Privileged User Rules of Behavior

Animal and Plant Health Inspection Service
APHIS

Information Technology (IT) Systems
Privileged User Rules of Behavior

Issue Date: 9-24-2010
Effective Date: 9-24-2010
Updated Date: 6/25/2013

Animal and Plant Health
Inspection Service

PRIVILEGED USER RULES OF BEHAVIOR
STATEMENT OF ACCEPTANCE OF RESPONSIBILITIES

INFORMATION SYSTEM PRIVILEGED ACCESS AGREEMENT &
ACKNOWLEDGEMENT OF RESPONSIBILITIES

I understand that as a privileged user on the (System) Administrative LAN, or WAN I will have two user accounts. One for Administration "Administrator" functions such as creating user accounts, resetting passwords, installing software, configuring security settings, etc. The other account will be used for normal day to day functions such as e-mail, browsing the WWW, creating documents, etc.

I understand that I will not use the Administrator "root" account for administration except when necessary for system restore functions when my privileged user account does not have the necessary privilege to do so.

I understand the need to protect all passwords at the highest level of data they secure. I will not share any password(s) or account(s) with other coworkers or other personnel. As a privileged user, I understand the need to **protect the root or administrator password** at the highest level of data it secures. I **will NOT share the administrator or root password** with coworkers who are not authorized **administrative** access.

I understand that I am responsible for all actions taken under my account(s), root or otherwise. I will not attempt to "hack" the network, any connected information systems, or gain access to data for which I am not authorized. I will not access any network under an identity other than my own.

I understand my responsibility to appropriately protect and label all output generated under my account (to include printed materials, magnetic tapes, floppy disks and downloaded hard disk files).

I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate APHIS ISSO, Management or ISSM.

I will NOT install, or modify, any personal, unlicensed or forbidden software (i.e. freeware/shareware, security tools, etc.) without written permission and approval from the APHIS ISSO or ISSM. I will remove personal, unlicensed or forbidden software

I will not add any user names to the Domain Administrators, Local Administrator or Power Users group without the prior approval and direction of the APHIS ISSO, Management or ISSM.

I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the APHIS local area networks or wide area networks.

I understand that I am prohibited from the following while web browsing, specifically while logged in with an administrator account:

a. Introducing Classified, Sensitive But Unclassified (SBU) information or, Security Sensitive Information (SSI) into an unclassified system or environment.

b. Accessing, storing, processing, displaying, distributing, transmitting or viewing material that is pornographic, racist, or illegal in nature.

c. Storing, accessing, processing, or distributing Classified, Proprietary, Sensitive But Unclassified (SBU), For Official Use Only (FOUO) or Privacy Act protected information in violation of established security and information release policies.

d. Obtaining, installing, copying, pasting, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret or license agreement.

e. Fund raising activities, either for profit or non-profit unless the activity is specifically approved by the agency (e.g. social event fund raisers, charitable fund raisers etc.).

f. Gambling, wagering or placing of any bets.

g. Writing, forwarding or participating in chain letters.

h. Posting personal home pages to APHIS computers.

i. Accessing the internet or email while logged in with an administrator account.

Encryption of personal electronic communications is strictly prohibited and can result in the immediate termination of access. This includes, but is not limited to, establishing VPN connections with external parties or utilizing encrypted instant messaging programs.

I understand that if I am in doubt as to any of my roles or responsibilities I will contact the APHIS ISSPM, or Supervisor for clarification.

I understand that all information processed on the APHIS network is subject to monitoring, this includes E-mail and Web Browsing.

I will not allow any user access to the network or any other connected system that is not cleared without prior approval or specific guidance of the APHIS ISSO, ISSM or APHIS Management. I will not grant access to APHIS resources to anyone involved in employee misconduct investigations without written permissions from MRP-HRD-EMIB.

I will ONLY use the special access or privileges granted to me to perform authorized tasks.

I will not use any APHIS owned information systems to violate software copyright by making illegal copies of software.

I will only use my PRIVILEGED USER account for official administrative actions. This account is NOT to be used for day-to-day network communications.

I understand that failure to comply with the above requirements will be reported and may constitute the following actions:

a. APHIS revoking privileged access and/or user privileges
b. Counseling
c. Discharge or Loss of Employment
d. Other Administrative and/or disciplinary and/or adverse action as appropriate

Information Technology (IT) Systems
Privileged User Rules of Behavior

Animal and Plant Health Inspection Service
APHIS

REVIEW AND APPROVAL SIGNATURE

The Animal and Plant Health Inspection Service (APHIS) Privileged User Rules of Behavior (ROB) were prepared for the exclusive use of the APHIS and non-APHIS users with elevated privileges to APHIS IT systems and networks. I have reviewed and concur with the attached Privileged User Rules of Behavior.

Name_____

Role/Title _____

Systems Assigned _____

Signature_____

Date_____

Approved by: _____ 7/18/13
APHIS CIO Date

Animal and Plant Health
Inspection Service