Peace Corps Office of the OCIO
Information and Information Technology Governance and Compliance
Rules of Behavior for General Users

Table of Contents

Rules of Behavior for General Users 1

A. Accountability 1

B. System Use Notification (Login Banner) 1

C. Non-Compliance 1

D. System Access 2

E. User IDs 2

F. Passwords 2

G. Electronic Information 3

H. Agency Electronic Mail (email) 3

I. Remote Access 4

J. Computer Equipment 5

K. Unofficial Use of Government Equipment 5

L. Unattended Computer Equipment 6

M. Protection of Copyright Licenses (Software) 6

N. Authorized Software and System Configuration 6

O. User Responsibilities to protect Peace Corps Sensitive Information 7

P. Classified Information 7

Q. Cyber Security Incident Reporting 7

R. Disposal of Peace Corps information systems 8

S. Personnel Orientation 8

Users' Verification Form 10

Peace Corps Office of the OCIO
Information and Information Technology Governance and Compliance
Rules of Behavior for General Users

Rules of Behavior for General Users

The Rules of Behavior constitute the requirements, practices, and controls governing the handling of sensitive information and the use of Peace Corps information systems. "Sensitive information" includes Personally Identifiable Information (PII), electronically protected health information (ePHI), and information not approved for release to the public. Peace Corps information systems include applications, computers, mobile IT devices, network, infrastructure, bandwidth, or any other component that has computing capabilities or enables access to Peace Corps information. All users of Peace Corps information systems are expected to utilize such resources in a professional, responsible, ethical, and legal manner consistent with applicable federal and Peace Corps requirements. These Rules of Behavior are applicable to all individuals with access to Peace Corps information systems.

A. Accountability

Users of Peace Corps information systems are accountable for their actions and may be held liable for any unauthorized actions. Any failure to comply with the Rules of Behavior shall be considered a security incident. If the security incident is deemed willful, it will be escalated to a security violation.

B. System Use Notification (Login Banner)

When accessing a Peace Corps information resource, the user agrees to the following System Use Notification, even if the entire banner is not displayed due to technology constraints:

> This computer system is the property of the United States Peace Corps. It may only be accessed and used for official Government business by authorized personnel.
> Unauthorized access or use of this computer system is strictly prohibited and may subject violators to criminal, civil, and/or administrative action. The Peace Corps may monitor any activity, information, or communication on the system.
> All activity, communication, and information on this system may be intercepted, recorded, read, copied, retrieved, and disclosed by and to authorized personnel for official purposes, including criminal investigations.
> Users have no right of privacy or any reasonable expectation of privacy in the use of this computer system and any communication or information stored within the system.
> Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to all of these terms.

C. Non-Compliance

These Rules of Behavior and Peace Corps Manual Sections are based on federal laws and regulations. There are administrative, civil, and criminal consequences for non-compliance. Depending on the number of security violations and the sensitivity of the information involved, noncompliance with these rules and Peace Corps Manual Sections will result in sanctions commensurate with the level of infraction. Sanctions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

D. System Access

To be granted access to Peace Corps information systems, users must complete the required personnel screening and new user security awareness training, and submit a signed Rules of Behavior acknowledgement form.

- Initial access to Peace Corps information systems and any changes to that access require authorization by a supervisor.
- The level of access to Peace Corps information systems granted to each user is based on the user's organizational role and specific assigned duties, and is constrained to the minimum set of privileges required to perform those duties.
- Users shall work within the confines of the access allowed to them and shall not attempt to access systems or applications, control information, software, hardware, and firmware to which access has not been authorized.
- Individuals will not retrieve information from an information system for someone who is not authorized to access the information system and who does not need the information to perform their assigned duties.
- Users are required to successfully complete the annual Cyber Security Awareness Training to retain their access to Peace Corps information systems.
- Users must not access an information system that they are no longer authorized to access (e.g., completion of project, transfer, retirement, or resignation).

E. User IDs

User IDs are assigned to individuals and should not be shared with or used by other persons or groups. Remote access tokens are another form of authentication, and should not be shared with or transferred to any other individual.

F. Passwords

G. User passwords must be created in accordance with Peace Corps policy. See Peace Corps Cybersecurity and Policy Catalog for requirements.

