Department of Defense
Office of Inspector General
Non-classified Internet Protocol Routing Network (NIPRNET)
Personal User Network Security Agreement

Printed User Name: _____

The Office of the Inspector General, Department of Defense (OIG) provides staff with computers, computing systems, and their associated communication systems to support the Agency's official business. DoD regulations require each employee execute a user agreement to be provided access to a DoD communication system. This agreement sets forth the duties and responsibilities of user issued equipment. This security agreement applies to all uses of the OIG computers and networks regardless of the means of access whether local or remote.

1. I will not load or run any software or install hardware on any OIG computer or network without advanced written approval from the OIG Designated Approving Authority (DAA). This includes, but is not limited to, malware (i.e., viruses, trojans, worms, etc,), "sniffer" or hacker-related software and file-sharing (P2P) software (i.e., Napster, Gnutella, KaZaA including MP3 music and video files) or games.

2. I will not attempt to access data, use operating systems or programs, or modify existing applications, except as authorized. The OIG allows OIG personnel reasonable use of computing resources (for example, hardware, software, networks, and printers) for brief personal purposes unrelated to their work assignments. Such limited personal use is authorized for non-work-related activities if they satisfy the following criteria:

a. Does not interfere with official business needs.
b. Does not interfere with job performance.
c. Does not cause any significant costs to the OIG.
d. Does not compromise information security in any way.
e. Does not involve illegal activities.
f. Are not related to personal business activities or to any political activities.
g. Does not involve activities that could potentially embarrass the OIG or DoD.

3. The following are some examples of illegal and/or inappropriate use of OIG resources which are strictly prohibited. The list should not be considered all-inclusive, but provides examples of prohibited activities:

a. Supporting or accessing Internet sites that promote hate crimes or discriminatory acts such as harassment, intimidation, property damage, or threats.
b. Supporting or accessing Internet sites that demean or degrade others on the basis of race, religion, gender, sexual orientation, age, disability, nationality, or ethnicity.
c. Creating, downloading, viewing, storing, copying, or transmitting sexually oriented material (e.g., pornography)
d. Gambling and gaming (including fantasy sports).
e. Use of computers for commercial purposes; support of for-profit organizations; or other outside employment or businesses activities.
f. Endorsing any product or service.

g. Participating in any partisan political activity.
h. Misleading someone into believing you are acting in an official capacity.
i. Hosting services (for creating or storing web sites) for purposes not related to OIG official business.
j. Using any software that allows your computer to be shared outside the OIG firewall without advanced written approval of the OIG DAA.
k. Creating or forwarding chain letters and mass mailings.
l. Violating license and other computer-related contract provisions - particularly those that expose the OIG to legal costs or damages.
m. Using software, such as password-cracking tools, vulnerability scanners, and network sniffers, without the express written consent of the OIG DAA.

4. I understand I will be issued a user identifier (user ID) and a password to authenticate my computer account. After receiving them:

a. I will not allow anyone else to have or use my password. If I know that my password is compromised, I will immediately notify the System Administrator and the Information Assurance Officer.
b. I am responsible for all activity that occurs on my individual account once my password has been used to log on. I will ensure that my password is changed at least once every 90 days or if compromised, whichever is sooner.
c. Only Information Systems Division (ISD) issued personal digital assistants (PDA) may be used for storing passwords electronically.
d. If I write down my password: I will NOT store it where it is easily accessible to the computer, I will NOT keep the password and user ID together, I will store it in a locked drawer, cabinet, or container, and I will seal the password in an envelope and sign across the seal to detect tampering.
e. I will not tamper with my computer settings to avoid adhering to DOD password policy.
f. I will never leave my computer unattended while I am logged on unless the computer is protected by a "password protected" screensaver or the Public Key Infrastructure (PKI) Common Access Card (CAC) is removed from the card reader. I will log off the network at the end of each workday.

5. I acknowledge that it is a violation of OIG policy for any user to try to mask or hide his or her identity, or to try to assume the identity of someone else.

6. I will not connect an unclassified computer to any classified networks (i.e. SIPRNET, JWICS). I will not transfer information from a classified system to an unclassified system, nor connect a classified system to an unclassified network.

7. I will use my PKI CAC to digitally sign all e-mail that is for official business.

8. I will ensure that all Controlled Unclassified Information (CUI) is protected by encryption. I will use my PKI CAC to encrypt all e-mail that is considered CUI. Per Presidential Memorandum "Designation and Sharing of Controlled Unclassified Information" dated May 9, 2008, CUI is defined as follows: "Controlled Unclassified Information" is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States

or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination."

9. I will protect my PKI CAC and will immediately inform the OIG Office of Security if my card is lost or stolen.

10. I will not connect any personally owned IT device (e.g., PEDs and PDAs (such as Palm Pilots), personal computers, MP3 players, thumb drives, cell phones, etc.) to my OIG computer or OIG network without advanced written approval of the OIG DAA. Only OIG issued equipment may be connected to the OIG LAN with the exception of remote VPN users who are using computers issued by other Government agencies to access the OIG Network via the authorized OIG extranet website or using and authorized OIG extranet client. Those non-OIG Government computers must have prior approval from the OIG, DAA after being scanned for malware and compliance with DoD Information Assurance Vulnerability Management (IAVM) system. Personally owned computers are not allowed to access the OIG Network through any means. You must use a Government computer when teleworking if you access the OIG network.

11. I will ensure that my anti-virus software on my computer is updated at least weekly.

12. I will not use web based e-mail (e.g., Gmail, Yahoo, AOL, etc.) or Internet "chat" services (e.g.,, Google Chat, America Online (AOL), Microsoft Network (MSN) Instant Messenger, Yahoo, etc.) from my computer.

13. I understand that having both a wired connection and a wireless connection to the OIG Network at the same time is not authorized. I will disable the wireless connection and the wireless card on my computer when I am accessing the OIG Network via a wired connection.

14. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify the OIG Technical Support Center.

15. By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

a. You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

b. You consent to following conditions:

i. The U.S. government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

ii. At any time, the U.S. Government may inspect and seize data stored on this information system.

iii. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

iv. This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy.

v. Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work products are private and confidential, as further explained below:

a. Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operations, protections or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

b. The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigations against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

c. Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD Policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

d. Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

e. A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or

confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communications or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

f. These conditions preserve the confidentiality of the communications or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

vi. In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapist, or clergy, and their assistants), 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 of disclosure of such information.

vii. 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 a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions and regardless of whether the banner expressly references this User Agreement.

OIG Contact Information:
Technical Support Center
Phone: 703-604-9865
E-mail: techsupport@dodig.mil
E-mail: Helpdesk@dodig.mil

Date: _____

User Signature: _____

Reset Form