5 Only approved versions of browser software may be used or downloaded. Approved sources for licensed Web software shall be made available to users.

67.1.6 Sensitive information shall not be stored unencrypted on any Web server available to the public but it may be published (so that it cannot be altered) on public web servers if the appropriate levels of risk mitigation and data protection have been implemented in accordance with Peace Corps and federal policies.

67.1.7 Before information may be posted on the Web-based system it must be reviewed and approved for release under the provisions of the Publishing Guide of the appropriate agency office or business unit.

67.1.8 Permission to use copyrighted information must be obtained before it may be posted on the agency's Web site.

67.1.9 The Peace Corps shall establish a Web Council that shall be the approving and authorizing body.

67.2 Browser and Mobile Code Requirements

67.2.1 Only approved versions of browser software may be used or downloaded on the agency's Web-based systems.

67.2.2 Web browsers shall be configured with the settings approved for mobile code use in the agency.

67.2.3 Mobile code use and browser settings are contained in the Technical Configuration Guide, which is maintained in the Office of Information Resource Management.

67.3 Web server requirements

67.3.1 Users are not permitted to install or run Web servers on Peace Corps systems.

67.3.2 Web servers and data that are accessible to the general public must be located on a screened subnet; such as the DMZ (The DMZ is a part of a network that is protected by a firewall but may be accessed by external Internet clients. It generally contains servers such as mail servers, remote access machines an/or web servers.).

67.3.3 All network applications other than HTTP shall be disabled if not specifically needed for services, e.g., SMTP, FTP.

67.3.4 Information servers shall be located on a screened subnet, such as the DMZ, to isolate them from other systems on the site.

67.3.5 When using a Web remote administrative tool, access by remote users is restricted to authorized systems (via IP address, rather than hostname).
DEFAULT PASSWORDS MUST NOT BE USED.

67.3.6 When processing or transmitting sensitive information over the public internet, users shall ensure that the Secure Sockets layer (SSL) or other such NIST approved mechanism is used to encrypt the message as it is sent from the

user's browser to the Web server. Messages must be encrypted when sent from a browser to the Web server.

67.3.7 All publicly accessible Peace Corps Web sites must be thoroughly tested to ensure all links work as designed and are not "under construction" when the site is opened to the public. Under construction areas are not permitted to appear on publicly accessible Web sites.

67.3.8 The Web server software, and the software of the underlying operating system, shall contain all manufacturer-recommended patches for the version in use.

67.3.9 On UNIX systems, Web servers shall not be run as "root."

67.3.10 The implementation and use of CGI scripts shall be discouraged. When their use is necessary, CGI scripts shall be very carefully monitored and controlled.

67.3.11 Web forms shall not accept unchecked input. Any programs that run externally with arguments shall be configured to screen for and reject metacharacters.

68.0 Remote Administration/Development Security

Installing software on agency Web servers to permit remote administration puts the systems at risk. The following requirements are intended to mitigate the risks:

- (a) Remote administration traffic shall be encrypted so that attackers monitoring network traffic cannot obtain passwords or inject malicious commands into conversations;
- (b) Packet filtering shall be used to allow remote administration only from a designated set of hosts; and
- (c) Remotely administrated Web hosts shall be maintained at a higher degree of security than normal hosts, as determined by the IT Security Program Manager.

69.0 Responsibilities

69.1 Chief Information Officer

The Chief Information Officer shall:

- (a) Be responsible for the effective use of the Peace Corps Web-based systems and other IT resources, directives, and policies governing the use and implementation of the agency's Internet and other IT resources;

- (b) Provide guidances with respect to establishing, operating, and maintaining Web sites;
- (c) Provide and manage Web services that support the IT infrastructure; and
- (d) Review and approve additions and changes to Web policy and procedures.

69.2 Office Directors and Web Managers

Office directors and Web managers shall:

- (a) Oversee the implementation of the agency's Web policy within their respective office; and
- (b) Ensure that sensitive information and information resources are protected from inappropriate use, access, tampering, destruction, and the unauthorized release of sensitive information.

69.3 Office Heads

Each office head responsible for an official Web-based site shall:

- (a) Own and be responsible for the content of the site documents, including studies, forms, pictures, and graphics;
- (b) Ensure the timeliness and accuracy of information posted on the Internet server site for which they are responsible; and
- (c) Ensure that Web-based services conform to §508 of the Rehabilitation Act of 1973, as amended.

69.4 Network Administrators

Network administrators shall:

- (a) Be responsible for the day-to-day upkeep of agency IT systems, including the installation, management, content development, configuration, and maintenance of the computers, sites and networks;
- (b) Keep current with, and evaluate and expeditiously apply, security patches, as appropriate;
- (c) Keep the operating system at a level supported by the vendor;

- (d) Restrict access to information consistent with the agency's policies and procedures;
- (e) Provide and store backup of data;
- (f) Upgrade and provide capacity planning for server and application software and hardware;
- (g) Remove sample applications and directories;
- (h) Configure a browser policy within each zone (zones are based on IP address spacing and denote internal versus external address spacing); and
- (i) Remove unnecessary services from the Web server.