Users are responsible for:

- Maintaining the secrecy of their password, which means that a user's password may not be revealed to anyone, regardless of position, either inside or outside of the Peace Corps;
- Creating and using passwords that meet or exceed the required complexity, length, and strength;
- Changing their passwords in accordance with Peace Corps policy (see Peace Corps Cybersecurity and Policy Catalog);
- Notifying the Peace Corps Service Desk (ServiceDesk@peacecorps.gov) to report an incident and change their passwords if they suspect the password has been compromised;

Users must not utilize another individual's password and User ID or allow others to utilize their password and User ID.

H. Electronic Information

All electronic information, records, files and emails created, collected, processed, transmitted, aggregated, stored, or disposed of via Peace Corps computers or networks are the property of the Peace Corps and may be accessed by the Peace Corps. Users will abide by the requirements established in MS 892 - Records Management for the policies regarding the management of files, records, and non-records. Users should have no expectation of privacy when using Peace Corps information systems, including when using Peace Corps email systems or the internet.

Except as necessary to perform their jobs, users may not create, download, view, store, copy, or transmit any materials related to gambling, illegal weapons, terrorist activities, other illegal or prohibited activities, or any sexually explicit or sexually oriented materials. Users must also comply with the law that regulates the political activities of federal employees and some state and local government workers, known as the Hatch Act. Downloading information from the Internet should be done with care.

I. Agency Electronic Mail (email)

Each Peace Corps user will be provided a peacecorps.gov email account for conducting official Peace Corps business. This account shall be the only account Peace Corps personnel may use to conduct official Peace Corps business. As with all Peace Corps electronic information, email messages are government property and Peace Corps officials may have access to those messages whenever there is a legitimate governmental purpose for doing so.

The following are prohibited:

- Use of the peacecorps.gov email account for non-Peace Corps business other than limited personal use in accordance with MS 547 - Use of Government Technology Services and Equipment, section 4.2: Limited Personal Use.
- Use of non-Peace Corps issued email accounts for official Peace Corps business, unless specifically authorized by an individual's supervisor during a disruption of Peace Corps email service;
- Use of the Peace Corps email system for business purposes other than Peace Corps business, including using the system for private commercial activities;
- Using or sending anonymous email for any purpose (email communications must accurately identify the sender);
- Use of the email system to intentionally misrepresent oneself or the Peace Corps;
- Establishing a personal social media account using a peacecorps.gov email address
- Use of the email system to send or receive any information that is sexually explicit or derogatory toward any race, religious, or ethnic group, any harassing or obscene material or any mass mailing, such as spam, chain letters, or junk mail;
- Use of the email system to send Peace Corps Sensitive or proprietary information to unauthorized individuals, or to breach the standards of conduct;
- Use of the email system to transmit classified information;
- Use of the email system for unlawful activities or to send any communication that violates security policies, federal laws, or regulations;
- Use of the email system for malicious activities, such as knowingly activating and/or propagating computer viruses or other malicious code, or purposefully disguising the true content of an email message with a subject or title that is not reflective of the message content;
- Permitting others (supervisors, secretaries, assistants, or any other subordinate) to use your email accounts as their own;

Peace Corps email users have the responsibility to protect email services by:

- Not opening email of an unknown or unexpected origin; unexpected email or email from unknown senders may contain malware or be part of a phishing scheme. If in doubt, do not open such email. Contact the OCIO Security Office for further action.
- Ensuring that emails that are considered official records are not deleted.
- Ensuring that email messages that are no longer required are deleted.
- Using "Reply" rather than "Reply to All "when responding to an email, unless the response is applicable to all addressees. Email should be sent only to those parties to whom action or pertinent information is directed. The "Reply to All" email response

slows messaging for all employees and regularly creates backlogs in employees' inboxes.

J. Remote Access

- Individuals may be granted remote access privileges as a part of their roles and responsibilities.
- Remote access is subject to the same rules of behavior that apply when a user is physically located at a Peace Corps facility as well as the MS 545 Mobile Information Technology Device Policy and the associated Remote Access and Mobile IT Device User Guide.
- Modifying remote access software or other security configuration e.g., VPN clients, and access settings, on a mobile device is prohibited.
- Peace Corps remote access use is a privilege that can be revoked at any time without prior notice.

