

Volume VIII , Section 5 – COD System Security

Privacy Notice

The COD System is a United States Department of Education computer system, which may only be used for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

If you use this computer system, you must understand that all activities may be monitored and recorded by automated processes and/or by Government personnel. Anyone using this system expressly consents to such monitoring. Warning: If such monitoring reveals possible evidence of criminal activity, monitored records will be provided to law enforcement officials.

This system contains personal information protected under the provisions of the Privacy Act of 1974, 5 U.S.C. §552a - - as amended. Violations of the provisions of the Act may subject the offender to criminal penalties.

COD Website Access

Schools and Third Party Servicers who wish to receive on-line access to the COD web site must identify personnel to serve as administrators. Administrators will be able to establish additional users within their individual organizations and provide access to the COD web site. The number of administrators is at the discretion of the institution, although it is strongly recommended that the number be limited.

System Administrator Request

In order to establish an administrator account for the COD web site, organizations should submit an administrator request letter printed on university or corporate letterhead to the COD School Relations Center at:

US Department of Education
FSA School Relations Center
P.O. Box 9003
Niagara Falls, NY 14302

This letter must include the following information:

- Security administrator's First Name
- Security administrator's Last Name
- Keyword – Mother's maiden name (used as an identifier if the user forgets their password)
- Work telephone number
- Email address
- OPE ID (For School Requests Only)
- Organization Name (School or Third Party Servicer)
- Job Title
- Work address
- Work fax number
- Security administrator's signature
- School approving authority's name, title, and signature (e.g., Financial Aid Director).

After the COD Relations Service Center has successfully processed the administrator request, administrators will receive their User ID and password through the email address provided in the response letter. An initial email will contain the assigned User ID for the COD web site, along

with instructions for accessing the web site. For security purposes, the password will be delivered in a separate email.

Rules of Behavior

Schools are encouraged, but not required, to establish Rules of Behavior as part of their business processes related to the COD System. The Rules of Behavior developed by the United States Department of Education are available for reference. Please note that these rules have been established for Department of Education employees. Your institution's rules may be different, but should cover all the areas covered in this example.

Introduction

A good security posture supports the business purpose of the organization. Rules of behavior are designed to provide a schema for sustaining the business process, minimizing disruption, maintaining the ability to continue customer support, and supporting a planned and orderly restoration of service in an emergency.

Federal Student Aid (FSA), Common Origination and Disbursement (COD), processes and stores a variety of sensitive data that is provided by students, colleges/universities, financial, and Government institutions. This information requires protection from unauthorized access, disclosure, or modification based on confidentiality, integrity, and availability requirements. The "Rules of Behavior" apply to all employees/users (including corporate, Government, Modernization Partner, and Trading Partner) of the FSA/COD computer system and their host applications.

The rules delineate responsibilities and expectations for all individuals supporting the COD programs. Non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. Depending on the severity of the violation, sanctions may range from a verbal or written warning, removal of system privileges/access for a specific period of time, reassignment to other duties, or termination. Violation of these rules and responsibilities could potentially result in prosecution under local, State, and/or Federal law.

Physical Security

- Keep all badges, access codes, and keys under personal protection.
- Wear your assigned identification security badge at all times while in the office/building.
- Ensure your visitors have signed the visitor's log/are escorted at all times.
- Never allow any individual who does not have proper identification access to the office space.

- Stop and question any individual who does not have proper identification, and contact Security immediately. Seek the support and cooperation of co-workers as appropriate.
- Maintain control over your corporate/Government provided hardware/software to prevent theft, unauthorized use/disclosure, misuse, denial of service, destruction/alteration of data, violation of Privacy Act restrictions.
- Keep your desk clean to ensure that sensitive and proprietary information does not get hidden in minutia and therefore not properly secured/protected when not in use because it is not visible.

