

# **System Rules of Behavior**

**National Aeronautics & Space Administration**

**Goddard Space Flight Center**

## **System Rules of Behavior for the Management Operations Directorate (MOD) Computer Systems**

Issue Date: *07-11-08 (original)*

Effective Date: *08-01-08 (original)*

Verify that this is the correct version before use.



National Aeronautics and  
Space Administration



## DOCUMENT CHANGE HISTORY

<b>Version Number</b>	<b>Date</b>	<b>Author</b>	<b>Description</b>
1	10 July 2008	Kim Wiggins / Robert Peirce	Initial Draft

## TABLE OF CONTENTS

<b>1.0</b>	<b>INTRODUCTION .....</b>	<b>5</b>
<b>2.0</b>	<b>RESPONSIBILITIES .....</b>	<b>6</b>
<b>3.0</b>	<b>OTHER POLICIES AND PROCEDURES .....</b>	<b>13</b>
<b>4.0</b>	<b>APPLICATION RULES .....</b>	<b>14</b>
<b>5.0</b>	<b>LETTER FOR EXTERNAL (NON-NASA USERS) .....</b>	<b>16</b>
<b>6.0</b>	<b>APPENDICES .....</b>	<b>17</b>
	<b>Appendix A: Rules of Behavior Certification .....</b>	<b>17</b>

# MOD Computer User Rules of Behavior

## 1.0 INTRODUCTION

The rules of behavior contained in this document are to be followed by all users of the Management Operations Directorate (MOD) Computing Systems. All civil servant and contract employees who access any MOD system shall follow these rules. The rules clearly delineate responsibilities of and expectations for all individuals with access to the system. Users are held accountable for their actions on the MOD 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.

### **Purpose**

The purpose of these rules is to increase individual awareness and responsibility, and, to ensure that all users are utilizing Agency, Center, and/or Directorate Information Technology (IT) resources in an efficient, ethical, and lawful manner.

### **Scope**

These rules apply to all MOD civil servant and contract employees who access any NASA GSFC system. These rules shall be considered an addendum to the annual SATERN IT Security training module and are intended to provide additional guidance and policy for MOD employees. The user is requested to sign the signature page, Appendix A, to acknowledge he/she has read and understands the MOD Rules of Behavior.

### **Authority**

NPR 2810.1A, NASA Procedural Requirements, Security of Information Technology  
NPD 2540.1F NASA Policy Directive, Personal Use of Government Office Equipment  
Including Information Technology

GPR 2810.2, Goddard Procedural Requirements, Wireless Networks and Access Points

<http://cio.gsfc.nasa.gov>

<http://cne.gsfc.nasa.gov>

[http://ohcm.gsfc.nasa.gov/employee\\_relations/disciplinarytable.htm](http://ohcm.gsfc.nasa.gov/employee_relations/disciplinarytable.htm)

<http://code200.gsfc.nasa.gov>

### **Authorized Use of Government Equipment**

Government IT resources (e.g., computer equipment, networks, etc.) and electronic communication facilities (such as e-mail) are for authorized Government use only.

*See related requirements in NPR 2810.1, Chapter 4 (<http://nodis3.gsfc.nasa.gov>)*

- Authorized Use of Computers and Computing Resources

- Authorized Use of the Internet, the World Wide Web (WWW) and Related Internet Services

By virtue of the fact that these are government computers for official government use, users consent to monitoring and security testing to ensure proper security procedures and appropriate usage are being observed for Center IT resources.

## **2.0 RESPONSIBILITIES**

The System Owner of MOD Management is responsible for ensuring that an adequate level of protection is afforded to the MOD System through an appropriate mix of technical, administrative, and managerial controls. The System Owner of MOD Management 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 System Owner of MOD Management 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.

### **Requirements for the Use of Government Equipment**

It is important that each civil servant and contractor employee understand IT security responsibilities and demonstrate skills needed to carry them out. Therefore, each user of IT equipment is required to complete annual Basic IT Security training, as well as any additional IT Security Training commensurate with their responsibilities, via SATERN (<https://satern.msfc.nasa.gov>) and provide a copy of the completion certificate(s) to the appropriate personnel (e.g. Branch, Division, office management, etc.) within the organization.