K. Computer Equipment

Unless specifically issued a laptop or other mobile computing device, individuals may not remove Peace Corps equipment from a Peace Corps facility without proper authorization.

When using Peace Corps furnished computer equipment, individuals shall:

- Take reasonable steps to safeguard computer equipment against waste, loss, abuse, unauthorized access/use, and misappropriation;
- Hand carry the mobile device; never include the mobile device with checked baggage during travel; keep the device out of plain view; store the device in a locked location; and carry removable and hard drives separate from the device when not in use;
- Use only that equipment they have been authorized to use;
- Promptly report missing computer property to the Peace Corps Service Desk (ServiceDesk@peacecorps.gov) to report an incident [see section Q for more details on cyber security incident reporting]; and
- Only use software that has been licensed for use and only for authorized purposes.

When using Peace Corps furnished equipment, individuals shall NOT:

- Eat, drink, or smoke near computer equipment or storage media in a manner that would endanger the equipment or media;
- Store highly combustible materials near the computer;
- Move or remove any computer equipment without proper permission;
- Install any non-approved hardware, including media players and USB devices;

- Remove, sanitize, or destroy any Peace Corps-issued computing device, hard drive, or storage media without proper authorization;
- Allow anyone to perform maintenance on computer equipment without proper authorization;
- Download or install any unapproved software, including peer to peer (P2P) file sharing software (e.g. Torrent software); and
- Transmit, post, store, or otherwise distribute information to individuals without authorized access.
-

L. Unofficial Use of Government Equipment

Agency personnel shall use Peace Corps information systems for official and authorized purposes only, except as permitted under MS 547 - Use of Government Technology Services and Equipment.

M. Unattended Computer Equipment

Users are responsible for securing computer equipment issued to them. Within Peace Corps facilities this means that users must always activate their password protected screen saver, lock their computer, or log off of their computer when stepping away from their work space. All activity occurring when the workstation is functioning is the responsibility of the logged-on user. Users are to protect terminals or workstations from unauthorized access.

When departing their workspace, users must log off of their computer but leave the computer powered on. (Powering off equipment prevents it from receiving required maintenance and patching and this could cause your computer to be vulnerable to viruses, spam, etc.).

For mobile devices - which include laptops, smart phones, thumb drives, or any other portable IT device capable of creating, collecting, processing, storing, aggregating or transmitting information – users are responsible for taking reasonable precautions when transporting and using these devices outside of Peace Corps facilities. This includes securing both the physical device and the Peace Corps information you may possess. Additional guidance can be found in MS 545 – Mobile Information Technology Device Policy.

N. Use of Loaner Equipment

- When using loaner equipment all related Peace Corps policies, procedures and guidelines must be followed. Unauthorized use of any Peace Corps mobile IT device is prohibited. Additional guidance can be found in these rules of behavior, MS 511 Personal Property

Management, IPS 1-17 Information Security Program, MS 545 Mobile Information Technology Device Policy, and MS 547 Use of Government Technology Service and Equipment.

- Upon separation separation from the Peace Corps, the user will return the laptop to the CIO/CSS office for inventory.
- Processing or storing Peace Corps sensitive information, which includes personally identifiable information (PII), as deifned in IPS 1-17 Information Security Program, on a personal device, incuding thumb drives, or personal email account is prohibited. The only exception to this rule is when the Peace Corps Continuity of Operations (COOP) Plan is activated.

O. Use of Personal Equipment

The Peace Corps does not provide technical support for personal (non-Peace Corps) owned equipment or software e.g., a personal smartphone with BYOD services loaded onto it or a personal tablet with the VMware View application loaded onto it.

P. Protection of Copyright Licenses (Software)

All users shall comply with software licensing agreements and Federal copyright laws.

Q. Authorized Software and System Configuration

Users may not download, install, or use unauthorized software, including freeware, shareware, or public domain software, on Peace Corps information systems without OCIO approval. If new software is required, a request must be submitted through the Service Desk, the Post's IT Specialist, or the business unit's OCIO Point of Contact. Individuals are not permitted to circumvent system permissions. Individuals may 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 information systems, unless explicitly tasked to do so by OCIO as an official duty. Security vulnerability tools are to be used by approved personnel ONLY and use must be limited to a pre-approved period of time. Individuals are prohibited from installing or using malicious software, such as computer viruses or worms.

Users shall:

- NOT attempt to modify or disable any of the security features/programs on Peace Corps computers, including virus protection software and the password-protection function on screen savers;

- 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
- Notify the Service Desk immediately upon the detection or suspicion of any malicious code stored or transmitted on the Agency's network, to include related computer equipment and media; and cooperate fully with efforts by technical support staff to address the problem.

R. User Responsibilities to protect Peace Corps Sensitive Information

Peace Corps Sensitive Information is any information that has limited access, is not explicitly intended for public consumption, or has internal constraints on its access. Examples of Peace Corps sensitive information include, but are not limited to the following: Personally Identifiable Information (PII), electronic Protected Health Information (ePHI) or other medical information, inter-agency or intra-agency memorandums, information in Privacy Act systems of records, internal personnel rules and practices of the Peace Corps, trade secrets, privileged or confidential commercial or financial information obtained from a person, and records of information compiled for law enforcement purposes.

PII refers to information, such as name, social security number, or biometric records which alone or when combined with other personal or identifying information linked or linkable to a specific individual, such as date and place of birth or mother's maiden name, can be used to distinguish or trace an individual's identity.

Peace Corps Sensitive Information may not be accessed, retrieved, shared with, or distributed to individuals without authorized access.

Except by explicit waiver, all Peace Corps Sensitive information that includes PII and ePHI must be encrypted using a FIPS 140-2 compliant encryption package before transmission across public communication systems. This includes email. Peace Corps' Secure File Transfer Protocol (SFTP) email system meets this requirement. All removable media, printouts or other material containing Peace Corps Sensitive Information must be picked up from the printer immediately.

S. Classified Information

Classified information shall NOT be processed or stored on Peace Corps information systems. See MS 405 Classified National Security Information, which provides procedures for the handling of classified information

T. Cyber Security Incident Reporting

Individuals must report all cyber security violations, incidents, vulnerabilities, or suspicious

events or behavior involving Peace Corps information or information systems to their supervisor and to the Service Desk or the Post's IT Specialist immediately. This includes missing computer equipment such as laptops, tokens, mobile IT devices, and any media that contains Peace Corps Sensitive Information. If a user suspects their password has been compromised, they must immediately report this to the Service Desk or their Post's IT Specialist and their immediate supervisor as an incident. If a cyber security incident involves Personally Identifiable Information (PII) or electronic Protected Health Information (ePHI), the user must report it within 24 hours of detection to the Service Desk (202-692-1000 or helpdesk@peacecorps.gov) and Cyber Incident Response Coordinator (CIRC).

U. Disposal of Peace Corps Information Systems

The disposal of Peace Corps information systems must adhere to MS 511 Property Management. Prior to disposal, any information and information systems capable of creating, collecting, processing, storing, aggregating, or transmitting information must be properly sanitized to ensure Peace Corps Sensitive Information is not retrievable. This includes shredding of documents and optical media and degaussing or overwriting of electronic media in accordance with Peace Corps Media Sanitization Procedures.

V. Personnel Orientation

The review and acknowledgement of these Rules of Behavior is a required step in the orientation of all personnel and must be completed in advance of access being granted to Peace Corps information systems.

This page is intentionally left blank

Users' Verification Form

I, _____ (PRINT full name):

have read the Peace Corps Information and IT security Rules of Behavior for General Users and I agree to abide by these rules. I understand that I am responsible for protecting Peace Corps information systems and shall receive documented approval from authorized parties before deviation from the Rules of Behavior and Peace Corps requirements.

I understand that, Peace Corps mobile device use is a privilege that can be revoked at any time without prior notice.

I understand that, if I do not comply with the Rules of Behavior and Peace Corps requirements, I am subject to have sanctions placed against me such as, but not limited to, disciplinary actions for such violations, administrative leave, suspension, termination, and/or civil or criminal prosecution.

I understand that I may be asked to reimburse the agency for the cost of computer equipment, only in circumstances that clearly demonstrate a lack of reasonable steps to safeguard against waste, loss, or abuse.

_____ (Signed)

_____(Date mm/dd/yyyy)