Computer Virus Protection

- Use the approved anti-virus software on your personal computer.
- Avoid booting from the A: drive.
- Scan all new diskettes before using or distributing them.
- Write-protect all original vendor-supplied diskettes.
- Back up all data on your workstation and file server regularly.
- Use only authorized and appropriately licensed software.
- Report all incidents of computer viruses to your SSO or manager.
- Do not download, introduce, or use malicious software such as computer viruses, Trojan horses, or worms. All users are required to comply with safe computing practices to reduce the risk of damage by any type of computer virus.

Computer System Responsibilities

- Do not make copies of system configuration files for your own use, unauthorized use, or to provide to others for unauthorized use.
- Do not attempt to access any data or programs on the COD system for which you do not have authorization or explicit consent from the owner of the data or program.
- Do not, without specific authorization, read, alter, or delete any other person's computer files or electronic mail (E-mail), even if the operating system of the computer allows you to do so.

- Do not engage in, encourage, conceal any “hacking” or “cracking,” denial of service, unauthorized tampering, or unauthorized attempted use of (or deliberate disruption of) any computer system within the COD program.
- Do not purposely engage in any activity with the intent to:
 - Degrade the performance of the system;
 - Deprive an authorized user access to a resource;
 - Obtain or attempt to obtain extra resources beyond those allocated; or
 - Circumvent security measures in order to gain access to any automated system for which proper authorization has not been granted.
- Do not download, install, or run security programs or utilities that might reveal weaknesses in the security measures or access privileges of any system. Inform the SSO when you find such a weakness.
- No user, software developer, or Web developer should write or put into production any computer code, program, or script that is considered to be a Trojan Horse (applications that attempt to circumvent any security measures) or any “back door” means of accessing the system or applications.
- Any user that is found to introduce “Trojan Horse” type code, program, or script, is subject to prosecution under local, State, and Federal law and is subject to local department/corporate policies that enforce disciplinary action up to and including dismissal. This policy includes the use of *.rhosts* and *.netrc* files in any user’s home directory for the purpose of avoiding entering keystrokes to gain access to any system.
- No user of any software application should attempt to circumvent any security measures for that application.
- Users should access only the resources of an application that is necessary to perform their job assignments, even though an application may grant further access privileges.

Unofficial use of Government equipment

- Users should be aware that personal use of information resources is not authorized unless sanctioned by management.

- Do not utilize corporate/Government resources for commercial activity or any venture related to personal profit or gain.
- Do not utilize corporate/Government resources for behaviors that are unethical or unacceptable for the work environment.

Work at home

The COD Personnel Policy Directive authorizes Division Directors to designate specific employees (e.g., critical job series, employees on maternity leave, employees with certain medical conditions) as eligible for working at home.

Any work-at-home arrangement should:

- Be confirmed writing.
- Stipulate the duration of the arrangement.
- Identify what corporate/Government equipment/supplies the employee will need, and how the equipment/supplies will be transferred, protected, and accounted for.
- Be discussed with the SSO prior to the start of the employee working at home.
- Reviewed by the Personnel Office prior to commencement.

Dial-in access

The CIO may authorize dial-in access to the COD System. It is understood that dial-in access poses additional security risks, but may become necessary for certain job functions.

If dial-in access is allowed, the CIO and the security office will regularly review telecommunications logs and COD phone records, and conduct spot-checks to determine if COD business functions are complying with controls placed on the use of dial-in lines.

All dial-in calls will use one-time passwords.

If dial-in access is allowed to other applications on the system on which COD resides, the managers of those applications should also determine if such access could pose a risk to COD data.

Do not divulge dial-up modem phone numbers to anyone. If an employee needs dial-up access, refer him or her to the LAN team.

Connection to the Internet

- Use of corporate/Government resources to access the Internet must be approved, and the access should be used for authorized business purposes only.
- Use of corporate/Government resources for accessing the Internet for personal gain or profit, even though you may be using your own ISP, and on your lunch hour/break, is unacceptable.
- Use of corporate/Government provided Internet access is subject to monitoring. Accessing web sites that contain material that is deemed by management to be inappropriate for the workplace, including but not limited to obscene, or sexually oriented material, is prohibited. Disciplinary action may be taken.