69.5 System Designer/Developers

System designers/developers shall:

- (a) Be responsible for IT activities, such as software installation, content development, and application configuration;
- (b) Restrict access to information consistent with the agency's policies and procedures;
- (c) Provide test procedures for installations of new software or configurations;
- (d) Upgrade and provide capacity planning to the agency's server and application software and hardware;
- (e) Remove unnecessary services; and
- (f) Ensure that Web forms do not accept unchecked input. Any programs that run externally with arguments shall be configured to screen for and reject meta-characters.

69.6 IT Security Program Manager

The IT Security Program Manager shall:

- (a) Provide guidance on policy, reviewing procedures, and reporting incidents;
- (b) Ensure that the Web-based server environment is secured;

(c) Recommend policy and procedural guidance that protects the availability, confidentiality and integrity of sensitive information with respect to establishing, operating, and maintaining Web-based sites; and

(d) Provide recommendations on Web-based services and risk management issues.

69.7 Users

Users shall:

(a) NOT download, install, or run Web server software;

(b) Report all security violations, incidents, and vulnerabilities to the Peace Corps IT Security Program Manager, as detailed in the Peace Corps Computer Incident Response Capabilities procedures in Subsection F, and notify a supervisor.

Subsection J: IT Security Awareness, Training, and Education

72.0	Purpose	55
73.0	Applicability	55
74.0	Definitions	55
74.1	“Awareness programs”	55
74.2	“Training programs”	55
74.3	“Education programs”	56
75.0	Policy	56
76.0	Minimum Requirements	56
76.1	Awareness requirements	56
76.2	Training requirements	56
76.3	Education requirements	57

72.0 Purpose

The comprehensive IT Security Awareness, Training, and Education program set out in this policy is intended to:

- (a) Help reduce inappropriate behavior, errors and omissions by users when they operate the agency’s IT systems and handle sensitive data;
- (b) Engender users with a sense of personal value and responsibility for IT security; and
- (c) Provide periodic reminders to users of their responsibility for IT security.

73.0 Applicability. This policy applies to all users of Peace Corps IT systems, wherever they are located.

74.0 Definitions

74.1 “Awareness programs” are programs that set the stage for training by changing organizational attitudes toward the importance of security and the adverse consequences of its failure.

74.2 “Training programs” are programs intended to teach IT professionals the skills that will enable them to perform their jobs more effectively.

74.3 “Education programs” are programs with in-depth specialized training that is targeted at security professionals and those whose jobs require expertise in automated information security.

75.0 Policy

It is the policy of the Peace Corps to develop and implement a comprehensive IT security awareness, training, and education program designed to:

- (a) Raise employee awareness of security threats and vulnerabilities and the need to protect systems, data, and networks;
- (b) Train every employee on security policies, procedures, and practices that relate to the employee’s roles and responsibilities; and
- (c) Educate IT security professionals (full and part-time) to perform complex multi-disciplinary IT security activities and provide the skills needed to keep pace with security threats and technological changes.

76.0 Minimum Requirements

76.1 Awareness Requirements

The IT security awareness program shall:

- (a) Be designed to raise staff awareness of, and sensitivity to, security threats and vulnerabilities, as well as the need to protect systems, data, and networks;
- (b) Require that every system user attend refresher awareness programs on an annual basis. Refresher program activities may be in the form of seminars, briefings, videotapes, or computer-based products delivered via CD-ROM, Intranet, Internet, or local area network (LAN). The simple distribution of newsletters or security awareness items, such as, key chains, pens, buttons, or notepads, can be used to supplement the refresher courses; and
- (c) Require all system users to receive, and acknowledge receipt of, the Peace Corps IT Users’ Security Brochure, maintained in IRM, which outlines responsibilities and establishes computer system rules, before they are granted access to the agency’s IT applications and systems.

76.2 Training Requirements

The training program shall:

