

Copyright © SecureInfo® Corporation. All Rights Reserved. Contains proprietary and confidential information of SecureInfo® Corporation. Subject to the terms and conditions of the applicable license agreement including, but not limited to, those regarding confidentiality and use restrictions.

Rules of Behavior for the Sciences and Exploration Directorate, Code 600

As an employee or contractor of the National Aeronautics and Space administration (NASA), you are required to be aware of and comply with the NASA's policy on usage and security of computer resources in accordance with NPR 2810.1A Security of Information Technology, and NPD 2540.1F Personal Use of Government Office Equipment. Any other use may be considered misuse of Government property and place you in violation of Federal regulations. Failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action and/or civil and criminal prosecution.

Much of the policy for Federal and Agency IT can be found at the following links:

- OMB Circular A-130:
http://www.whitehouse.gov/omb/circulars_a130_a130trans4/
- NIST FIPS and SP publications:
<http://csrc.nist.gov/index.html>
- NASA Policy Directives (NPD) and NASA Procedural Requirements (NPR); NASA Interim Directives (NID); NASA Interim Technical Requirements (NITR); and IT Security Handbooks (ITS-HBK):
<http://www.nasa.gov/offices/ocio/itsecurity/index.html>

The rules 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 SED MPP systems.

YOU ARE RESPONSIBLE FOR ALL ACTIONS PERFORMED WITH YOUR PERSONAL USER ID.

- UserIDs and passwords are for your **individual** use only and are considered confidential.
- **You must not disclose your password to anyone at anytime for any reason.** Furthermore, you must take necessary steps to prevent anyone from gaining knowledge of your password.
- Your UserID and password must be used solely for the performance of your official job functions, and to support NASA's operations (Refer to NPD 2540.1F "Personal Use of Government Office Equipment").
- In addition to being federal and agency policy, the SED recognizes that the principal of "least privilege" is a best practice and can **substantially reduce the number of incidents** on our computers and networks. As such, the account that you, as an end user doing your day to day work, shall be your "regular" user account. This account **shall not have Elevated Privilege (EP) associated with it** (also known as administrative or root access). Verify with your system administrator to ensure that your machine and account are configured this way.
- Due to the increased risk to NASA computers, networks and data, **the SED controls, limits access to, and tracks who has Elevated Privilege (EP) on our computer systems.** User access to **Elevated Privilege is not granted by default** and is limited based on work related need and requires justification. If Elevated Privilege is required for you to perform your work duties, you agree to abide by the process for requesting and

maintaining Elevated Privilege set forth by the Agency and/or the SED which includes, but is not limited to, proper justification and annual system administrator training in SATERN.

- If you are a non-privileged user or a user with shared elevated privileged access but whose primary role is NOT system administration or IT security, you shall not make any attempt to disable or circumvent the IT security software or settings on your computer without explicit prior approval by your organization's Computer Security Official or by the Directorate IT Security Engineer.

POLICY STANDARDS AND PROCEDURES MUST BE FOLLOWED.

- **Use of personally owned computers to physically or wirelessly connect to NASA networks and utilizing NASA IP space other than the Guest Wireless network is prohibited** by NITR 2830.1A "Networks in NASA Internet Protocol (IP) Space or NASA Physical Space". This extends to using personally owned computers to remotely connect into NASA networks using the VPN. VPN access is restricted to GFE equipment only.
- All Microsoft Windows and Apple Macintosh GFE computers are required to have the KACE patch reporting agent installed and reporting to the server; and have the Symantec Endpoint Protection(SEP) anti-virus agent installed and reporting to the server. There are KACE agent requirements for other operating systems as well; your SA or CSO will inform you of these requirements. The anti-virus requirement for linux/unix is ClamAV. You are required to ensure that your machine is compliant with these requirements. Contact your SA if it is not compliant or if you have any questions.
- You must be aware of, and abide by the "Computer Fraud and Abuse Act of 1986" (Public Law 99-474), the civil and criminal penalties of the Privacy Act, the Trade Secrets Act (18 U.S.C. S905), and other Federal Regulations applying to authorized use of NASA information, including but not limited to, files, records, and data. NASA's "SATERN" training is provided to educate you about your responsibilities under these statutes.
- Be aware that all computer resources assigned, controlled, accessed, and maintained by NASA employees and contractors are subject to periodic test, review, and audits.
- Use of all computer resources, including computers, laptops, NASA's network, communication lines, and all other resources are restricted to NASA authorized purpose. **Some limited personal use is acceptable** but only when adhering to the constraints defined by NPD 2540.1F "Personal Use of Government Office Equipment". Users are strongly encouraged to read this document as it clearly outlines what is permissible and what is not.

The following are some examples of Inappropriate Personal Use. This is not intended to be an exhaustive list.

1. Any personal use that could cause inordinate congestion, delay, or disruption of service to any Government system or component or that would violate Agency information technology security policy and procedural requirements.
2. Using the Government system as a staging ground or platform to gain unauthorized access to

other systems.

3. The creation, duplication, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of subject matter.
4. Using the Government equipment for activities that are inconsistent with Federal Standards of Conduct and Equal Opportunity regulations such as hate speech or material that ridicules others on the basis of race, religion, color, sex, disability, national origin, or sexual orientation.
5. The creation, downloading, viewing, storage, copying, or transmission of materials describing or depicting sexually explicit conduct, as defined by 18 U.S.C., § 2256, or sexually oriented materials.
6. The creation, downloading, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities otherwise prohibited.
7. Use for commercial purposes or in support of "for profit" activities or in support of other outside employment or business activity such as a personal business, assisting friends, relatives, or others in such activities (e.g., consulting for pay, sales or administration of business transactions, and sale of goods or services).
8. Engaging in a personal or private capacity in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited political activity (e.g., expressing opinions about candidates, distributing campaign literature).
9. Posting Agency or proprietary information to external newsgroups, bulletin boards, or other public forums without approval or authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee or uses at odds with NASA's mission or positions. Inappropriate use also includes participating in Chat Rooms, News Groups, or other similar activities where the posting and NASA internet address will be seen by the public. Adding a disclosure statement that the views expressed do not represent those of the Agency is not an acceptable alternative.
10. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, privacy information, copyrighted, trademarked, or material with other intellectual property rights (such as literature, music, and videos beyond fair use), proprietary data, or export controlled software or data.
11. Peer-to-peer (p2p) file sharing activities. This includes SKYPE. A waiver to use p2p is available for work related activities. Contact your CSO for information.
12. Utilizing Government office equipment to "push" non-official information to others is inappropriate.

ACCESS TO INFORMATION MUST BE CONTROLLED.

- Access ONLY the information for which you are authorized, and/or have "need-to-know/access."

- Do not leave computers logged on and unattended. You must log off, use "lock workstation" feature, or use an access control function (i.e. Screen Saver with password or lock your office when possible) during unattended periods.
- If you believe that a person, other than yourself, has used or is using your credentials (i.e. UserID and password) or has gained unauthorized access by any other means, or if you have observed any other compromise of IT security (e.g. malware, theft) involving your computer, you must report the incident immediately to your supervisor. In addition, you must report the incident immediately either to your organization's Computer Security Official (CSO), the Code 600 Directorate Computer Security Official (DCSO) or the Code 600 Directorate Computer Security Engineer (DCSE). The list of these individuals is available at http://code700.gsfc.nasa.gov/security/contact/Contact_CS0.html
- Take the necessary steps to maintain security of computer files and reports containing NASA information.
- Access to the Internet is closely controlled and monitored by the Information Technology Communications Directorate, Code 700. You must be aware that accessing the Internet is restricted to NASA authorized purpose and the network is monitored.

YOU ARE RESPONSIBLE FOR THE PROPER USE OF YOUR COMPUTER RESOURCES.

- **Only use NASA-approved software or software that can clearly be demonstrated to be necessary for your job duties, and comply with vendors software license agreements.** 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 software licensed for single-use is also prohibited.
- **The primary use of the CNE "guest wireless" is for our visitors and guests; and for personally owned devices.** However, the SED recognizes that GFE equipment such as laptops, tablets and other mobile computing devices may also need to use the "guest wireless" on occasion. **SED GFE is permitted on the "guest wireless" on an ad-hoc, occasional basis providing it meets the following criteria:**
 1. It is properly registered in IPAM/GSARS or in the supplemental asset tracking spreadsheet on VST;
 2. It is set up and configured with the appropriate CIS or FDCC benchmark settings (if applicable);
 3. It has a "gs6" compliant local host or computer name;
 4. It has a KACE agent installed and reporting (if applicable) and it has the Symantec Endpoint Protection (SEP) anti-virus client installed and reporting (if applicable).

Users are required to verify with their system administrators in advance that their GFE equipment meet these criteria if they foresee the future need for the use of the CNE "guest wireless".

- Make sure your data is stored in a location where it gets backed up, and do not store sensitive or mission-critical information on your computer without adhering to the storage and handling requirements specified in NPR 1600.1 “NASA Security Program Procedural Requirements w/Change 2 (4/01/2009), Chapter 5. Classified National Security and Sensitive but Unclassified (SBU) Information Management”.
- All NASA computer resources and the electronic information or data residing on them, including hardware, software, files, paper reports, and the information are sole property of NASA and the United States Government.

Some Common User-initiated IT Security Incidents(not an exhaustive list):

- Downloading and/or installing software for personal (non-business) use of:
 - Tool bars, (e.g. Weather Bug, eBay, etc.)
 - Tax software
 - Music down loaders (Napster)
 - Games
 - Photo/Scrapbook Sharing
 - Gambling Software
 - Coupon Software
 - Screen Savers
 - Emoticons
 - Desktop Themes
- Browsing inappropriate content such as:
 - Pornographic Material
 - Gambling Sites
 - Terrorist or other Militant Sites
- Using peer-to-peer applications/protocols without a waiver, some examples include:
 - Bit Torrent
 - Lime Wire
 - Groove
 - eDonkey
 - Napster
 - Skype (without an approved waiver)
 - Any other peer-to-peer applications
- Responding to email-borne phishing and scam attempts
- Clicking on Web pop-up links that may lead to malware-infested sites
- Downloading anti-virus/spyware software (Users should not install this, ODIN or your local systems administrator (SA) will ensure that your virus protection software is installed)

USER CERTIFICATION

Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval by my organization’s CSO. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording and I will have no expectation of privacy in my use of and content on these systems and the computer equipment. I further understand that failure to

abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

I certify that I have read the above statements, fully understand my responsibilities, and agree to comply.

Name (Print): _____

Signature: _____ Date: _____