Prior to user accounts being assigned and issued, the individual shall (1) Take the SATERN-based Basic IT Security Awareness training modules; (2) Read and accept the Information Technology Security User Responsibilities information located on the CNE web site <http://cne/forms/InformationTechSecurityUserResponsibilities.pdf> ; (3) Download and complete Email and Active Directory Account Request form found at [http://cne.gsfc.nasa.gov/forms/email\\_domain\\_acct.html](http://cne.gsfc.nasa.gov/forms/email_domain_acct.html); and (3) Submit the form to the CNE. The user's management or management designee shall cosign this form. Computer Security Officials (CSO) shall retain a physical file of the CNE form and the Rules of Behavior Certification.

### **Physical Security**

Users must lock their office and/or laboratories when they leave for the day. If an office or laboratory is opened in the absence of the primary occupant, it is the responsibility of the person who opened the office/laboratory to ensure that the office/laboratory is locked when they have completed the task that required them to access the office/laboratory.

Special attention should be paid to laptop computers and other handheld IT devices. These IT resources should not be left in open view or open areas when the assigned user is not around. The Travel Office issues advisories concerning the extra care users need to take in protecting these IT resources from being stolen when traveling.

Users have a right to and should ask for a badge or other identification for unknown personnel in their work areas.

A user will obtain a property pass from the property custodian before taking any government or ODIN-owned equipment off site. The user will use this equipment for government-related business only.

### **Access Control**

Unless required as part of his/her normal duties, if the user leaves his/her work area for more than 15 minutes, he/she shall log off his/her computer, lock the computer, or activate a screen saver with password protection that will prevent unauthorized use of his/her computer. The user's office door must be locked after hours.

It is required users shut down their computers at the end of the workday, unless directed otherwise (i.e., data backup or other reasons) by their System Administrator (SysAdmin). If the user has other reasons to leave his/her computer on, he/she must notify the CSO or disconnect his/her computer from the network. If a user leaves his/her computer up and on the network overnight and on weekends, the risk of hacker attacks significantly increases.

### **Foreign National Access**

Foreign nationals requesting access to NASA IT resources are required to undergo personnel screening. (A foreign national is defined as anyone who is not a citizen of the United States.) Only foreign nationals covered under a NASA International Agreement shall be granted "privileged" or "limited privileged" access to NASA computer systems. The Center Chief Information Officer (CIO) must approve a waiver of this requirement. A user must contact his/her CSO for additional information regarding IT access requirements for foreign nationals.

### **Password Management**

Users are responsible for any and all activity generated through the use of their user IDs and passwords. IT resources, which use passwords for user authentication, will meet the password standards defined in NPR 2810.1A, (i.e., minimum of 8 characters; at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, and special characters). Users are to keep all passwords confidential and are not to share passwords with anyone.

Each individual will be held accountable for:

- Providing protection against loss or disclosure of passwords in his/her possession.
- All activity that occurs as a result of deliberately revealing his/her user ID

and password.

### **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 or applications to which access has not been authorized. At all times the guiding principal will be the authorization for the user of least privilege needed to perform the user's assigned tasks.

### **Individual Accountability**

Users are held accountable for their actions on any and all MOD systems. This is stressed during annual computer security awareness training sessions.

### **Account Management**

Users shall only use accounts for which they are authorized. Users shall not divulge account access procedures to any unauthorized user. Secure passwords are required on all user accounts.

Specific protection of user-owned files and file sharing are controlled by the file ownership and permissions set by the user. The user should check with his/her SysAdmin if he/she doesn't know how to do this.

A user is responsible for protecting and maintaining any information used or stored on his/her accounts, on his/her local machine, and on the MOD servers. If a user determines that he/she is unable to protect and maintain data integrity, the user must proactively seek assistance from his/her SysAdmin, CSO, or manager. This includes, but is not limited to, making sure that information/software is not lost, modified by or released to unauthorized persons.

A user shall not attempt to access any data or programs contained on systems for which he/she is not authorized nor has explicit consent of the data/program owner. When a user no longer requires access to these IT resources, or leaves or transfers out of the organization, he/she must promptly notify the responsible parties and make no further attempt to access these resources. All access authorizations (e.g., reissuing keys, identification cards, building passes; closing old accounts; establishing new accounts; and changing system access authorizations) shall be the responsibility of the organizations.