- (a) Be designed to effectively train IT professionals in relevant security procedures and necessary security skills and competencies, such as those in management, systems design and development, acquisition, and auditing;
- (b) Train individuals according to each person's roles, responsibilities, needs, and job functions;
- (c) Consist of formal trainings that are classroom or computer-based, and/or specific trainings in the form of "expert" workshops or briefings (attendance at vendor marketing briefings cannot be used to meet agency training requirements);
- (d) Require individuals in positions of moderate or high risk, as defined by the IT related personnel investigation policy in Subsection L, to attend IT security program office update meetings throughout the year (Overseas and regional staffs shall be updated by E-mail and at headquarters when attending trainings and conferences.);
- (e) Require all supervisors and office directors of IT professionals to participate in a minimum of two formal security trainings per year;
- (f) Provide IT security training updates by E-mail for overseas and regional IT professionals and through conferences and trainings for users at Headquarters; and
- (g) Require 30 hours of formal IT security training per year for part time (74% or less of duties) security professionals who are Computer Security Coordinators. (Qualifying training may include, but need not be limited to, workshops, seminars, security conferences, video training, computer-based training, and/or product-specific training). However, attendance at vendor marketing briefings cannot be used to meet this requirement;
- (h) Require all IT professionals to participate in quarterly training events, especially when:
 - (1) There is a significant change in the IT security environment or procedures; or
 - (2) IT professionals enter a new position which deals with sensitive information.

76.3 Education Requirements

The IT security educational program shall:

(a) Require IT security professionals, consisting of the IT Security Program Manager and his or her staff, to routinely update their security skills and stay abreast of changes in technology that affect security. This means they should:

(1) Understand the IT security policies and practices and the rationales behind them;

(2) Maintain an in-depth knowledge of the ever-evolving threats to, vulnerabilities of, and safeguards for IT systems; and

(3) Maintain a thorough understanding of categories of concerns and how to apply appropriate safeguards.

(b) Require all full-time (75% or more of duties) IT security professionals to receive 60 hours of formal security education each year. Qualifying education may include workshops, seminars, security conferences, computer-based training, and/or product-specific training. However, attendance at vendor marketing briefings cannot be used to meet this requirement.

Subsection K: Certification and Accreditation Policy

80.0	Purpose	59
81.0	Applicability	59
82.0	Definitions	60
	82.1 “Accreditation”	60
	82.2 “Certification”	60
	82.3 “Designated Approving Authority (DAA)”	60
	82.4 “Risk”	60
	82.5 “Risk management”	60
	82.6 “System operational status”	60
83.0	Policies	60
84.0	Responsibilities	61
	84.1 IT Security Program Manager	61
	84.2 Designated Accrediting Authority	62
	84.3 Offices with Sensitive Systems	62
85.0	Certification Process	62
	85.1 Types of Certification	62
	85.2 Certification Verification Program	63
	85.3 Interim Authority to Operate	63
86.0	Waivers	64
87.0	Post Accreditation Activities	65

80.0 Purpose

The purpose of this policy is to set out the agency’s computer system security certification and accreditation (C & A) policies. Detailed C & A Procedures are set out in Attachment E.

81.0 Applicability

This policy applies to:

- (a) The agency’s IT and office officials who are responsible for establishing and implementing the agency’s C & A policies and procedures; and

(b) All agency IT systems or networks that process, store, communicate or provide access to sensitive information.

82.0 Definitions

82.1 “Accreditation” is an official approval, based on a certification, to operate an IT system or network.

82.2 “Certification” is an official determination that the security vulnerabilities of an agency IT system or network have been adequately identified and appropriately addressed, and that the system is in compliance with federal information security guidelines, laws and regulations, including OMB Circulars, and Peace Corps policies. Certification is a process that produces a judgment, a statement of opinion. It is not a guarantee that a system is secure in its operation.

82.3 “Designated Approving Authority (DAA)” is the senior management official who has the authority to accredit an IT automated information system (major application or general support system) and accept the risk associated with the system. The DAA also has the authority to decide the acceptability of the security safeguards in place for an IT system.

82.4 “Risk” means the possibility of harm to or loss of the agency’s computer system.

82.5 “Risk management” is the ongoing process of assessing the risk to automated information resources and data by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

82.6 “System operational status” is a statement of the operational status of an agency computer system. Systems shall be “operational,” “under development,” or “undergoing a major modification.” **“Operational”** means a system is currently functioning properly and available for regular use. **“Under Development”** means a system is currently under design, still being tested for errors, or otherwise not yet ready for regular use. **“Undergoing a major modification”** means a system is currently undergoing a major conversion or transition.

83.0 Policies

83.1 An agency computer or network system that contains sensitive information shall not be put into operation unless it has conditional or unconditional certification AND an accreditation, or has been granted an Interim Authority to Operate (IAO) or a waiver under Section 86.0 of this manual section.

83.2 The agency shall establish a security verification program designed to ensure that, early in the life cycle of each computer system (that is, as the system is conceived, designed, and implemented), its security protections and procedures are in compliance with federal law and agency computer security policies and procedures.

83.3 All agency computer or network security systems that contain sensitive information shall be certified and accredited as expeditiously as possible, consistent with applicable regulatory guidelines. The current federal guidance for certification and accreditation is contained in the Federal Information Processing Standard (FIPS) Publication (PUB) 102, *Guideline for Computer Security Certification and Accreditation*.

83.4 Responsible IT and management officials may establish certification and accreditation standards more stringent than those detailed in FIPS PUB 102, as long as they are consistent with those set out in this policy.

