

Department of Education  
Federal Student Aid (FSA)  
Financial Partners Data Mart (FPDM)  
Rules of Behavior

**“Rules of Behavior”**

**1. 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.

The Financial Partners Data Mart (FPDM) 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, and Trading Partners) of the FPDM and their host applications.

The rules delineate responsibilities and expectations for all individuals supporting the FPDM. 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.

**2. 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 is not hidden in minutia and therefore not properly secured/protected when not in use because it is not visible.

**3. 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.

Department of Education  
Federal Student Aid (FSA)  
Financial Partners Data Mart (FPDM)  
Rules of Behavior

- 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.

**4. Computer System Responsibilities**

- Do not make copies of system configuration files (that is, /etc/password) 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 FPDM 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 FPDM.
- 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 which 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.

**5. Unofficial use of Government Equipment**

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

Department of Education  
Federal Student Aid (FSA)  
Financial Partners Data Mart (FPDM)  
Rules of Behavior

- 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.
- 6. Work at Home**
- FPDM Personnel Policy Directive authorizes Division Directors to designate specific employees (e.g., critical job series, employees on maternity leave, and employees with certain medical conditions) as eligible for working at home.
  - Any work-at-home arrangement should:
    - Be confirmed in 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.
- 7. Dial-in Access**
- The Chief Information Officer (CIO) may authorize dial-in access to FPDM. 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 FPDM phone records, and conduct spot-checks to determine if FPDM 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 FPDM resides, the managers of those applications should also determine if such access could pose a risk to FPDM data.
  - Do not divulge dial-up modem phone numbers to anyone. If an employee needs dial-up access, refer him or her to the Local Area Network (LAN) team.
- 8. 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 Internet Service Provider (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.

Department of Education  
Federal Student Aid (FSA)  
Financial Partners Data Mart (FPDM)  
Rules of Behavior

**9. 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.

**10. 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 FPDM personnel must be understood and complied with.

**11. User IDs**

- Do not share user identification (IDs) or system accounts with any individual.
- At any time when leaving a session unattended, always 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.

**12. 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 alphabetic and numeric characters (1 special character, 4/5 alphabet, 3/2 numeric).
- Contain at least three of the four criteria: upper case, lower case, number, or special character.
- Be changed immediately if you suspect it has been compromised.

Report all violations of the "Rules of Behavior" to the SSO.

Page 4 of 7 Pages

Updated: 05/26/11

Department of Education  
Federal Student Aid (FSA)  
Financial Partners Data Mart (FPDM)  
Rules of Behavior

Your password SHOULD NOT.....

- Have the same character/alphanumeric appear more than once.
- Be shared with anyone.
- Be written down, posted on a "post it note" 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.

### 13. 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.***

### 14. 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 FPDM. The rules are consistent with the policy and procedures described, but not limited to, the following directives:

As an employee or contractor, you are required to be aware of and abide by laws and regulations that apply to the unauthorized use of files, records, and data. Below are brief descriptions of your obligations under some of these laws and regulations.

- The [Computer Abuse and Fraud Act of 1986](http://www.panix.com/~eck/computer-fraud-act.html) <<http://www.panix.com/~eck/computer-fraud-act.html>> indicates that you shall not knowingly, and with intent to defraud, access a protected computer without authorization or beyond your authorization level.
- The [Privacy Act of 1974](http://www.usdoj.gov/foia/privstat.htm) <<http://www.usdoj.gov/foia/privstat.htm>> indicates that any U.S. citizen or alien lawfully admitted for permanent U.S. residence can request information about themselves.
- The [Freedom of Information Act of 1966](http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) <[http://www.usdoj.gov/oip/foia\\_updates/Vol\\_XVII\\_4/page2.htm](http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm)> indicates that all Government agencies are required to disclose records upon receiving a written request for them, except for those records that are protected from disclosure by the [Freedom of Information Act](http://www.ed.gov/offices/OCIO/foia/whats_is_foia.html) [http://www.ed.gov/offices/OCIO/foia/whats\\_is\\_foia.html](http://www.ed.gov/offices/OCIO/foia/whats_is_foia.html) (Exemptions) .
- The [ED Personal Use of Department Equipment Policy](#) indicates that you may not, while using Government equipment, engage in any activity that is illegal or otherwise expressly prohibited (e.g. political activity or lobbying activity prohibited by law). You are, however, permitted occasional

Report all violations of the "Rules of Behavior" to the SSO.

Page 5 of 7 Pages

Updated: 05/26/11

Department of Education  
Federal Student Aid (FSA)  
Financial Partners Data Mart (FPDM)  
Rules of Behavior

personal use provided that such use incurs only a negligible additional expense to the Department, does not impede your ability to do your job, does not impede other employees' ability to do their jobs, occurs during off-duty hours whenever possible and is not for the purpose of generating income for yourself or any other employee.

- The divulging of information should be handled according to the standards set forth in the Freedom of Information Act of 1966 and the Privacy Act of 1974.
- The integrity of information must be maintained. Therefore, information in any form shall be appropriately protected. You must not maliciously destroy data.
- Be aware that all computer resources used and accessed by Financial Partners Data Mart (FPDM) users are subject to periodic test, review and audit.

These responsibilities will be reinforced through scheduled security awareness training.

All violations of the Rules of Behavior should be reported to the FPDM System Security Officer (SSO).

Department of Education  
Federal Student Aid (FSA)  
Financial Partners Data Mart (FPDM)  
Rules of Behavior

I acknowledge receipt of, understand my responsibilities, and will comply with the "Rules of Behavior" for the Financial Partners Data Mart. 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.

Employee:

Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Company/Employer: \_\_\_\_\_

Site Location: \_\_\_\_\_

Date: \_\_\_\_\_

FPDM System Security Officer (SSO):

Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Report all violations of the "Rules of Behavior" to the SSO.  
Page 7 of 7 Pages