### **Anti-virus Software**

Desktop computer users are required to have anti-virus software on their machines. Users are required to ensure that anti-virus software is installed and running on their computers. GSFC has a site license for anti-virus software for PCs and Macs; it is available for download from the CNE website at [http://cne.gsfc.nasa.gov/application/cne\\_sppt\\_sw/](http://cne.gsfc.nasa.gov/application/cne_sppt_sw/). The MOD SysAdmins will help users with any questions concerning the procedure to download the current version of the software and the virus signature data file. The virus signature file is updated on the server weekly or whenever special alerts are issued. Users are responsible for keeping the virus signature file on their workstations current.

### **Patch Management and Other Remote Management Software**

NASA policy requires the use of patch management software (i.e. Patchlink®) on networked computers. This software is installed and configured to manage security patches. Under no circumstances should it be disabled or removed by a systems user. GSFC, Directorate, and Division management may elect to use other patch management tools (Microsoft Active Directory, etc.) to manage IT resources within their organization. Users attempting to bypass or disable these remote management tools may have their network access blocked.

### **Remote Management Software**

NASA does not prohibit the use of remote management software applications (i.e., PC Anywhere, Remote Anywhere, Timbuktu, etc) on network computers. However, the use of these types of tools requires FIPS-compliant encryption. Any user using these tools without encryption may have their network access blocked.

### **Backup Procedures**

Backing up the local disks of workstations and personal computers is the responsibility of the user, with assistance from the SysAdmin. Backing up refers primarily to active data and document files and does not apply to applications, which should be available via the media upon which they were originally distributed. A user should work with the SysAdmin of his/her organization to identify the back-up procedures used and the method(s) that works best for the user in his/her situation and circumstances.

*NOTE - In the case of ODIN supported seats, back-up services may be purchased and all configuration/scheduling issues worked with the service provider.*

### **Restoration of Service**

The availability of the MOD systems is a concern to all users. All users are responsible for ensuring their systems are backed up on a regular basis. In the event the system is non-operational, the user will ensure restoration of service, with the assistance of the SysAdmin or service provider.

### **Disposal of IT Resources**

Sensitive information (including copyrighted software, personnel information, and proprietary scientific data) is to be removed from hardware devices prior to being put in excess, or prior to transferring ownership of those devices unless the information/software is specifically included in the transfer. Users are to notify their property manager, SysAdmin, and CSO before any IT resource is put in excess, moved, or reassigned to another employee.

### **Reporting of IT Security Incidents**

Users are required to report all observed compromises of IT security (viruses, unauthorized access, theft, inappropriate use, etc.) to the SysAdmin and/or the CSO. Users should call or visit the SysAdmin or CSO to report an incident; they should **NOT** email. If a SysAdmin or CSO is not available, the user shall inform his/her manager. The

CSO will get clearance from the Center Information Technology Security Manager (C-ITSM) before taking any action and may power the machine off if the situation warrants.

In some circumstances, compromised systems may be tagged with a crime scene or 'Do Not Touch' Notice. Under no circumstances should a user disregard or bypass any of these notices.

### **Handling of Sensitive but Unclassified (SBU) Information**

In accordance with NPR 1600.1, ensure that all administratively controlled information ACI/SBU (Administratively Controlled Information/Sensitive But Unclassified) information relating to the NASA mission includes “For Official Use Only”, SEB, Privacy Act, Procurement Sensitive or proprietary information shall be encrypted. Sensitive information and licensed software are the responsibility of the user/owner. Prior to a system being sent out for maintenance, discretion should be used with regards to removing sensitive data. Paper copies of sensitive information are to be shredded and sensitive information on hard drives of computers to be erased. CDs, USB memory sticks, DVDs, etc., with sensitive information are to be stored in locked containers when not in use or when you leave your work area. CDs, DVDs, or documents containing sensitive information should be clearly labeled as such with NASA form 1686-SBU cover sheet on canary yellow paper.

### **Web Server Security Guidelines**

MOD utilizes the services of Code 700 to publish web content for organizations and projects. MOD personnel shall not have personal or other special purpose Web pages without the authorization of their management.

Web services shall not be hosted from end user desktops.