83.5 An agency computer or network security system must be certified prior to being accredited. Certifications shall be documented and based on reliable and independent technical sources. A certification package shall include:

- (a) A security plan that incorporates federal certification and accreditation requirements;
- (b) Documentation of an independent review ensuring that the certification methodology used to determine that the level of security is complete and effective, and that the certification could withstand both internal and external reviews by the Inspector General, Audit Staff, OMB, the GAO, or Congress.

83.6 Agency computer systems or networks shall be re-certified and re-accredited at least once every three years.

84.0 Responsibilities

84.1 IT Security Program Manager

The IT Security Program Manager is responsible for:

- (a) Monitoring the compliance of the security systems with applicable federal statutes, policies, and regulations;
- (b) Assisting offices with IT security programs to implement federal and Peace Corps certification and accreditation requirements; and
- (c) Overseeing the Certification Verification Program.

84.2 Designated Accrediting Authority

Agency office directors shall be the accrediting authorities for sensitive computer systems or networks within their area of responsibility. The Designated Approving Authority is authorized to:

- (a) Approve the security safeguards in place for a particular IT system or network;
- (b) Issue statements that record decisions regarding the adequacy of system security safeguards; and
- (c) Redirect resources to secure a system, when necessary.

84.3 Offices with Sensitive Systems

Peace Corps offices with oversight of sensitive computer systems are responsible for:

- (a) Preparing the certification documentation required for each sensitive system; and
- (b) Performing system security certification testing as required by their own unique security needs.

85.0 Certification process

85.1 Types of Certification

A certification may be conditional or unconditional.

85.1.1 An unconditional certification is a statement that all of the security requirements have been reviewed and have been satisfied. An unconditional certification is valid for three years.

85.1.2 A conditional certification is a statement that, although not all of the certification conditions have been met, at least an approved system security plan, risk assessment, and security test and evaluation have been successfully completed and submitted to the IT Security Program Manager with an assurance that the IT system does not introduce any vulnerabilities to the agency.

A conditional certification may be provided for up to 18 months. Once all of the certification conditions have been met, an unconditional certification may be provided for three years.

85.2 Certification Verification Program

85.2.1 The IT Security Program Manger shall develop a Certification Verification Program to make available certification assistance and oversight to offices with sensitive computer systems. Under the program, an office may request assistance at any stage of the certification process and the IT Security Program Manager shall verify that an office's certification activities are consistent with the requirements of this policy.

85.2.2 Offices should begin the certification process early in the development of their sensitive systems because early certification efforts:

- (a) Improve the agency's coordination of security overall;
- (b) Ensure involvement of all participants in every phase of the development; and
- (c) Ensure integration of appropriate security measures when they will be the least costly to implement.

85.2.3 When an office completes the required certification activities for an IT system, it shall request the IT Security Program Manager to review and document the activities and verify that the office followed the required policies and procedures. The written request shall be made in the form of a memorandum and shall identify the IT system, the type of system (general support or major application), location, projected start-up date (if new or a significantly modified system) and the point of contact.

85.3 Interim Authority to Operate

85.3.1 When it is not feasible to certify and accredit an IT system before it goes into operation, an Interim Authority to Operate (IAO) may be obtained by the responsible office through the IT Security Program Manager Security Certification Verification Program.

85.3.2 IAOs are typically obtained for special situations, such as, a pilot program, a prototype system, or a system that is currently operational but requires completion of the system's security plan and scheduling of the security activities in order to accomplish the accreditation.

85.3.3 The following documentation is required to obtain an IAO:

- (a) A system security plan;

(b) A statement of the measures in place to prevent the compromise, loss, misuse, or unauthorized alteration of sensitive data; and

(c) A schedule to accomplish the certification activities.

85.3.4 An IOA must have an expiration date, and may be granted for no more than 180 days. An additional 180 days may be granted, if necessary and if the IT Security Program Manager reviews the documentation required by Section 85.3.3 to ensure compliance with the conditions which are set forth in the initial IAO.

85.3.5 An IOA must be re-examined if a major deficiency is identified through the certification activities rendering the office's information vulnerable to harm.

86.0 Waivers

86.1 A waiver from the requirements of this subsection may be requested when limitations in the agency's resources and technical capabilities prevent or delay satisfactory compliance with IT security requirements. For example, compliance may not be possible without unbudgeted procurement requests or unacceptable delay in achieving program requirements. An approved waiver indicates that the implementation of one or more security requirements may be postponed and that satisfactory substitutes for those requirements will be used for a specified period of time.

86.2 The agency's Chief Information Officer or designee shall be the approving authority for all waivers of this subsection. The Director of IRM may not use his or her authority under Section 5.1.2 to waive this rule.

