System Rules of Behavior

For the
Flight Projects Directorate

National Aeronautics & Space Administration

Goddard Space Flight Center

Issue Date: *05-11-2007*
Effective Date: *05-11-2007*

V1.0

Verify that this is the correct version before use.

National Aeronautics and
Space Administration

THIS PAGE LEFT INTENTIONALLY BLANK

Review and approval signature

The Flight Projects Directorate Rules of Behavior were prepared for the exclusive use of the NASA Goddard Space Flight Center. I have reviewed and concur with the attached Rules of Behavior.

Approved by: _____ 5/11/07
George Morrow Date
Deputy Director of
Flight Projects Directorate

Approved by: _____ 5/11/07
George Barth Date
Deputy Director for
Planning and Business Management, Flight Projects Directorate

DOCUMENT CHANGE HISTORY

Version Number	Date	Author	Description
Ver 1.0		D. Whorton	Initial Creation from current RMS template.

Table Of Contents

Flight Projects Directorate
System Rules of Behavior

1.0 INTRODUCTION

The rules of behavior contained in this document are to be followed by all users of the FPD (Flight Projects Directorate) system. The rules clearly delineate responsibilities of and expectations for all individuals with access to the system. Users are accountable for their actions on the FPD System. If an employee violates NASA policy regarding the rules of the system, they may be subject to disciplinary action at the discretion of management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

2.0 RESPONSIBILITIES

The Center ITSM (Information Technology Security Manager) is responsible for ensuring that an adequate level of protection is afforded to the FPD System through an appropriate mix of technical, administrative, and managerial controls. The ITSM develops policies and procedures, ensures the development and presentation of user and contractor awareness sessions, and inspects and spot-checks to determine that an adequate level of compliance with security requirements exists. The ITSM is responsible for conducting periodic vulnerability analyses to determine if security controls are adequate. Special attention is given to those new and developing technologies, systems, and applications that can open or have opened vulnerabilities in the NASA's security posture.

3.0 OTHER POLICIES AND PROCEDURES

These Rules of Behavior do not supersede applicable laws, contracts, agreements, grant terms, or existing policy. Rather they are intended to enhance and further define the specific rules each user must follow while accessing FPD System. The rules are consistent with the policies and procedures described in the following directives:

NASA NPR-2810.1a. The revised directive, dated May 16, 2006, contains computer security guidance on a wide range of topics, (i.e., personnel security, incident handling, access control mechanisms.) This document contains responsibilities for the Information System Security Official (ISSO), managers, and users.

NASA NPR-2540.1F. This directive, dated May 25, 2005, contains specific guidance for all users regarding appropriate use of government equipment, including Information Technology.

NASA NPR-1600.1. This directive, dated November 03, 2004, contains responsibilities for FPD System data owners and application administrators and the security officer.

4.0 APPLICATION RULES

4.1 Monitoring of Data and Access

Use of these Information Technology (IT) resources gives consent for monitoring and security testing to enforce proper security procedures and appropriate usage of FPD IT resources. **YOU SHOULD HAVE NO EXPECTATION OF PRIVACY**. By continuing, you consent to your keystrokes and data content being monitored.

4.2 Dial-up and Remote Access

Dial-up and Remote VPN access is possible through the CNE other Network facilities, or via private Internet Service Providers (ISPs).

Only a valid user (i.e. one with an account and password) can log in to FPD System machines through a dial-up Internet service (terminal servers, CNE Annex, or ISPs). These computer accounts are authorized and granted by each Division's Government personnel.

NASA operates the remote access facilities to provide GSFC personnel with a means to connect to the Goddard network from home or while on travel. Its intent is to allow users a method of checking mail and doing other minor network related work from home or while on travel. Accounts are not transferable. Misuse by the remote access account user or usage by a person other than the authorized user may result in the user's remote access privileges being revoked.

The current policy for Dial-up is that users should not exceed 2 hours per connection, and should limit dial-up use to 4 hours a day on the local number and 2 hours a day on the 1-800 number. For more information about CNE policies and usage restrictions, see Dialup Networking - The CNE Annex. CNE policies may be modified once the GSFC Telecommuting Policy is established.