### **File Transfer Protocol (FTP) Servers**

FTP servers shall not be hosted from end user desktops. FTP is not an appropriate means of transferring sensitive data such as ITAR/EAR. A user should contact the local SysAdmin for help in performing these activities in a secure manner on an organizational server using SSH services.

### **Use of Government IT Resources for Personal Use**

Per requirements in the NASA Policy Directive (NPD) 2540.1F, permission is granted to civil servant and contract personnel for the following uses of government IT resources.

Because there is no measurable cost, some *limited* personal use of Internet services, such as the World Wide Web and electronic mail, is permitted provided it does not interfere with the employee's work or the work of others.

When communication shall not reasonably be made during non-business hours, employees may exchange brief messages with such persons or entities as the following:

- a. Spouse or dependent.
- b. Someone responsible for the care of a spouse or dependent.
- c. State and local government agencies on personal matters.
- d. Medical and dental care providers.
- e. The appropriate responder persons in emergency situations.
- f. Instant Messaging (IM) and/or Chatting  
Please visit <http://code700.gsfc.nasa.gov/policy/> Instant Messaging Announcement 07-11-i) Use of Instant Messaging (IM)-ii) List of approved solutions, where i) is the actual announcement 01-11, and ii) is the list of approved instant messengers.

Extreme care must be taken regarding content matter. Under no circumstances is it permissible to access or download material that would create a hostile or offensive work environment, such as racist or sexually explicit material. Use must be kept to brief periods when it can reasonably be assumed that the employee is in a non-duty status, such as during lunch breaks.

It is imperative that common sense is used to ensure that these privileges are not misused and an incident does not lead to an IG seizure or a General Accounting Office (GAO) investigation into the utilization of government resources for inappropriate behavior. If a user has any doubt regarding any uses he/she should contact his/her immediate supervisor or CSO to obtain clarification on the use in question. This reduces the probability of error later.

The following activities are NOT permitted from a government owned computer network:

- Non-work related Internet Chat Rooms, News Groups, or similar activities.
- Peer-to-Peer (P2P) file sharing.
- Creating, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.
- Installing and using computer games of any type (Internet-based, and/or local).
- The installation of unauthorized software.
- Maintaining or conducting an outside business.
- Monitoring network traffic (e.g. run a sniffer) to access IT resources; or copy data, files, or software without authorization.
- Advertising goods or services for sale for monetary or personal gain
- Sending chain letters, personal mass mailings, hoaxes, or harassing messages

**Use of the Internet, the World Wide Web (WWW), and Related Internet Services**

Employees are prohibited from browsing or viewing Internet sites that contain obscene,

hateful, or otherwise objectionable and/or offensive materials, which is strictly prohibited on Agency, Center, resources (i.e., computers, networks, [to include dial-in via an access account]).

Employees are also prohibited from sending or receiving any material that is obscene or defamatory or which is intended to annoy, harass, or intimidate any person, co-worker, supervisor, or others. Unsolicited materials received should be forwarded to [abuse@abuse.gsfc.nasa.gov](mailto:abuse@abuse.gsfc.nasa.gov) for Center disposition.

Employees shall not represent personal opinions as those of the Agency, Center, or Directorate via chat rooms, newsgroups, or Internet email messages.

Employees' government email address shall not be published in bulletin board systems (BBS), mail lists, trade journals, etc., for non-NASA or non-government purposes with the exception of those non-work related activities that are endorsed by NASA and/or GSFC and support the NASA quality of life (e.g., GEWA).

Unauthorized disclosure of Agency, Center, or Directorate trade secrets, confidential information, or privileged communications is prohibited.

Use of the Internet for gambling, whether supports betting, casino betting, or otherwise, is prohibited.

Unauthorized copying and distribution of copyrighted materials (i.e., software, music files, movies, etc.) is prohibited.

Before downloading any software or electronic files, employees must implement Agency-approved virus protection software.

### **File Sharing Applications**

File sharing and P2P applications such as KaZaA, Morpheus, DC++, Bit Torrent, Grokster, Gnutella and other similar applications shall not be used on GSFC networks. These applications are primarily intended to share files that may contain copyrighted, obscene, hateful, objectionable materials. When in use, these applications pose a resource and security threat to the network. Only approved methods and protocols for file sharing and collaborative activities may be used. File sharing is prohibited on Windows, Mac, or other operating systems..