86.3 A waiver request shall:

(a) Identify the security requirement for which the security waiver is being requested and the federal or Peace Corps reference which cites the requirement;

(b) State the effect of the requirement on proposed or current operations and describe the specific operational or technical difficulties which will result from compliance and the impact of the Program Office mission;

(c) Submit a written technical review on the information system waiver. The review should identify and security risks, vulnerabilities and anticipated threats to the system as a result of granting the waiver; and

(d) Identify actions to be taken and the estimated date the waiver will no longer be needed.

86.4 The Program Office receiving the waiver shall ensure that the necessary programmatic, funding and planning resources shall be available to implement the required controls.

87.0 Post Accreditation Activities

87.1 After an IT system has been certified and accredited, the IT Security Program Manager must be notified if there has been a:

- (a) Proposed change to the system prior to the expiration of the system's accreditation;
- (b) Proposed change in the sensitivity of the information processed by the system;
- (c) Proposed change in the security mode of the system's operation;
- (d) Proposed change in the system's physical environment; or
- (e) Breach of the system's security that could possibly invalidate the certification.

87.2 After receiving the notice described in Section 87.1, the IT Security Program Manager shall determine whether the system needs to be re-accredited. Substantive changes in the system require re-accreditation. Simple technical changes, such as an upgrade to the hardware or software configuration of the system that does not effect the security status of the system, does not need re-accreditation. Non-substantive changes may be authorized by a memorandum forwarded by the IT Security Program Manager to the Designated Approving Authority stating that the change has been reviewed by the ITSPM and that re-accreditation is not necessary. The memorandum shall be kept with the original certification/accreditation documentation.

Subsection L: IT Personnel Investigation Policy

90.0	Purpose	66
91.0	Applicability	66
92.0	Definitions	66
92.1	“Database Administrator (DBA)”	66
92.2	“Sensitive information” and “Sensitive but Unclassified (SBU) Information”	67
92.3	“Sensitive system”	67
92.4	“Public Trust position”	67
93.0	Policies	67
94.0	Procedures and Standards	67
94.1	Investigation Form Requirements	67
94.2	General Users in Low Risk IT Positions	68
94.3	Privileged Users in Moderate Risk IT Positions	68
94.4	Privileged Users in High Risk Positions	69
94.5	Special Requirements for Contractors	70
94.6	Special Requirements for Temporary Contract Positions	70

90.0 Purpose

The purpose of this policy is to provide standards and procedures for minimum security background investigations and checks for users who access sensitive information in the agency’s computer systems.

91.0 Applicability

This policy is applicable to all users who are employees and domestic contract personnel and who have access to agency IT systems that include sensitive information. It does not apply to contract personnel overseas.

92.0 Definitions

92.1 A “**Database Administrator (DBA)**” is a person who manages one or more agency databases. A DBA’s tasks include assigning security privileges to databases, creating and designing databases, and controlling the importing and exporting of data between databases and external sources.

92.2 “Sensitive information” or “Sensitive But Unclassified (SBU) Information” refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act. The term does not include classified information.

92.3 “Sensitive systems” are computer systems that process, store or transmit sensitive information.

92.4 A “Public Trust position” is a position that does not involve national security or require a security clearance but does involve sensitive information designated as either high or moderate risk under the Office of Personnel Management’s Position Sensitivity Designation Guidelines.

93.0 Policies

93.1 In order to have access to systems that process, store, or transmit sensitive data, users of such agency IT systems must complete a personnel security questionnaire, and undergo and favorably pass the appropriate personnel security investigation or be granted a waiver from doing so, as set out under this policy.

93.2 Each IT position, the duties of which include the management, operation, or maintenance of a sensitive system, will be designated as either high, moderate, or low risk, depending on the duties performed and the potential for adverse impact on the computer system.

93.3 Security investigations shall be conducted and/or managed by the agency’s personnel security staff, who are responsible for establishing and managing the overall security policies and procedures for the agency’s employees and certain contractors.

94.0 Procedures and Standards

94.1 Investigation Form Requirements

All users except contractors shall submit their completed personnel security questionnaire forms to the agency’s personnel security office within 2 weeks of beginning work at Peace Corps. Contractors shall submit their forms to the personnel security office before beginning work at Peace Corps.

The various forms include: SF-85 Questionnaire for Non-Sensitive Positions; SF-85P Questionnaire for Public Trust Positions; SF-85PS Supplemental Questionnaire for

Selected Positions; SF 86 Questionnaire for National Security; SF-86A Continuation Sheet for SF-86, SF-85, and SF-85P.

94.2 General Users in Low Risk IT Positions

94.2.1 A general user (a user without special access privileges) may access the agency's computer systems with sensitive information after:

- (a) Forwarding a completed signed verification form required under Subsection A (*See Attachment A*) to the IT Security Program Manager; and
- (b) The Network Account Policy procedures have been performed (*See Subsection C*).

