

## USU COMPUTER USER AGREEMENT

As a user of an automated information system (IS) on any network at USU, I agree to adhere to the following in order to protect both the DoD military and USU educational networks.

1. Government information systems (computers, systems and networks) can only be used for authorized official purposes. I understand that access to USU computing resources is a revocable privilege and is subject to content monitoring and security testing.

2. Unlicensed, unaccredited or unapproved software is not authorized for use and cannot be installed on any Government system (computer, system or network). Requests to have previously unapproved software evaluated for use should be sent to the Helpdesk at 295-9800 or [help@usuhs.mil](mailto:help@usuhs.mil).

3. Non-government furnished hardware (i.e. personally owned external hard drives, thumb drives, etc) cannot be connected or installed on any Government system (computer, system or network). Exception requests should be sent to the Helpdesk at [help@usuhs.mil](mailto:help@usuhs.mil) for evaluation. NOTE: Grant-purchased thumb drives used only for official business are permissible. In addition, guest lecturer external drives and thumb drives used in lecture halls and meeting rooms running desktop virtualization are authorized.

4. I will not attempt to access data or use operating systems or programs from unapproved sources, except as specifically authorized.

5. USU or DoD-provided ISs will not be used for commercial financial gain or for illegal activities (surfing pornography, utilizing Peer-to-Peer, etc).

6. I will be issued a user identifier (user ID) and will authenticate using my Common Access Card (CAC), if possible, to log into the system on the NIPRNet or .edu network. After receiving them:

a. I understand that I am the only authorized user of this account and I will not allow anyone else to have or use my CAC card/PIN or user ID and password. If I know my PIN or password is compromised, I will report this to the Information Assurance Manager (IAM) at [ia@usuhs.mil](mailto:ia@usuhs.mil)

b. I am responsible for all activities that occur on my individual account once my password is issued to me.

c. I will ensure that any non-CAC password I have (NIPR or .edu) is changed every 90 days, or when compromised, whichever is sooner.

d. I understand that I must generate, store, and protect passwords and that passwords must consist of at least 15 characters with 2 each of uppercase, and lowercase letters, numbers, and special characters.

e. Common names, birthdays, phone numbers, military acronyms, call signs or dictionary words should never be used as passwords.

f. I will not store my password on any computer, personal digital assistant (PDA), personal electronic device (PED) or any magnetic or electronic media without encrypting the file IAW established DoD guidelines.

g. I will not tamper with my computer to avoid adhering to the USU/DOD security policies.

7. I know that it is a violation of DoD policy for any individual to try to mask his/her identity, or to try to assume the identity of someone else in order to gain access to DoD network resources.

8. All removable media (disks, CDs etc.) must be scanned for malicious software (i.e. viruses, worms) before using it on an USU IS or network.  
NOTE: USU's standard configured desktops and laptops automatically perform this function.

9. Chain e-mail, suspicious attachments or virus warnings should not be forwarded to other users. Instead report chain e-mail and virus warnings to the USU IA team at [ia@usuhs.mil](mailto:ia@usuhs.mil) and then delete the message.

10. "Sniffer" or any hacker-related software is not authorized for use or storage on any Government system (computer, system or network).

11. File-sharing software (including MP3 music, video files, and peer-to-peer) or games will not be downloaded or installed on any Government system (computer, system or network). In addition, unofficial streaming media such as Internet Radio is not permitted.

12. Personally owned IT equipment (PDAs, PEDs) will not be connected to any computer on the USU network without written approval by the IAM ([ia@usuhs.mil](mailto:ia@usuhs.mil)).

13. I will not conduct any government business over a commercial email system such as Gmail, Yahoo, AOL, Hotmail, etc.

14. Anti-virus software on my computer must be updated at least weekly.  
NOTE: This is an automated task for all systems connected to the USU network. Those who are traveling should connect weekly via VPN or immediately upon return to minimize system vulnerability.

15. Internet Chat or instant messenger services (i.e. AOL, MSN, Yahoo) are not authorized for use on DoD networks. I understand that this applies on both NIPR and .edu. DoD approved IM clients are available from Defense Connect Online (DKO).

16. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify my IAM. I know what constitutes a security incident and know that I must immediately report such incidents to the IA0.

17. I will use a password-protected screensaver, log off the workstation and remove my CAC when departing the area.

18. I will comply with the security guidance issued by the USU IAM.

19. If I have a public key infrastructure (PKI) certificate installed on my computer (i.e. software token), I recognized that I am responsible for ensuring that it is removed when no longer required. For proper removal, I will notify my local system administrator (SA) or the IAM. I understand that only DoD PKI certificates are authorized.

20. I understand that each IS is the property of the US Government and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to validate authorized use. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see. I acknowledge that the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of information on each IS.

21. Contractor-owned (non GFE) equipment will not connect to the USU network, and no government data will be processed over it without written approval from the IAM. NOTE: This does not apply to HJF and grant purchased equipment WITH a logistics property sticker.

22. I understand this agreement and will keep the computer secure. If I am the site supervisor, group chief, or SA, I will ensure that all users in my area of responsibility sign this agreement.

23. When I no longer require network access, I will inform my IAM to have my access removed.

24. I know I am subject to disciplinary action if I violate the USU computer security policy. If I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code or Code of Federal Regulations.

25. I understand that all of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When the banner is used, it functions to remind me of the conditions that are set forth in this User Agreement, regardless of whether the banner described these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

This agreement must be signed by both parties prior to issuance of a network account and password. The IAM will retain a copy of each user's agreement until the individual no longer requires network access.

User Name: \_\_\_\_\_

User Signature: \_\_\_\_\_

Date: \_\_\_\_\_

User Department: \_\_\_\_\_

IA Branch Name: \_\_\_\_\_

IA Branch Signature: \_\_\_\_\_

Date: \_\_\_\_\_