



## DMIS/TROR Rules of Behavior

### Introduction

FMS relies increasingly on applications residing on IT systems to accomplish its mission. As IT system processing becomes more important, the requirements to safeguard FMS equipment, software and data also take on greater significance. This Rules of Behavior procedure was developed as a guide to ensure that external users of FMS IT systems are made aware of their security responsibilities before accessing FMS applications. The Rules of Behavior define responsibilities and procedures for secure use of FMS IT systems. By reading and acknowledging these rules, users accept the responsibility to protect FMS IT systems and data. Users are accountable for their actions and the requirements to protect FMS data and equipment from both malicious and accidental loss or damage.

The following Rules of Behavior are to be followed by all users of the FMS Debt Management Information System/Treasury Report on Receivables (DMIS/TROR). These rules clearly delineate the responsibilities of and expectations for all individuals with access to the application. Non-compliance with these rules will be enforced through sanctions commensurate with the level of infraction.

### 1. Responsibilities

All authorized users who have access to DMIS/TROR shall read, acknowledge understanding, and sign the Rules of Behavior before accessing the application and associated data.

By agreeing to and signing these rules, the user signifies:

- Understanding of the DMIS/TROR security requirements
- Acceptance of the FMS Applications security requirements
- Acknowledgement that disciplinary action may be taken based on violation of the Rules of Behavior

Federal Program Agency (FPA) Management shall verify that the users who require access to the DMIS/TROR systems have read and accepted (via signature on the acceptance form) these Rules of Behavior.

### 2. Other Policies and Procedures

These Rules of Behavior are based on the Financial Management Service Information Technology Rules of Behavior for External Users of FMS Systems, dated March 16, 2006. They are intended to enhance and further define the specific rules each user must follow while accessing the DMIS/TROR system. The rules are consistent with the policy and procedures described in the following directives:

- OMB Circular A-130, Management of Federal Information Resources, Appendix III – Security of Federal Automated Information Resources (Revised 2000)
- Privacy Act of 1974, as amended, 5 U.S.C. § 552a

- Public Law 107-347, E-Government Act of 2002, Title III – Federal Information Security Management Act of 2002 (FISMA)
- NIST Special Publication 800-18 - Revision 1, Guide for Developing Security Plans for Information Technology Systems, February 2006
- Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635
- Employee Responsibilities and Conduct, 5 CFR Part 735
- Supplemental Standards of Ethical Conduct for Employees of the Department of the Treasury, 5 CFR Part 3101
- Department of the Treasury Employee Rules of Conduct, 31 CFR Part 0
- Treasury Directive 87-04, Personal Use of Government Office Equipment Including Information Technology
- Appendix A to Treasury Directive 87-04
- Treasury Department Publication (TD P) 85-01, Treasury IT Security Program, 2003.

### **3. Application Rules**

The following Rules of Behavior are the minimum rules for external users who are requesting an FMS user account:

1. You must conduct only authorized business on the system.
2. Your level of access to the FMS system is limited to ensure your access is no more than necessary to perform your legitimate tasks or assigned duties. If you believe you are being granted access that you should not have, you must immediately notify the DMIS/TROR Administrator (202-874-8933) or the FMS Help Desk (202-874-4357).
3. You must maintain the confidentiality of your authentication credentials such as your password. Do not reveal your authentication credentials to anyone; an FMS employee should never ask you to reveal them.
4. You must follow proper logon/logoff procedures. You must manually logon to your session; do not store your password locally on your system or utilize any automated logon capabilities. You must promptly logoff when session access is no longer needed. If a logoff function is unavailable, you must close your browser. Never leave your computer unattended while logged into the system.
5. You must report all security incidents or suspected incidents (e.g., lost passwords, improper or suspicious acts) related to the FMS system to the DMIS/TROR Administrator (202-874-8933) or the FMS Help Desk (202-874-4357).
6. You must not establish any unauthorized interfaces between FMS applications and other non-FMS systems.
7. Your access to the FMS system is governed by, and subject to, Federal law, including, but not limited to, the Privacy Act, 5 U.S.C. 552a, if the applicable FMS system maintains individual Privacy Act information. Your access to the FMS system constitutes your consent to the retrieval and disclosure of the information

- within the scope of your authorized access, subject to the Privacy Act, and applicable Federal laws.
8. You must safeguard system resources against waste, loss, abuse, unauthorized use or disclosure, and misappropriation.
  9. You must not process classified national security information on the system.
  10. You must not browse, search or reveal FMS system information except in accordance with that which is required to perform your legitimate tasks or assigned duties. You must not retrieve information, or in any other way disclose information, for someone who does not have authority to access that information.
  11. By your signature or electronic acceptance (such as by clicking an acceptance button on the screen), you must agree to these rules.
  12. You must notify the DMIS/TROR manager if access to system resources is beyond that which is required to perform your jobs.
  13. You must attend computer security awareness training held by your employing agency.
  14. You must coordinate your user access requirements and user access parameters with the DMIS/TROR manager and/or designated security officer.
  15. You must ensure that when hard copies of sensitive information are no longer required, that they are destroyed commensurate with the sensitivity of the data.
  16. You should contact your DMIS/TROR Administrator (202-874-8933) if you do not understand any of these rules.



## DMIS/TROR Rules of Behavior

### ACCEPTANCE

I have read the above DMIS/TROR System Rules of Behavior for External Users of Financial Management Service (FMS) Systems. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to the FMS system is covered by, and subject to, such Rules. Further, I acknowledge and accept that any violation by me of these Rules may subject me to civil and/or criminal actions and that FMS retains the right, at its sole discretion, to terminate, cancel or suspend my access rights to the FMS system(s) at any time, without notice.

User's Name: \_\_\_\_\_ (printed)

User's Name: \_\_\_\_\_ (signature)

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