94.2.2 To retain their account privileges after the two-week period described in section 94.1, general users must:

- (a) Submit a completed Form SF-85 to the Personnel Security Office, and
- (b) Favorably pass a National Agency Check and Inquiries (NACI).

94.2.3 If a NACI raises security concerns and the Security Office so advises, the Peace Corps may suspend or deny access to the user until the concerns are satisfactorily resolved.

94.3 Privileged Users in Moderate Risk IT Positions

94.3.1 Moderate risk positions include, but are not limited to, local administrators, mainframe account managers, database administrators, and developers of sensitive systems.

94.3.2 Privileged access to sensitive systems by users in moderate risk positions may be provided after:

- (a) A signed verification form from the requester is forwarded by the user to the IT Security Program Manager;
- (b) The Network Account Policy procedures have been performed;
- (c) A completed Form SF-85P is submitted to the Personnel Security Office; and
- (d) The user favorably passes a Minimum Background Investigation (MBI).

94.3.3 No Objection Waiver

A No Objection Waiver (NOW) may be requested from the personnel security office when it is necessary to grant access to a sensitive system and the privileged user in a moderate risk position has not yet favorably passed the security check. The waiver shall be granted if the Personnel Security Questionnaire has not raised any significant concerns. If at any time during the pending investigation, any issues of concern are raised, the waiver may be withdrawn and privileged access must be terminated until the issue of concern is resolved. The waiver requirements shall remain in effect until the investigation has been completed and results in a favorable outcome.

94.4 Privileged Users in High Risk Positions

94.4.1 High risk positions include, but are not limited to, domain administrators, mainframe operators, Unix system administrators and/or those who have Unix “root” privileges, program managers involved with sensitive information, and agency IRM managers.

94.4.2 Privileged access to sensitive systems by users in high risk positions may be provided after:

- (a) A signed verification form is forwarded by the user to the IT Security Program Manager;
- (b) The Network Account Policy procedures have been performed;
- (c) The user has completed and submitted Form SF-86; and
- (d) The user favorably passes a Background Investigation (BI).

94.4.3 No Objection Waiver

A No Objection Waiver may be requested from the personnel security office when it is necessary to grant access to a sensitive system and the privileged user in a high risk position has not yet favorably passed the security check. The waiver shall be granted if the Personnel Security Questionnaire has not raised any significant concerns. If at any time during the pending investigation, any issues of concern are raised, the waiver may be withdrawn and privileged access must be terminated until the issue of concern is resolved. The waiver requirements shall remain in effect until the investigation has been completed and results in a favorable outcome.

94.5 Special Requirements for Contractors

94.5.1 Before working on a Peace Corps contract, “contractor entities” who work on-site, and those who work off-site and are designated by the Contracting Officer as subject to this requirement, must:

- (a) Provide all necessary background information requested by the agency for all on-site personnel, designated key personnel, and any other personnel deemed necessary by the Peace Corps; and
- (b) Certify in writing that they will notify the agency’s Office of Contracts and physical security office upon the termination or departure of any of their contract employees and accept responsibility for the return of all government owned or furnished equipment, keys, and identification badges.

94.5.2 Before working on a Peace Corps contract, “individual contractors” who work on-site, and contractors who work off-site and are designated by the Contracting Officer as subject to this requirement, must:

- (a) Submit their personnel security questionnaire forms to the personnel security office;
- (b) Submit a resume to the personnel security office; and
- (c) Favorably pass the appropriate security investigation or be granted a No Objection Waiver.

94.6 Special Requirements for Temporary Contractor Positions

Temporary contractor positions have special requirements for privileged access. The Director of IRM may issue a waiver of these requirements, on a case-by-case basis, for Temporary Contractor positions ONLY.

A temporary contractor position is a position where the total hours worked do not exceed an aggregate of 30 days per one year period, in either a single continuous appointment or a series of appointments.

94.6.1 Before working on a Peace Corps contract, temporary “contractor entities” who work on-site, and temporary contractors who work off-site and are by the Contracting Officer as subject to this requirement, must:

- (a) Provide all necessary background information requested by the agency for all on-site personnel, designated key personnel, and any other personnel deemed necessary by the Peace Corps; and

(b) Certify in writing that they will notify the agency's Office of Contracts and physical security office upon their termination or departure and will return all government owned or furnished equipment, keys, and identification badges.

94.6.2 Before working on a Peace Corps contract, temporary "individual contractors" who work on-site, and temporary contractors who work off-site and are designated by the Contracting Officer as subject to this requirement, must:

(a) Submit completed Personnel Security Questionnaire forms SF-85P or SF-86 to the personnel security office;

(b) Submit a resume to the personnel security office; and

(c) Favorably pass a NACI security investigation and credit check or be granted a No Objection Waiver.

Subsection M: Policy for Peace Corps' Data Center and Other IT-Sensitive Areas

100.0	Purpose	72
101.0	Applicability	73
102.0	Definitions	73
102.1	“Authorized Personnel”	73
102.2	“Computer Operations Staff”	73
102.3	“Data Center”	73
102.4	“IRM Labs”	73
102.5	“IT sensitive/secure areas”	73
102.6	“Telephone Closets”	73
102.7	“Uninterrupted Power Supply (UPS) Room” and “Pre-Action Valve Room”	73
102.8	“Visitor”	73
103.0	Policy	73
104.0	Level of Risk	74
105.0	Access to the Data Center	74
105.1	Full Access	74
105.2	Restricted Access	74
105.3	Temporary Access	75
105.4	Visitor Access	75
106.0	Access to Other IT Sensitive Areas	76
107.0	Roles and Responsibilities	76
107.1	Oversight Responsibility	76
107.2	Peace Corps IT Security Program Manager	77
107.3	Computer Operations Staff	77
107.4	Data Center Manager	77

100.0 Purpose

This subsection sets out the policy and procedures regarding the physical access of authorized personnel to the Peace Corps Headquarters' IT-sensitive/secure areas at headquarters, which include the Data Center, Telephone Closets, IRM Labs and the Uninterrupted Power Supply (UPS) Room.

101.0 Applicability

This policy applies to any individual requesting access to a Peace Corps IT-sensitive/secure area at headquarters.

102.0 Definitions

102.1 “Authorized personnel” means approved personnel who have been assigned a card or door key to the Data Center or have a restricted-level of access. Names of authorized personnel are listed and posted in the Data Center Access List Memorandum or the Restricted Access List.

102.2 “Computer operations staff” are agency personnel whose permanent work area is in the Data Center.

102.3 The **“Data Center”** is a secured area that is staffed twenty (20) hours a day, five (5) days a week, and from 9 A.M. through 5 P.M. on some Saturdays. The Data Center is located on the third floor of the Peace Corps Building in Room 3305.

102.4 “IRM labs” are rooms used by technical staff under IRM supervision for testing and maintenance of equipment.

102.5 The term **“IT-sensitive/secure areas”** includes the Data Center, IRM Labs, Telephone Closets, and the UPS Room.

102.6 “Telephone Closets” are rooms located on each floor of the headquarters building which contain phone trunks and telecommunications equipment, including routers and patch panels.

102.7 “Uninterrupted Power Supply (UPS) Room” or “Pre-Action Valve Room” is the room on the third floor of the headquarters building that contains UPS and the air-conditioning controls and equipment for the Data Center.

102.8 “Visitor” means anyone who has not been authorized or assigned a card key to access Peace Corps facilities, but who have a specific business-related need to access an IT-sensitive/secure area. Visitors’ names are not listed on the Data Center Access list.

103.0 Policy

No individual may access any Peace Corps IT-sensitive/secure area except as permitted under this subsection. No card key may be issued to an individual without prior approval from the IRM Director.

104.0 Level of Risk

All Peace Corps IT system users must successfully undergo the appropriate security investigation and approval process set out in Subsection L in order to access the agency's sensitive IT systems. When approved for access to the Agency's sensitive systems, each user is designated to have either a low, moderate or high risk level. When an individual is approved for permanent, unsupervised access to the Data Center, his or her risk level will be raised one level. Thus, if an individual's IT-position has been identified as having a moderate level of risk, the risk level will be raised to a high level of risk, if the individual is approved for access to the Data Center.

105.0 Access to the Data Center

Only authorized personnel on official business will be permitted to access the Peace Corps Data Center.

105.1 Full Access

"Full access" means authorized, unsupervised card key access to the Data Center for 24 hours a day, seven days a week.

105.1.1 Full access to the Data Center may be approved for:

- (a) Peace Corps staff members whose job functions require them to regularly access hardware in the Data Center within a two-week period;
- (b) Peace Corps staff members whose permanent work area is in the Data Center;
- (c) Authorized facilities staff members, such as cleaning staff;
- (d) Direct supervisors of any of the above; and
- (e) The Peace Corps Chief Information Officer (CIO), the Director of IRM, and the Information Technology Security Program Manager (ITSPM).

105.1.2 Individuals with full access authorization shall use an assigned card key for access, and their names shall be listed in the Data Center Access List that must be posted on the entrance doors to the Data Center and by the Visitor's Log inside the Data Center.

105.2 Restricted Access

"Restricted Access" means authorized, supervised access to the Data Center during business hours only.

105.2.1 Restricted access may be approved for users who require infrequent use of the Data Center, such as users who run periodic reports or are backups for “full access” users, or who are otherwise determined by the IRM Director to require restricted access.

