

NDU SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

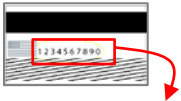
PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. PRINCIPAL PURPOSE: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of Individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records will be maintained in soft and/or hard copy2. ROUTINE USES: None. DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATION <input type="checkbox"/> USER ID: _____	DATE (yyyymmdd)
SYSTEM NAME	

PART I – USER INFORMATION, CONSENT, AGREEMENT AND RESPONSIBILITIES *(Completed by requester)*

1. NAME <i>(Last, First, Middle Initial)</i>		2. RANK/TITLE	
3. BUILDING #	4. OFFICE #	5. OFFICE PHONE #	6. Phone #
7. POSITION TITLE INTERNATIONAL STUDENT		8. ORGANIZATION:	
10. NDU PRIMARY E-MAIL ADDRESS		11. PERSONAL E-MAIL ADDRESS *Not .gov or .mil	
13. OFFICIAL MAILING ADDRESS		15. CAC USER <input type="checkbox"/> YES <input type="checkbox"/> NO <i>(Skip to 17)</i> CAC-EDIPI: _____	
14. CITIZENSHIP <input type="checkbox"/> US Citizen <input type="checkbox"/> US Resident <input type="checkbox"/> Foreign National: _____		17. USER TYPE <input type="checkbox"/> Military <input type="checkbox"/> Civilian <input type="checkbox"/> Contractor	
16. ACCOUNT TYPE <input type="checkbox"/> Faculty <input type="checkbox"/> Staff <input type="checkbox"/> Student <input type="checkbox"/> Intern <input type="checkbox"/> Volunteer <input type="checkbox"/> Summer Hire		18. MILITARY BRANCH <i>(If not military skip to 20)</i> <input type="checkbox"/> USAF <input type="checkbox"/> USA <input type="checkbox"/> USN <input type="checkbox"/> USMC <input type="checkbox"/> USCG <input type="checkbox"/> Foreign National	
19. PERSON REPLACED (If applicable)		20. ACTIVE DIRECTORY GROUP MEMBERSHIP	
21. ADDITIONAL INFORMATION			



22. IA TRAINING CERTIFICATION REQUIREMENTS (User must complete Cybersecurity training in JKO every 12 months)

Cybersecurity training certification will be verified via JKO prior to authorization of network account.

23. NDU STATEMENT OF INFORMATION SYSTEM USE AND ACKNOWLEDGEMENT OF USER RESPONSIBILITIES

PART A: MANDATORY NOTICE & 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, the given system(s) are not private, are subject to routine monitoring, interception, 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 protection of a privilege or confidentiality.
- Users should take reasonable steps to identify such communications of 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 provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

PART B: NDU STATEMENT OF INFORMATION SYSTEM USE AND ACKNOWLEDGEMENT OF USER RESPONSIBILITIES FOR UNCLASSIFIED SYSTEMS

FOR AUTHORIZED ACCESS:

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 is specifically authorized to handle. I understand all information processed on NDU-controlled Information Systems is subject to monitoring; that 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(s) or account(s) information with 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. I 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 the requisite security clearance and documented authorization (approved by my supervisor) of my need-to-know before accessing NDU/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 and 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) provided for U.S. Government-authorized use only; I understand I must complete designated IA training prior to initial 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 may be 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, 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 fundraisers, 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-NDU-controlled information technology on NDU-controlled computing assets.
- Any other actions prohibited by DoD 5500.7-R or any other DoD issuances.

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 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.

[ADDITIONAL PRIVACY ACT STATEMENT FOR NDU WIRELESS INTERNET GATEWAY USERS]

AUTHORITY: 5 U.S.C. 301; 10 U.S.C. 131. PRINCIPAL PURPOSE(S): Identifies the NDU Wireless Internet Gateway user as receiving usage and security awareness training governing use of the Gateway and agreeing to use the Gateway in accordance with security and wireless policies. The information is used for identification purposes and to verify compliance with DoD requirements regarding accountability of information processing systems, and provides emergency contact information on the user in the event that the user's access to the Gateway becomes compromised, or requires a reconfiguration due to security policy changes. ROUTINE USE(S): None. DISCLOSURE: Voluntary; however, failure to provide the requested information will result in denial of issuance of access to the NDU Wireless Internet Gateway.

NOTE: This form's Part I User Personal information is used to contact a (Wireless System) user in the event of a security incident or an emergency.

PART C: NDU WIRELESS GATEWAY USER ADDITIONAL STATEMENT OF INFORMATION SYSTEM USE AND ACKNOWLEDGEMENT OF USER RESPONSIBILITIES

The following preventive measure is required to ensure use of given device on the Wireless Gateway does not result in the release of DoD information to unauthorized persons: All devices connected to the NDU Wireless Network must be configured to require a passcode for device unlock. Sensitive data could be compromised if a device unlock passcode is not set up on a device connected to a DoD Network. These devices are particularly vulnerable because they are exposed to many potential adversaries when they are taken outside of the physical security perimeter of DoD facilities, and because they are easily concealed if stolen. DoD CIO Memorandum, "Policy on Use of DoD Information Systems Standard Consent Banner and User Agreement," 9 May 2008 requirements:

All above previous Part A user agreement statements herein apply to the NDU Wireless Gateway along with the following additional Acceptable Use requirements:

- Forfeiture - any personally-owned device involved in a CAT 1 security incident involving classified information shall be forfeited and will not be returned to the user.
- Users of any personally-owned mobile device on the Wireless Gateway shall ensure the given device is kept up-to-date with anti-virus definitions and security vulnerability updates.
- All NDU Government-issued devices authorized for use on the Wireless Gateway must be online and physically connected to the NDU intranet once a week, for at least 4 hours, between Wednesday and Friday to ensure necessary device patches and anti-virus updates get installed.
- Wireless Gateway users shall follow security policies which govern use of that connection; additionally, the following activities are prohibited: -
 - Transmitting or downloading sensitive information (i.e., PII, HIPPA, FOUO, etc.), or classified information.
 - Transmitting or downloading sexually explicit information, material that could be considered sexually harassing, or obscene language or material.
 - Attempting to defeat any Wireless Gateway associated security systems.
 - Viewing, changing or deleting files of another user without appropriate authorization or permission.
 - Obtaining, installing, copying or using software in violation of the license agreement of the vendor.
 - Unauthorized music and movie downloads (peer to peer activity), or improperly storing or processing copyrighted material.
 - Transmitting or downloading offensive material, such as racist literature, and any activities for personal or commercial gain.
- Wireless Gateway users are required to report any Wireless Gateway system security incidents to the NDU Information Assurance Manager via the NDU IT Helpdesk.

ALL MUST READ AND SIGN:

I understand that failure to comply with the requirements of this User 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

23a. [] I HAVE READ, UNDERSTAND, AND WILL COMPLY WITH THE REQUIREMENTS SET FORTH IN THIS USER AGREEMENT. IN THE EVENT OF CONFLICT, PART I TAKES PRECEDENCE OVER ABOVE PART II.

23b. SIGNATURE:

23c. DATE: