



USDA COMPUTER USER AGREEMENT

As a user of an information system, I will adhere to the following security rules:

1. I will use USDA computer systems (computers, laptops, PDAs, and networks) only for authorized purposes.
2. If using USDA computer systems and networks for nonofficial purposes, I will do so within the bounds allowed by USDA policy and supervisor approval, and without interfering with official business.
3. I will not use USDA resources, including electronic mail and Internet/Worldwide Web access for purposes that violate ethical standards, including harassment, threats, sending or accessing sexually explicit material, racially or ethnically demeaning material, gambling, chain letters, for-profit activities, political activities, promotion or solicitation of activities prohibited by law, and so forth.
4. I will not load any unapproved software (software from home, games, etc.) or install hardware such as peripheral devices (external hard drives, docking stations, thumb drives) on any USDA system. If I need software or hardware installed on my system, I will obtain written approval from my supervisor and coordinate the installation with my System Administrator or the OCIO Help Desk.
5. I will not download file-sharing software (including MP3 music, and video files), peer-to-peer software (i.e. Kazaa, Napster, Limewire) or games onto my government computer, government IT system or network.
6. I will not try to access data or use operating systems or programs, except as specifically authorized.
7. I know I will be issued Government user identifiers (User IDs) and passwords to authenticate my computer account. After receiving them:
 - a. If given a temporary password, I will immediately change the password.
 - b. I will not allow anyone else to have or use my password. If I know that my password has been compromised, I will report this issue to my supervisor or to my agency assigned Information Systems Security Program Manager (ISSPM), or Information Systems Security Officer (ISSO).
 - c. I am responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when I am logged on a system with that account.
 - d. I will ensure that my password is changed on a regular basis or if it is compromised, whichever occurs first.

- e. I understand that USDA has a password complexity requirement, and I will use passwords that meet this requirement.
 - f. I will not write down my password or store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or on any magnetic or electronic media unless approved in writing by the IASO.
8. I will completely log off, or use screen savers that require a password to reactivate the workstation; any time I leave the workstation unattended (except in genuine emergencies, such as fire).
 9. I will scan all removable media (i.e. disks, CDs, thumb drives) or malicious software for viruses before using it on any government computer, system or network.
 10. I will practice good housekeeping with all electronic equipment, including keeping food, beverages, or other contaminants away from computers and data storage media.
 11. I will promptly report any actual or suspected violation of security to my supervisor or assigned USDA Security Staff.
 12. I will stay abreast of security issues via educations and awareness products distributed throughout USDA.