

**Federal Pell Grant
Rules of Behavior
A statement of User Responsibility**

User Acknowledgment - Personnel who use any ED/ACS/CSC computing resource (e.g., PCS, workstations) and associated networks shall read and sign this statement annually. The user will keep copies of the signed acknowledgment; the originals will be placed in the user's official personnel file.

For Official, Approved Use Only - the Government funds Pell Grant computing resources to support various programmatic efforts needed to accomplish the Department's mission. As such, these resources are to be used only for official Government business. Users should remember that when they use the Pell Grant computing resources, they are acting in their employment capacity for ED. Unless approved in writing by management, we must avoid any activity outside that employment capacity, or which could bring harm or embarrassment to ED/ACS/CSC.

Privacy Expectations - we caution all users that, overall, computers, networks, and information systems are not "private". Users should have no expectation of privacy when using computing resources. Electronic mail sent via the network may bear site-specific identifiers in the address (e.g., *name@cdis.com*, or *name@ed.gov*). As such, despite disclaimers, users using ED/ACS/CSC E-mail are representing the site and ED/ACS/CSC and must act accordingly.

Monitoring of Computing Resources - Activities on ED/ACS/CSC systems and networks are subject to monitoring, recording, and periodic audits to ensure that the resources are functioning properly and to protect against unauthorized use. The system administrator may access any "user's" computer system or data communications and disclose information obtained through such auditing to appropriate third parties, e.g., law enforcement personnel. Use of ED/ACS/CSC computing resources is expressed consent by the user to such monitoring, recording, and auditing.

Violations - Adherence to accepted user principles regarding appropriate use by all users is critical. Violations of these principles or ED/ACS/CSC computer policies may lead to disciplinary action, up to and including termination of employment.

Manager/Supervisor Responsibilities - Management personnel must be leaders in applying these user principles. Managers are responsible for implementing these accepted user principles in their organization and will be accountable for ensuring that users are aware of and acknowledge their responsibilities.

Accepted User Principles

Computer security personnel recognize users of ED/ACS/CSC computers, networks, and information Systems as an integral part of the overall ED computer security program. Users' access to computing resources shows a level of trust bestowed upon them by their management and ultimately by ED. Users are responsible for their actions and need to be aware of and acknowledge their responsibilities.

At a minimum users are responsible for these principles:

- Ensuring that ED/ACS/CSC, computing resources are used only for official government business. The employee's manager must approve any other use in writing.
- Knowing who their site computer security personnel are and how they can be contacted.
- Ensuring that all software is used according to licensing agreements **and** has been authorized for use by management.
- Protecting the information, they are processing from access by, or disclosure to, unauthorized personnel.
- Immediately reporting all security incidents and potential threats and vulnerabilities involving computing resources to designated computer security personnel.

[Sample]

- Protecting their authenticators, such as passwords. Reporting any compromise or suspected compromise of a password to designated computer security personnel.
- Using only systems, networks, data, control information, and software, for which they are authorized.
- Ensuring that system media and system output are marked according to their sensitivity and are properly controlled and stored.
- Knowing required storage sanitization procedures (e.g., overwriting disks that contain sensitive data before reuse).
- Informing management when access to a particular computing resource is no longer required, such as when the user completes a project.
- Avoiding the introduction of malicious code into any computing resource.
- Preventing physical damage to the system.
- Ensuring that Card Keys/Cipher lock combinations to the work area are secured always and not duplicated.
- Notifying management before relocating computing resources. Not removing equipment or storage media from the work area without prior written authorization from the Project Manager or the Pell Grant ACSO.
- Following procedures for signing out sensitive application documentation from the library and ensuring that we do not remove sensitive information from the work area.

Privileged User Principles

Privileged users include those with “superuser, root,” “RACF Master Keys”, or equivalent access to a system (e.g., system administrators; computer operators; ACSOs; those who have control of the operating system of the computer or network or who set up and administer user accounts, passwords, etc.; users having access to change control parameters such as routing tables or path priorities on routers, multiplexors, or other key equipment; users whom we have given the power to control and change other users' access to data, programs, or applications; network administrators; database administrators; users whom we have given special access for trouble shooting or security management functions.) In addition to Accepted User Principles, Privileged Users are also responsible for:

- Protecting the root, superuser, master key, password and not sharing the password and/or account.
- All supervisors, root, master key actions using his or her account.
- Reporting all information system/network, potential security-related incidents to designated computer security personnel.
- Using special access or privileges **only** to perform authorized tasks and functions.
- Using a **non-privileged** user account for everyday work not associated with the tasks of “a superuser or system administrator”.

Management may augment the previous list of responsibilities with additional requirements. Any question about your responsibilities as a user of computing resources should be discussed with your supervisor.

To be completed by the user:

I, _____ have read and understand my responsibilities as a user of ED/ACS/CSC computing resources and will perform my duties accordingly during my employment.

Signed: _____ Date: _____

To be completed by the user's supervisor of record:

[Sample]

I, _____ ensure that _____ has been provided computer security orientation, understands the responsibilities associated with computing resources, and have had all questions satisfactorily answered.

Signed: _____ Date: _____

[Sample]

[Sample]