105.2.2 Users with restricted access authorization are not assigned a card key to enter the Center. Rather, they must enter through the front door of the Center after being identified and permitted to enter by the Data Center manager or staff. Staff shall verify that they are in place to monitor the particular Data Center area to which the RA person is requesting access. Restricted access users must sign in and out in the visitor’s log inside the Center and must be accompanied and monitored by an individual with full access authorization.

105.3 Temporary Access

“**Temporary Access**” means authorized, unsupervised access with a card key to the Data Center only during business hours and only for a specified period of time, not to exceed one month.

105.3.1 Temporary access may be authorized for individuals who are working on a project that requires frequent access to the Data Center, as do full access users, but only for a specified period of time.

105.3.2 An individual with temporary access authorization may enter the Data Center during business hours with an assigned card key. During non-business hours, an individual with temporary access authorization will be treated as a visitor.

105.3.3 An Individual who would otherwise be issued full access but is awaiting the final security check will be given temporary access with their No Objection Waiver (NOW).

105.4 Visitor Access

105.4.1 Visitor access may be authorized for anyone who does not have access authority under Sections 105.1 through 105.3, whose authorized card key is not available, or whose access authority does not cover the time period for which the individual requests access to the Data Center.

105.4.2 A visitor whose name appears on the Data Center’s restricted access list will be allowed unescorted access to the Data Center during business hours. Except as described in Section 105.4.3, all other visitors must obtain prior approval before they can access the Data Center. A visitor who has been pre-approved shall ask the guard at the security desk to call the pre-assigned IRM contact who shall escort the visitor to the Data Center. If the visit has not been

pre-approved, the visitor will be denied access until the appropriate approval can be obtained.

105.4.3 Maintenance personnel on regularly scheduled visits shall have their identification verified by the Data Center staff and their name and the date and purpose of their visit noted in the visitors' log. Specific vendor maintenance personnel whose access has not been pre-approved will be granted access if they are responding to a call made by the Data Center operations staff. Police and fire personnel responding to an emergency call from the Peace Corps or building management may deviate from any part of the procedures in this subpart that inhibit their emergency response efforts.

105.4.4 All visitors shall enter the Data Center through the front doors in order to be visible to the Data Center manager and staff. Visitors must sign in and out in the visitors' log inside the Data Center. When a visitor is escorted, it is the responsibility of the escort to ensure that the visitor signs in and out.

105.4.5 A visitor's activities in the Data Center shall be monitored to ensure that the activities are consistent with the purpose of the visit noted in the visitors' log.

105.4.6 Tours of the Data Center must be scheduled in advance with the IT Security Program Manager. Each tour participant shall be identified and approved in advance, but only the tour leader or coordinator is required to sign the visitors' log. Tour participants are subject to all other requirements applicable to visitors in this subsection.

106.0 Access to Other IT-Sensitive Areas

Other IT-sensitive/secure areas are typically not staffed. The IRM Director will determine and approve access to these areas. Access by individuals who do not possess an assigned card key must be supervised.

107.0 Roles and Responsibilities

107.1 Oversight Responsibility

The Peace Corps IT Security Program Manager, Data Center Manager, and contractor computer operations staff are responsible for protecting the Data Center against unauthorized access. They must ensure that personnel have the appropriate authority, are trained in the physical access procedures, and challenge anyone WHO DOES NOT APPEAR TO BE CONDUCTING OFFICIAL BUSINESS. Computer operations personnel are also responsible for safeguarding confidential and/or sensitive information.

107.2 Peace Corps IT Security Program Manager

Under direction of the Director of IRM, the Peace Corps IT Security Program Manager is responsible for:

- (a) Authorizing physical access to the Data Center;
- (b) All policies regarding physical access to the Data Center;
- (c) Maintaining the full access list and restricted access lists that are posted in the Data Center; and
- (d) Controlling the method for obtaining card keys for all authorized IRM personnel, including contract personnel, in a manner that assures access to sensitive/secure areas only by authorized personnel.

107.3 Computer Operations Staff

Computer Operations personnel are responsible for:

- (a) Ensuring that access to the Data Center is monitored and that any violations are reported to the IT Security Program Manager;
- (b) Knowing the procedures for controlling access to the Data Center during non-business hours; and
- (c) Monitoring visitors in the Data Center.

107.4 Data Center Manager

The Data Center manager is responsible for:

- (a) Enforcing the policy in this subsection;
- (b) Supervising the Computer Operations staff in regard to their Data Center responsibilities;
- (c) Briefing new computer operations staff on the policies set out in the subsection upon their arrival;
- (d) Reviewing the policy in this subsection with the Computer Operations staff quarterly;
- (e) Maintaining the visitor log by reviewing entries daily and by archiving old logs, as necessary; and

(f) Promptly reporting any areas of security concern, such as identified areas of vulnerability or deficiency.

ATTACHMENTS:

A: Verification Form

B: Response Procedures for Domestic Security Incidents

C: Position Descriptions

D: Computer Security Coordinator Responsibilities