E-Mail

- Users will take full responsibility for messages that they transmit through corporate/Government computers and networks facilities.
- Laws and policies against fraud, harassment, obscenity, and other objectionable material apply to electronic communications as well as any other media. Corporate, local, state, and federal laws/rules and regulations may also apply.
- All e-mail that is transmitted on corporate/Government servers is subject to monitoring by corporate/Government personnel.

Copyright

- Never install or use any software that has not been specifically licensed or authorized for use.
- Never download software from the Internet to corporate/Government systems (which is strictly prohibited) without prior authorization/approval. Follow defined procedures for downloading software.
- Adhere to all purchased software copyright, duplication requirements, and license agreements that are imposed by the vendor. Violations place the individual, the corporation, and/or the Government at risk.
- Copyright licenses for software used by COD program personnel must be understood and complied with.

User IDs

- Do not share user identification (IDs) or system accounts with any individual.
- When leaving a session unattended for a short period of time, lock the keyboard with a password-protected screen saver.
- Employ the automatic password/screen saver option feature offered by the operating system (in Windows, use SETTINGS/DISPLAY/SCREEN SAVER) and set the time for 15 minutes as a minimum.)
- Logoff when leaving your session unattended for an extended period of time.
- Be aware of logon and logoff times to ensure that someone else is not using your ID.

Passwords

Your password SHOULD.....

- Be difficult to guess (Do not use names that are easily identified with you or appear in a dictionary, to include anniversary dates, etc.)
- Be changed frequently (at least every 90 days).
- Contain a minimum of 8 characters in length.
- Contain a mix of characters from at least three (3) of the following (4) categories:
 - English uppercase letters A,B,C,.....Z.
 - English lowercase letters a,b,c,.....z.
 - Westernized Arabic numerals 0,1,2,....9.
 - Non-alphanumeric (“special characters”) %, @, # such as punctuation symbols.
- Be changed immediately if you suspect it has been compromised.

Your password SHOULD NOT.....

- Have the same character/alphanumeric appear more than once.
- Contain the username or any part of the full name.

- Be shared with anyone.
- Be written down, posted on a “yellow stickie” stuck to your monitor or computer, documented on your calendar, stored in your wallet or purse, etc.
- Be stored on a programmable key.
- Do Not check the memorize password feature on your system, which would eliminate the necessity to respond to a password prompt with other than pressing the RETURN key.

Users

- Users are personnel authorized and able to access department IT assets. They include operators, administrators, and system/network maintenance personnel.
- All users are expected to understand and comply with this policy document and its requirements.
- Questions about the policy should be directed to the appropriate CSO or the DCIO/IA.

All users will report security problems or incidents to their respective SSOs or other appropriate security official as soon as practical. Violations of security policies may lead to revocation of system access or disciplinary action up to and including termination.

Other Policies and Procedures

The Rules of Behavior are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing the COD system. The rules are consistent with the policy and procedures described, but not limited to, the following directives:

- Freedom of Information Act.
- Privacy Act.
- Computer Security Act.
- Government Information Security Reform Act (GISRA).
- OMB publications.

- National Institute of Standards and Technology (NIST) publications.
- Network security manuals/procedures.
- System security manuals/procedures.
- Personnel security manuals/procedures.
- Software security manuals/procedures.
- Department of Education publications.

These responsibilities will be reinforced through scheduled security awareness training.

I acknowledge receipt of, understand my responsibilities, and will comply with the “Rules of Behavior” for the COD System. I understand that failure to abide by the above rules and responsibilities may lead to disciplinary action up to and including dismissal. I further understand that violation of these rules and responsibilities may be prosecutable under local, State, and/or Federal law.

Print Name: _____

Signature: _____

Date: _____