PPS Staff Rules of Behavior

February 5, 2020

This set of rules are intended for users who are members of the PPS staff. This includes the agency standard Rules of Behavior covered during your annual SATERN security awareness training. Additional expectations and clarifications are provided in this document. While these expand on the agency rules, they are in no way intended to rescind or revoke any of them. PPS employees must have at least initiated a National Agency Check with Interview (NACi) by supplying the necessary information. Note that account processing for foreign nationals requires significant additional processing, which takes a minimum of several weeks to complete. When a user no longer requires access to a given system, PPS management should be notified so the account can be disabled; no further access should be attempted after that. If the user no longer requires access to any PPS system (typically when terminating PPS employment), they should close the "PPS Account" application in IdMax.

A quick summary of the rules is provided here:

- Complete the Basic IT Security Awareness Training before account access is granted, and annually thereafter. This training provides additional rules which users are expected to follow as well.
- Ensure your local workstation is properly secured—fully patched operating system and applications, scanned for and remediation of security vulnerabilities, and running anti-virus/spam/adware/spyware applications. (Avoid using shared, particularly public workstations.)
- When communicating to account hosts remotely, use data-encrypting protocols
- Restrict activity in the account to your approved purpose
- Report all IT security issues to appropriate channels, preferably by phone and never by unencrypted email.

Account Usage

Users must only use accounts and related resources – such as data archives - for which they are authorized and must not share their account with any other user.

NASA follows the Federal Desktop Core Configuration (FDCC) Password Policies. This requires passwords to be at least 12 characters long and have at least one uppercase letter, one lowercase letter, one digit, and one special character, to be changed at least every 60 days. You should choose passwords that are difficult to guess and which are not representative of your name, a family member's name, a name or acronym of a NASA or your organization, or a dictionary word (English or other language) even with numerals used to replace letters (though if you use a special character other than "-" you should be fine on that last requirement). Your passwords on PPS systems should be different from those on other systems, particularly from those used to access PPS systems remotely. If you write down your password, you must keep that locked away; if you store it in a file it must be encrypted.

Ensure your local workstation is properly secured—keep your operating system and applications patched and run some form of anti-virus/spam/adware/spyware application so you know your keystrokes are secure. Avoid using shared, particularly public-access workstations.

Users should be aware that all non-public access to PPS is governed by the privacy, security and notices posted at the link at the bottom of the login page. You should review this information. However, in particular you should note the following:

> For site security purposes and to ensure that this Web service remains available to all users, this Government computer system employs software programs that monitor network traffic to identify unauthorized attempts to upload or change information. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, such evidence may be provided to appropriate law enforcement officials.

Assignment and Limitation of Privileges

PPS limits access to privileged system accounts (e.g. root, administrator) on its shared hosts—primarily servers—to officially-appointed system programmers. For individually-assigned workstations, system privileges are limited to the workstation's assigned user (and the system programmers). All users with Elevated Privileges (for systems administration access) must take OS-specific training and apply through IdMax.

PPS does adhere to the federal "least privilege" policy to help reduce vulnerability to malware. As such, you should use your unprivileged account for your normal work and only switch to root/admin access when required. If required by PPS system programmers and authorized NASA security personnel, the user must provide privileged access (though not the password) to their workstation. All workstations (including laptops) should have personal firewalls enabled. Users must get special permission to open the PPS firewall to allow external access to services such as ftp, http, or ssh. These are normally reserved for computers maintained and monitored by PPS system programmers. For any change needed in privileges, contact the facility manager.

PPS recognizes other privileged accounts, access to which is limited to specifically-identified and qualified users—e.g., operations, database accounts, and certain restricted scientific data. Users with access to restricted data are expected to preserve that restriction in any copies they make of the data.

Authorized Use

Government IT resources (e.g. computer equipment, printers/copiers, networks, etc.) and electronic communication facilities (e.g. email) are for official and authorized Government use only. Users must not use Government IT resources to maintain or operate a personal business or charitable organization, advertise goods or services for sale, engage in any activity for monetary or personal gain, or perform consulting work. Users must consent to monitoring and abide by all applicable user requirements.

Users must not participate in any activity or information exchange that would violate federal law, regulation or policy. Examples of such activity or information exchange include the creation, downloading, viewing, storing, copying or transmission of material related to illegal weapons, illegal gambling, terrorist activities, child pornography, sexual harassment, hate literature, sexually explicit or sexually-oriented material, and racist literature.

Users must not download or install software onto a Government computer that is not applicable to the user's job duties. Freeware or shareware games are particularly known for containing hidden spyware that can track a user's computer use, monitor keyboard activity including typed passwords or even steal copies of sensitive electronic files.

Users are permitted some occasional personal use of government office equipment provided it does not interfere with the employee's work or the work of others. Use of government computing systems for personal use must be limited to brief periods, involve only minimal additional expense to the Government, and must not interfere with the user's job duties. When using government resources for authorized personal use, employ your best judgment and avoid browsing web sites that might have controversial aspects. Though your use of the site may well be entirely innocent, the fact that there may be some controversy associated with the site should suggest that its use may be monitored by security personnel and could trigger a security incident.

Do not use unauthorized peer-to-peer applications, such as Bit Torrent or similar downloaders. Chat room participation is limited to NASA-provided services (such as Yammer, https://www.yammer.com/nasa.gov).

Software

The PPS facility manager is the source for licensed software for PPS personnel, keeping track of the licenses, and who has a licensed copy of the software. Users are responsible and accountable for ensuring the valid licensing of any software on their workstations. Users must not make or use unauthorized copies of copyrighted software or other electronic information except as permitted by law or by the owner of the copyright. Though this is not true of **all** licensed software, some licenses do allow for concurrent copies on both a workstation and a laptop and some even allow for an additional copy on a home system. Generally, the intent is that only one copy may be in use at any given time by the licensed user (e.g., not by family members). See the copyrighted software's "End User License Agreement" (EULA) for details regarding permitted use.

PPS personnel must keep an inventory of all external software applications installed on their workstations. The PPS facility manager can ask to review this inventory. This inventory should be referred to at least monthly as a reminder to check for, download, and install software updates, and to uninstall software that is no longer needed or which is no longer being adequately maintained. (Unused and, particularly, old software could have latent vulnerabilities that might be exploited in the future.)

When downloading and installing software, keep in mind that NASA is considered a commercial organization; some otherwise free software is **not** free for NASA. Contact the facility manager to purchase necessary software. Only install software that is directly related to your job responsibilities, not software related to "acceptable personal use"—e.g., media services and players. The Internet has much of value but it also is a source of many risks. Only interact with trusted sites. Particularly, only download and install software from Internet sites with which you have a strong sense of trust.

All NASA--owned workstation and laptop computers connected to a NASA network are required to have certain security software installed, including antivirus scanning software, antispyware software, and inventory software. Users are required to keep this software current with the latest updates. Consult a PPS system programmer for proper configuration of these products.

Backups

Users must ensure that there are appropriate procedures in place to protect the integrity of their workstation information. PPS provides the Networker facility to support backups, but the user is responsible for assuring the correct data are being selected. In addition, production code should be properly committed to software repositories as required by Configuration Management procedures.

Connecting to the Network

Only Government-Furnished Equipment (GFE) may be connected to the NASA wired networks or the NASA Wireless Network. Only GFE media, such as flash drives, optical disks, and portable hard drives may be connected to GFE computers. The Guest CNE Wireless Network is distinct from the above; its primary purpose is for use of non-GFE computers and media.

Email

Users should use their NASA email address in a professional manner and remember that its use may be seen as a reflection on the agency.

Users must use caution and not open any unsolicited or suspicious email, particularly if it contains an attachment or contains active content such as HTML encoding, without first verifying its source. "When in doubt throw it out." Users must not send or forward chain letters, personal mass mailings, hoaxes, or harassing messages. PPS's primary email server is the NASA-provided NOMAD system, typically used for personally-addressed email. PPS maintains the PPS mail system for email related to operations support. Both systems perform antivirus and antispyware checking of email. Users should keep in mind that unencrypted email is fairly easily compromised and subject to disclosure; it should not be used for subjects of a sensitive nature. Even encrypted emails have plaintext subject lines that have this vulnerability.

Handling Sensitive Information

The annual security training provides detailed information on the definition and handling of sensitive information in various forms. PPS personnel are explicitly directed to adhere to these guidelines. Failing to do so can lead to disciplinary action, dismissal, or both. The PPS system collects no secure PII (personally identifiable information) in any form. If users become aware of information they suspect to be sensitive, they should alert management in order that appropriate safeguards can be applied.

Property Management

All users are typically assigned primary/exclusive use of government-owned equipment—at least a workstation and monitor. In addition, the facility manager is assigned a significant inventory of shared services equipment, including spare parts and tools. Each user is accountable for his/her equipment and must take adequate steps to safeguard it, immediately notifying the PPS Facility Manager and the GCDC property manager of any loss. Laptop and mobile device users must be particularly vigilant to keep this equipment in a locked room/cabinet when it is not in active use. This is even more an issue when this portable equipment is taken home or on travel. Since even spare parts and supplies such as printer toner have significant market value, these should be kept in restricted-access areas. Users are required to notify the GCDC property manager and facility manager of any government property that is moved between offices, assigned to another user, or excessed. Any property taken off-site requires a 20-4 form that can be obtained from the GCDC property manager.

Remote Access and Teleworking

Staff who need remote access to PPS machines are required to ssh to the hrunting server using two-factor RSA tokens. When using a non-NASA workstation, it should be one the user has confidence is being maintained with vigilance similar to NASA workstations and has a high likelihood of being free from vulnerabilities: one that is up-to-date with all critical operating system patches as well as anti-virus and anti-spyware software and updates.

The following are required of PPS staff members who wish to telecommute:

- You must have adequate work that can be effectively accomplished remotely.
- You must select at most one scheduled day per week for teleworking, Tuesdays and Wednesdays excluded. (As a rule PPS meetings will be scheduled for Tuesdays. Nevertheless, important PPS meetings have precedence over your teleworking schedule.)
- You must have a broadband high-speed Internet access connection and an adequately-performing workstation. Your telework workstation should be maintained and used with the same degree of professionalism as your at-work workstation.
- You must agree to these Rules of Behavior with respect to your telework workstation, including:
    - Patch OS, applications (particularly web browsers, anti-virus/anti-spyware)
    - Run anti-virus, anti-spyware applications
    - Perform backups of non-reproducible data
    - Protect NASA data
- You must limit personal-use activities during scheduled time in the same way you would at work. You must be as productive at home as you would be in the office.
- You must obtain permission for teleworking from both PPS and civil service/contractor management. You must sign the PPS Teleworking Agreement asserting your intention to abide by PPS's teleworking requirements.
- You must have an RSA token to log in to PPS.

NASA mandates two-factor authentication for non-public external access to PPS services, which for most is only to the hrunting bastion server (though system programmers use it elsewhere). Normally RSA (PIN and token code) authentication is used, but a failover to Linux passwords is available should the RSA authentication have an extended outage. Should that occur, staff would be notified by email.

The RSA token is acquired via the NAMS system, https://nams.nasa.gov. Click "Your NAMS Requests" and make a new request for the "Agency RSA SecurID Token." Set your sponsor to be Charles Cosner if it isn't already. Test the token by accessing https://agencytokens.nasa.gov when you first receive the token, it has been a while since your last RSA login, or you are having problems logging in.

A failed login on hrunting occasionally means the RSA servers have issued a "challenge," but usually it means you've not correctly entered your PIN followed by the token value. If you get three failures in a row, the servers will lock your account. You will get a NOMAD email noting the success or explaining the failure and, in the latter case, how to get it unlocked by contacting the NASA Enterprise Service Desk, 877-677-2123. ESD is available 24×7.

PPS has implemented the NASA-mandated automated 60-day expiration for all personal account passwords. (Those using shared group accounts are encouraged to change the password on a similar schedule.) When an account's password is within seven days of expiring, a successful login will prompt you to change the password. Be sure to update this password as required; otherwise you will be locked out of the account even using the RSA token!

Let the PPS SPers know if you have any unaddressed questions or login problems:
sysgods@mail.pps.eosdis.nasa.gov

Users often need to transfer files between home computers and work computers, but the prohibition against the use of personal flash drives and other media in government computers and vice versa has made this difficult. In addition to using email for small files and the NOMAD Large File Transfer (https://transfer.ndc.nasa.gov) for large ones, PPS users can use an scp application such as winscp. "NASA data" is supposed to be restricted to systems owned and maintained by NASA. Of course, copies of public data may be used anywhere. Other data should be treated with caution, particularly if it is in any way sensitive.

Physical Security

Users must activate their computer's screen lock or log off their computer when it is to be left unattended. Power off the computer if it is to be unused for a prolonged period. Rooms containing IT should be secured. Lock the door when the room is unoccupied. Do not prop open a door designed to automatically close. If the room (or building) is key-carded, use your keycard even if immediately following someone else who has just done so. If an unknown person is observed within their work area and, particularly, who is not displaying an appropriate badge, users are expected to either ask for proper identification or immediately contact GSFC's security office. Maintenance personnel should always sign the visitor's log when entering and exiting controlled rooms such as C101. Continuously escorted visitors (e.g., tours) need not sign.

Reporting IT Security Incidents

Users are required to report any observed compromise of IT security (viruses, unauthorized access, theft, inappropriate use, suspicious activity, etc.) involving their workstation as soon as possible but no later than within two hours of detection. The user must not continue to use the affected computer or change its operating state (e.g. log off the computer) until they have received instruction from those they contact. Users must make contact with an individual on this list. If not the first, then the second, and so on until **successful** contact is made with a person. Do not just leave a message, except to mention that you are checking with the next individual on the list. (PPS will send out periodic refreshes of this list by email, both as reminders and as personnel change.)

(1) Charles Cosner (301-614-5294), Quyen Nguyen (301-614-5070), Tony Stocker(301-614-5738), Toan Tran (301-614-5065), Marissa Ocher (301-614-5684)
(2) Erich Stocker (301-614-5178) or Yi Song (301-614-5375)
(3) Code 610.2 CSO: Gail Wade (301-614-5237)
(4) Mission Systems CSO: Terri Chow (301-614-6339)
(5) Code 600 DCSE: Mike Bur (301-614-6661), Jeff Simpson (301-286-7496), Emre Kaymaz (301-286-6879), Jewel Taylor (301-286-5083)
(6) Code 600 DCSO: Rosa Kao (301-614-5673)
(7) Code 700 DCISO Roopalee Nesson (301-286-0033), CISO Sergio McKenzie (301-286-0877)
(8) NASA Security Operations Center (SOC), 1-877-NASA-SEC (877-627-2732), available 24×365

Typically it is the PPS system programmer/facility manager who should contact the Directorate and Center personnel. All communication must be in person, by phone, or via encrypted email. **Do not use clear text email!**

Access Banner

Whenever you log into the system you will see a banner similar to the following.

By accessing and using this information system, you acknowledge and consent to the following:

You are accessing a U.S. Government information system, which includes: (1) this computer; (2) this computer network; (3) all computers connected to this network including end user systems; (4) all devices and storage media attached to this network or to any computer on this network; and (5) cloud and remote information services. This information system is provided for U.S. Government-authorized use only. You have no reasonable expectation of privacy regarding any communication transmitted through or data stored on this information system. At any time, and for any lawful purpose, the U.S. Government may monitor, intercept, search, and seize any communication or data transiting, stored on, or traveling to or from this information system. You are NOT authorized to process classified information on this information system. Unauthorized or improper use of this system may result in suspension or loss of access privileges, disciplinary action, and civil and/or criminal penalties.

Additional Useful Information

Visitors must be met at the GSFC main gatehouse (or the equivalent temporary space, usually located in the visitor's center parking lot), signed in, provided with a temporary badge, and escorted while on GSFC property. They are expected to return the temporary badge to the gatehouse drop slot. Phones and faxes should be used for business purposes with some limited "personal use" as elsewhere discussed.

Consequences of Behavior Inconsistent with These Rules

Failure to abide by these rules may result in termination of access privileges. Failure to abide by the rules described under "Copyrighted Software" can be even more severe, including fines and criminal or civil penalties.