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

What is a Privileged User?

A privileged user is someone who has been granted privileged access to information or information systems. Privileged users possess administrative or other elevated privileges and are authorized to perform security-relevant functions that general users are not authorized to perform. These privileges include system engineering responsibilities, or the ability to alter an information system or application configuration settings of any type. Privileged Users may include, but are not limited to, domain administrators, elevated users, system administrators and/or those with root privileges, program managers involved with Peace Corps sensitive information, Agency managers, local administrators, database administrators, and developers of Peace Corps systems. Potential compromise of privileged user accounts carries a risk of substantial damage and therefore privileged user accounts require additional safeguards. Privileged users will also be assigned a general user information systems account.

Rules of Behavior for Privileged Users

Privileged users should follow the rules outlined in the Rules of Behavior for General Users and the rules of behavior contained within this document. Any failure to comply with the Rules of Behavior for Privileged Users or violation of their administrative privileges shall be considered a security incident. If the security incident is deemed willful, it will be escalated to a security violation. Noncompliance with these rules and the Rules of Behavior for General Users will be addressed through sanctions commensurate with the level of the infraction. Depending on the number of security violations, their severity, and the sensitivity of the information involved, disciplinary actions for such violations may consist of a letter or warning/caution, a suspension, or termination.

A. System Privileges

Privileged access to information or information systems will not be granted without completion and approval of the Information System Access Authorization Form by the privileged user's sponsor/supervisor. Once privileged access is provided by the Service Desk (202-692-1000) to an authorized user, the privileged user will not:

- Elevate privileges of any user without completion and approval of the Information System Access Authorization Form;
- Circumvent Peace Corps policies or security controls;
- Use a privileged account for non-administrative duties;
- Use a privileged account for internet access except in support of administrative-related activities**.**

Individuals are granted privileged access either on a temporary or permanent basis to applicable Peace Corps information systems based on a need to perform their role's assigned tasks. Privileged users shall work within the confines of the access allowed to them as identified in the Information System Access Authorization form and shall not attempt access to information systems or applications to which access has not been authorized by the information system owner (business process owner). Privileged users will not retrieve information from an information system for someone who is not authorized to access the information or who does not

need the information to perform their job. Privileged users are granted elevated access based on their roles and responsibilities and according to "need to know"[1] and "least privilege."[2]

B. User IDs and Passwords

All users with privileged access to Peace Corps information and information systems require a unique User ID and Password, unless otherwise authorized in order to support specific business requirements. User IDs are assigned to individuals and should not be shared with or used by other persons or groups. Privileged users are responsible for:

- Utilizing the privileged account only for its intended purpose**;**
- Creating and using passwords that meet or exceed the required complexity and length established in the Systems Access and Account Management Standard Operating Procedures;
- Changing their passwords at least every 90 days and immediately if they suspect the password has been compromised;
- Protecting "privileged accounts passwords" at the highest level demanded by the sensitivity level of the system;
- Storing administrator passwords in a designated locked file cabinet or safe to prevent the passwords from being acquired by a malicious party with physical access to the work space.

If a user suspects their password has been compromised, they must immediately report this to the Service Desk, their Information System Security Officer (ISSO), and their immediate supervisor as an incident.

C. Individual Accountability

Privileged users are accountable for all actions associated with the use of their assigned User ID(s). Privileged users will be held responsible for unauthorized actions found to be intentional, malicious, or negligent. Every action taken with an individual's User ID(s) will be monitored and recorded as being done by that individual. Privileged users will not remove, destroy, or alter system audit, security, event, or any other log data unless authorized by the information system owner and ISSO in writing.

Privileged users will only use their own privileged user account(s) and only for official administrative actions, not for general account activities. Privileged users will log off the privileged account when official administrative actions are completed and conduct normal daily responsibilities on their general user account. Once the privileged user account is no longer needed, the user must contact the Service Desk (202-692-1000) immediately to have the privileged account disabled.

[1] having the specific work related reason to know that information
[2] having the minimum set of systems access privileges required to perform the assigned duties

D. E-mail Usage

Privileged users will not use their privileged account(s) for non-administrator related communications.

E. Contingency Plans

Privileged users will understand and follow system disaster recovery and contingency plans.

F. Incident Response

Privileged users will report and follow-up on all system security incidents in a timely manner. Privileged users will also follow the Incident Response Plan (IRP) when a security incident occurs and notify the Service Desk and the ISSO.

G. Authorized Software and System Configuration

Privileged users will not:

- Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information system security controls, unless authorized by OCIO.
- Introduce unauthorized code or malware (e.g. computer viruses, worms, Trojan horses, spyware, logic bombs, and other malicious and unwanted software or programs) into Peace Corps information resources.
- Develop, code, compile, store, transmit, or transfer malicious software code.
- Circumvent or disable Anti-Virus Software.

All software in use on a Peace Corps information system must first be approved by the OCIO Change Control Board (CCB) (cioccb@peacecorps.gov) for inclusion in a baseline configuration. Privileged users will ensure that information placed on a public access system is approved in accordance with Peace Corps' policies regarding content and security.

Privileged Users' Verification Form

I, _____ (PRINT full name):

Have read the Rules of Behavior for Privileged Users and agree to abide by these rules in addition to the rules outlined in the Rules of Behavior for General Users. I understand that I am responsible for protecting Peace Corps information and information systems and shall receive documented approval from the OCIO before deviation from the Rules of Behavior and Peace Corps requirements.

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.

_____ (Signed)

_____ (Date mm/dd/yy)