### **Consequences of Behavior Inconsistent with the Rules**

Behaviors inconsistent with these rules are handled by the SysAdmin, CSO, or by MOD and/or Center management, as appropriate and dependent upon the gravity of the situation. Examples of consequences include but are not limited to the following:

- A machine or system using an invalid IP address may be disconnected from the network
- A network segment with a serious computer security incident may be

- disconnected at the building router level.
- Ethics violations may result in personnel action being taken.

A user may have restricted access to resources if warranted. Failure to abide by Agency, Center, Directorate, Division or specific organizational policies shall constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

The Office of Human Resources provides a guide to use when determining whether and/or to what extent formal disciplinary action is necessary in dealing with issues of employee misconduct. Please visit

[http://ohr.gsfc.nasa.gov/employee\\_relations/disciplinarytable.htm](http://ohr.gsfc.nasa.gov/employee_relations/disciplinarytable.htm)

for additional information.

### **3.0 OTHER POLICIES AND PROCEDURES**

This document is not to be used in place of existing policy, rather it is intended to enhance and further define the specific rules each user must follow while accessing MOD systems. The rules are consistent with the policies and procedures described in the following directives:

NASA Procedural Requirements (NPR) 2810.1A, Security of Information Technology 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 also contains responsibilities for the MOD Security Officials, managers, and users.

A new separate NASA Access Control Management Directive does not yet exist. But NASA Procedural Requirements (NPR) 2810.1A, Security of Information Technology earlier directive, dated May 16, 2006, contains responsibilities for MOD system data owners and application administrators and the security officer.

#### **IT Security Support**

##### ***Computer Security Officials (CSOs)***

See the list of IT Security Officials for MOD at:

<http://code700.gsfc.nasa.gov/Security/Contact.html>.

#### **Desktop Support**

(i.e., application errors, computer configuration inquiries, virus scans, etc.)

ODIN Supported Seats – users should submit an ODIN ticket (x63100)

Non-ODIN Supported Systems – users should contact local SysAdmin

A user **should not** ask the local SysAdmin to perform any system administration tasks on ODIN supported machines. The local SysAdmin is NOT the system administrator for

ODIN seats and NASA risks a **high** return-to-service fee if ODIN 'asserts' that damage to the user's system was caused by the local SysAdmin.

## **4.0 APPLICATION RULES**

### **Work At Home**

NASA NPR 3800.1 (Employee Benefits chapter 7 "Operation of NASA Telework Programs"), dated May 16, 2005, states the telework program provides workplace options for employees to facilitate work/family needs and commuting requirements. It is primarily a management option rather than an employee benefit and does not change the terms and conditions of appointment. Telework positions must include duties suitable to being performed away from the official duty station. Participation is voluntary and requires management approval. Accordingly, there is no employee entitlement to participate in teleworking. Any work-at-home arrangement should:

Be in writing.

Identify the time period for which the work at home is allowed.

Identify what government scanned equipment and supplies are needed by the employee at home, and how the equipment and supplies are to be transferred and accounted for.

Use of government computer for government business only, not personal use.

Use of PKI is required for SBU data.

Be reviewed by the NASA personnel office prior to commencement.

### **Remote Access**

Remote Access to the GSFC network from home or while on travel is available through the CNE Dial-up or Virtual Private Network (VPN) services. Users working from home shall abide by CNE IT User Responsibilities (<http://cne.gsfc.nasa.gov>). If the users 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/Confidential Information, ITAR, etc.) Employees who participate in the GSFC Teleworking Program shall follow the requirements specified for telecommuters (<http://ohcm.gsfc.nasa.gov/>). It is suggested that government-related data not be put on home computers. A user is required to check all files created at home for viruses before copying these files to their onsite workstation. Remote accounts are not transferable. Misuse of a remote access account by the authorized user or allowing any other person to access the account shall result in the user's remote access privileges being revoked.

Only a valid user (i.e., one with an account and password) can log into MOD machines through the CNE. These computer accounts are authorized and granted by a SysAdmin within the MOD divisions with concurrence from the CSO and line management.

### **Dial-In Access of non-Server Systems**

Users working from home shall abide by the rules for remote access noted above

(<http://cne.gsfc.nasa.gov>). There are no restrictions on when the user can access a GSFC system on government owned or personally owned computers.

