Acceptable Use Policy (AUP)

MANDATORY NOTICE AND CONSENT FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

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

> 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.

You consent to the following conditions:

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.

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

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.

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.

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 product are private and confidential, as further explained below:

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, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

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 investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

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 ofa privilege or confidentiality.

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.

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 communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

These conditions preserve the confidentiality of the communication 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.

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, psychotherapists, 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 or disclosure of such information.

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 provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

NDU STATEMENT OF INFORMATION SYSTEM USE AND ACKNOWLEDGEMENT OF USER RESPONSIBILITIES

I will use NDU Information Systems for official use and authorized purposes only in accordance with DoD 5500.7-R Joint Ethics Regulation. I will not introduce or process data which the Information System has not been specifically authorized to handle. I understand that all information processed on NDU-controlled Information Systems is subject to monitoring. This includes email and web browsing. I may also be held both criminally and financially responsible for any damages that may occur to the network, systems, other electrical and non-electrical equipment, or computing devices, if my actions are determined to be deliberate, willful, or malicious.

I understand the need to protect all passwords at the highest level of data they secure. I will not share my password or account(s) information with coworkers or other personnel not authorized to access the Information System.

I understand that I am responsible for all actions taken under my account(s) either as an authorized or privileged user and will not attempt to “hack” the network, any connected Information Systems, or gain access to data which I am not authorized to access.

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

I understand I must have requisite security clearance and documented authorization (approved by my supervisor of my need-to-know before accessing DoD information and Information Systems.

I understand my responsibility to ensure Privacy Act, and other protected personal information (such as personally identifiable information) is protected while it is being processed or accessed. In computer environments outside the NDU physical data processing installations requiring access to NDU Information Systems (such as remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities), I know I must ensure appropriate protection of personal and sensitive data.

I understand by signing this document I acknowledge and consent that when I access NDU and/or any DoD Information System:

I am accessing a U.S. Government information system (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only. I understand I must complete designated IA training before receiving system access.

I understand that security protections may be utilized on NDU information systems to protect certain interests that are important to the Government. For example, passwords, access cards, encryption, or biometric access controls provide security for the benefit of the Government. These protections are not provided for my benefit or privacy and maybe modified or eliminated at the Government's discretion.

I understand that I am prohibited from the following:

Introducing classified information into an unclassified system or environment.

Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, racist, promotes hate crimes, or subversive in nature, or objectionable by nature to include; material that encourages criminal activity or violates any applicable local, state, Federal, national, or international law.

Violating the established security, release, and protection policies for information identified as Classified, Proprietary, Controlled Unclassified Information (CUI), For Official Use Only (FOUO), or Privacy Act-protected during the information handling states of storage, process, distribution or transmittal of such information.

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. This includes peer-to-peer file sharing software or games.

Installing any unauthorized software (e.g., games, entertainment software) or hardware (e.g., sniffers).

Knowingly writing, coding, compiling, storing, and transmitting. Or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.

Engaging in prohibited political activity.

Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g.• eBay), or stock trading (i.e., issuing buy, hold and/or sell directions to an online broker).

Engaging in fundraising activities, either for profit or non-profit unless the activity is specifically approved by the Command (e.g.• Command social event fundraisers, charitable fund raisers, etc.).

Gambling, wagering, or placing of any bets.

Writing, forwarding, or participating in chain letters.

Posting personal web pages, using my personally-owned information technology (IT such as personal electronic devices (PEDs), personal data assistants (PDAs), laptops, thumb drives etc.), or non-DISA-controlled information technology on DISA-controlled computing assets.

Any other actions prohibited by DoD 5500.7-R or any other DoD issuances.

Personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

I will immediately report any person suspected of engaging in, or any other 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 Information Assurance (IA) Management or senior IA Technical Level representatives.

I will not install, modify, or remove any hardware or software (i.e. freeware, shareware, security tools. etc.) without written permission and approval from the Information Assurance Manager (IAM) or senior IA Technical Level representative.

I will not remove or destroy system audit, security event, or any other logs without prior approval from the IAM or senior IA Technical Level representative.

I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into NDU information systems or networks.

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 IA Management.

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

I agree to notify the organization that issued the account when access is no longer required.

In addition to the above statements of acceptable use for NDU Information Systems, the use of NDU's Wireless Gateway also requires:

Users of any personally-owned mobile device shall ensure the device is kept up-to-date with anti-virus definitions and security vulnerability updates.

All NDU Government-issued devices must be online and physically connected to the NDU wired network once per week, for at least 4 hours, to ensure necessary device patches and anti-virus updates get installed.

ALL MUST READ AND SIGN:

I understand that failure to comply with the requirements of this Agreement will be reported and investigated. The results of the investigation may result in one or all of the following actions:

- Immediate revocation of system access and/or user privileges
- Job counseling, admonishment
- Revocation of Security Clearance
- Uniform Code of Military Justice and/or criminal prosecution
- Disciplinary action, reassignment, discharge, or loss of employment

I HAVE READ, UNDERSTAND, AND WILL COMPLY WITH THE REQUIREMENTS SET FORTH IN THIS AGREEMENT.

Name:

Date:

Signature: