PPS External User Rules of Behavior

February 5,2020

This set of rules are intended for users with login (SSH) accounts who are considered External Users, i.e., not members of the PPS staff. This includes the NASA 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. 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, PPS should be notified to disable the account; no further access should be attempted after that.

The basic rules are simple:

- Communicate to account hosts using data-encrypting protocols—e.g., ssh, sFTP; where possible, use a NASA-provided VPN and two-factor authentication.
- Use well-maintained, secure systems and networks to do your remote access.
- Restrict activity in the account to your approved purpose.
- Report security problems promptly.

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 upper case letter, one lower case 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 members 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.

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 and not included as a component of the computer's operating system distribution media. 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 strongly encouraged to keep a log of software installed, including the date and version.)

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).

Requests for Access Privileges and Software Installation

If you need PPS privileges or software installation beyond those normally assigned to your account, contact the help desk. PPS also recognizes privileged accounts having access to certain restricted scientific data. Users with access to restricted data are expected to preserve that restriction in any copies they make of the data.

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.

External Access

You must agree to these Rules of Behavior with respect to the workstation you use to access PPS, 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

NASA mandates two-factor authentication for non-public external access to PPS services, which for external users is only to the hrunting bastion server . 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, you 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." 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 trouble 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 RSA servers will lock your account. You will get a NOMAD email noting the success or explaining the failures 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, including hrunting. 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

Reporting IT Security Incidents

Users are required to report any observed compromise of IT security (viruses, unauthorized access, theft, inappropriate use, suspicious activity, etc.) 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. If at all possible, do not just leave a message, except to mention that you are checking with the next individual on the list.

1. Charles Cosner (301-614-5294), Quyen Nguyen (301-614-5070), Tony Stocker(301-614-5738), Toan Tran (301-614-5065), Marissa Ochir (301-614-5684)
2. Erich Stocker (301-614-5178) or Yi Song (301-614-5375)
3. 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.

Consequences of Behavior Inconsistent with These Rules

Failure to abide by these rules may result in termination of access privileges.