4.3 Work at Home

Users working from home shall abide by the dial-up access computer security rules of behavior. If they have government related files on their home computers, they shall make adequate backups of these files. Users must use authorized procedures for handling and storing sensitive information (including Privacy Act, Classified, or Confidential information). Employees who telecommute will follow any additional Telecommuting Computer Security Guidelines.

A user must get a property pass from the property custodian before taking home any government owned equipment. The user will use in accordance with the section 5.0 Unofficial Use of Government Equipment.

4.4 Connection to the Internet

Most FPD personnel have access to the Internet. Access to the Internet must be closely controlled by the ISSO. Divisions, staff managers, and technicians should know that only NASA-authorized Internet connections are allowed, and that all connections must conform to the NASA's security and communications architecture.

5.0 UNOFFICIAL USE OF GOVERNMENT EQUIPMENT

Occasional personal use of Project assets is permitted within the scope defined in paragraph 11.3.4, NPR 2810.1A. We have provided some FPD guidelines for this type of use. For further clarification please consult NPR 2540.1F.

a. The activity must take place during non-work time, be of reasonable duration and frequency, and must not interfere with or adversely affect the individual's performance or other organization requirements.

b. Supplies must be purchased by the individual or be of insignificant value, and the activity must not reduce the useful life expectancy of any durable asset.

c. The activity must not be in support of any: (a) personal business venture, the business of any other corporation or firm, consulting effort or similar profit venture; (b) political interests; or (c) activity involving harassing, threatening or sexually explicit materials or (d) illegal purpose or purpose that would cause embarrassment to the Project or otherwise be adverse to its interests.

d. The activity must not compromise security.

e. Assets (other than supplies of insignificant value) must remain on Project controlled property, or authorization must be obtained from cognizant management for removal of the asset.

6.0 PROTECTION OF COPYWRITE LICENSES (SOFTWARE)

FPD System and PC users are not to download FPD resident software. Audit logs are reviewed to determine whether employees attempt to access system servers on which valuable, off-the-shelf software resides, but to which users have not been granted access. Audit logs also show users' use of a "copy" command; this may indicate attempts to illegally download software. Unauthorized copying of PC-based software is also prohibited.

7.0 USE OF PASSWORDS

Users are to use passwords of a length specified by the FPD System Project SOPs, and at least – a mix of eight (8) alpha, numeric, and special characters. They are to keep passwords

confidential and are not to share passwords with anyone.

8.0 SYSTEM PRIVILEGES

Users are given access to the system based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems, data or applications to which access has not been authorized.

9.0 INDIVIDUAL ACCOUNTABILITY

Users are accountable for their actions on the FPD . This is stressed during annual computer security awareness training sessions. Failure to adhere to these rules may constitute grounds for termination of access privileges, administrative action, and/or referral of the case to the NASA Inspector General's Office for further actions.

10.0 SECURITY INCIDENT REPORTING AND HANDLING

FPD users that suspect they are experiencing an IT security incident (virus, malware, etc.) should notify their CSO (Computer Security Official (or alternate)) and ISSO (Information System Security Officer), or DCSO (Directorate Computer Security Official) if their CSO is unavailable, and follow any instructions given by the CSO, ISSO, and/or DCSO regarding the affected system.

Until further guidance from one of the listed responsible officials, do not allow anyone to manipulate the system in any way, unless there is some safety issue or the system presents and serious risk of damage to other NASA assets or information. To assist in the protection of the system, a NASA official evidence poster should be placed on the system. Once an evidence poster has been placed on an affected system, Users and System Administrators shall not modify the state of the system in any way, including powering the system down, removing network or power cables, removing external storage, stopping programs, starting programs, examining system logs, etc. Performing actions which modify the system state can destroy data needed for a successful investigation or prosecution. Failure to comply with the instructions on the evidence poster can result in criminal charges.

11.0 ACKNOWLEDGEMENT

I acknowledge receipt of these Rules of Behavior; I understand my responsibilities under the Rules of Behavior for the NASA FPD System.

_____ _____

Signature of User Date