The current policy is that users should not exceed 2 hours per connection, up to 4 hours a day on the local number, and 2 hours a day on the toll-free number. For more information about CNE policies and usage restrictions, see <http://cne.gsfc.nasa.gov>.

#### **VPN Access**

MOD highly encourages that VPN accounts can only be used to connect from a government owned computer. User's home computer systems are subject to adhere to the same Center's system requirements when connecting to the Center's internal network (CNE): fully patched and up to date operating system with a current and updated anti-virus program installed.

#### **Wireless Access**

Devices such as laptops equipped with a wireless Ethernet card, wireless Personal Digital Assistants, and Internet capable cell phones shall be treated the same as remote user access requirements noted above (see GPR 2810.2, Wireless Networks and Access Points).

The current policy has no time limit restrictions.

#### **Access of Server Systems**

No dial-in access is used to access any MOD system servers. However, if a justifiable need occurs, the CSO may authorize dial-in access to an MOD system server. It is understood that dial-in access would pose additional security risks, but may become necessary for certain job functions. If dial-in access is allowed, the CSO and the MOD DCSO must regularly review telecommunications logs and NASA phone records, and conduct spot-checks to determine if business functions are complying with controls placed on the use of dial-in lines.

#### **Connection to the Local Area Network (LAN)**

Every system connected to a GSFC LAN (either directly or via a wireless access point) is required to have a designated SysAdmin. The SysAdmins must have "administrator" or "root" level access to all systems for which they are responsible. Blocking or disabling SysAdmin access will result in the revocation of user privilege. For new users and/or computers, the appropriate SysAdmin will configure the computer with the required software security settings for network connectivity. Systems being connected to the GSFC LAN must undergo a security scan prior to their being assigned a network address. At the time of initial configuration, the SysAdmin will work with the CSO to obtain and properly register an Internet Protocol (IP) address from the Center Network Environment (CNE) for the GSFC and any applicable domains (i.e., EngNet). The user cannot do this. Any changes to or deletions of IP addresses will be coordinated through the CSO. Users shall not transfer an assigned IP address to another system.

Network access to a system may be blocked for security reasons, and under no

circumstances should the user change the network settings/address in an attempt to circumvent the block.

Personally owned computers are not to be connected to the GSFC network (i.e., CNE or VPN) except through dial-up access. **Government resources cannot be used to maintain or administer personally owned systems. The Office of the Inspector General has the authority to confiscate any personally owned computer that is involved in an IT security incident.**

#### **Proper Use, Protection, and Storage of Copyrighted Software**

SysAdmins ensure that workstations have valid software licenses at the time of initial set up. Users are responsible for the valid licensing of software that they add to their workstation/computers. Users shall not make or use unauthorized copies of copyrighted software except as permitted by law or by the owner of the copyright.

Unauthorized copying or downloading of any MOD system-based software is prohibited.

Users are responsible for storing original diskettes or CDs for all software residing on their workstation that is not authenticated from one of the MOD servers. Software diskettes and CDs must be stored in a manner that provides reasonable protection from loss, misuse, or damage.

#### **5.0 LETTER FOR EXTERNAL (NON-NASA USERS)**

A letter for NonNASA users (which transmits the applicable NASA policies) must be provided to all non-NASA users while using any MOD systems or when using NASA systems and applications in general. These responsibilities must also be included in the training about security points of contact, and included in interagency agreements or other formal agreements or documents between NASA and other organizations.

**APPENDIX A: RULES OF BEHAVIOR CERTIFICATION**

I acknowledge receipt of these Rules of Behavior and I understand my responsibilities. As a user of the Agency, Center, and/or Directorate Information Technology (IT) resources, I have read and understood the policies and guidelines delineated in the document “MOD Computer User’s Rules of Behavior”.

Name: \_\_\_\_\_ Code: \_\_\_\_\_

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

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

Please return the signed certification to your Computer Security Official listed below:

- 200 - Kimberly Wiggins
- 200/SEB - William Brown
- 201 - Teresa Hewitt
- 210 - Mary Ann Bishop
- 220 - Patricia Bavis
- 240 - Caroline Ardolini
- 250 - Maria Hughes
- 270 - Thomas Weisz