# 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 | DATE (yyyymmdd) |
|---|---|
| ☑ INITIAL ☐ MODIFICATION ☐ DEACTIVATION ☐ USER ID: _____ | Enter Present Date |

SYSTEM NAME *(Platform such as NDU, Google Cloud, Blackboard, etc.)*

NDU and Blackboard

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

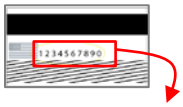
| 1. NAME (*Last, First, Middle Initial*) | 2. RANK/TITLE | 3. SOCIAL SECURITY # (*Last 4*) |
|---|---|---|
| Self Explanatory | Self Explanatory | Self Explanatory |

| 4. BUILDING # | 5. OFFICE # | 6. OFFICE PHONE | 7. COMMERCIAL PHONE |
|---|---|---|---|
| Normandy Hall SC-1 | Leave Blank | Leave Blank | Your Mobile # |

| 8. POSITION TITLE | 9. ORGANIZATION (*NDU Affiliation*) | 10. NDU BADGE # |
|---|---|---|
| Student | JFSC/NDU JCWS 17-1 | Leave Blank |

| 11. PRIMARY E-MAIL ADDRESS | 12. ALTERNATE E-MAIL ADDRESS | 13. BADGE EXPIRATION DATE |
|---|---|---|
| | | Leave Blank |

| 14. OFFICIAL MAILING ADDRESS | 15. CITIZENSHIP | 16. CAC USER |
|---|---|---|
| 7800 Hampton Blvd.<br>Norfolk, VA 23511 | ☑ US Citizen<br>☐ US Resident<br>☐ Foreign National: As it Applies | ☑ YES<br>☐ NO *(Skip to 17)*<br>CAC-EDIPI: On the back o |



| 17. ACCOUNT TYPE | | 18. USER TYPE | 19. MILITARY BRANCH *(If not military skip to 20)* | |
|---|---|---|---|---|
| ☐ Faculty | ☐ Staff | ☑ Military | ☐ USAF | ☐ USA |
| ☑ Student | ☐ Intern | ☐ Civilian | ☐ USN | ☐ USMC |
| ☐ Volunteer | ☐ Summer Hire | ☐ Contractor | ☐ USCG | ☐ Foreign Nation |

| 20. PERSON REPLACED (If applicable) | 21. ACTIVE DIRECTORY GROUP MEMBERSHIP |
|---|---|
| Leave Blank | NDU_JFSC_JCWS_Students |
| **22. ADDITIONAL INFORMATION** | |
| Leave Blank | |

**23. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (*User must complete IA training every 12 months*)**

23a. ☑ I have completed the Annual Information Awareness Training on the date indicated. 23b. DATE: Date from Cyber Awareness Cert.

**24. NDU STATEMENT OF INFORMATION SYSTEM USE AND ACKNOWLEDGEMENT OF USER RESPONSIBILITIES**

**PART I**

**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, 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 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 II**

**NDU STATEMENT OF INFORMATION SYSTEM USE AND ACKNOWLEDGEMENT OF USER RESPONSIBILITIES FOR UNCLASSIFIED AND CLASSIFIED**

**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 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(s) or account(s) information with other 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. 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) 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 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.
- Personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

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.

**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

24a. ☑ **I HAVE READ, UNDERSTAND, AND WILL COMPLY WITH THE REQUIREMENTS SET FORTH IN THIS AGREEMENT. IN THE EVENT OF CONFLICT, PART I TAKES PRECEDENCE OVER PART II ABOVE.**

| 24b. SIGNATURE: | 24c. DATE: Enter Present Date |
|---|---|

**PART II – ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (*If user is a contractor provide company name, contract # and contract expiration in 30a thru c*)**

25. JUSTIFICATION FOR ACCESS

JCWS 17-1 Student

| | | |
|---|---|---|
| 26. TYPE OF ACCESS REQUIRED | ☑ AUTHORIZED | ☐ PRIVILEGED |
| 27. USER REQUIRES ACCESS TO<br>☑ UNCLASSIFIED | ☐ CLASSIFIED<br>(Specify Category): _____ | ☐ OTHER<br>(Specify Category): _____ |
| 28. VERIFICATION OF NEED TO KNOW<br>I certify that this user requires access as requested ☐ | 29. ACCESS EXPIRATION DATE (*If contractor use expiration date in 32*) | |
| 30. COMPANY NAME (*If Contractor*) | 31. CONTRACT NUMBER (*If Contractor*) | 32. CONTRACT EXPIRATION DATE |

33. OPTIONAL INFORMATION (*Additional Information*)

| | | | |
|---|---|---|---|
| 34. SUPERVISOR NAME | 34a. RANK/TITLE | 34b. SIGNATURE | 34c. DATE |
| 34d. ORGANIZATION & DEPARTMENT | 34e. OFFICIAL MAILING ADDRESS | | 34f. PHONE |
| 35. IS OWNER OR APPOINTEE NAME | 35a. RANK/TITLE | 35b. SIGNATURE | 35c. DATE |
| 35d. ORGANIZATION & DEPARTMENT | 35e. OFFICIAL MAILING ADDRESS | | 35f. PHONE |
| 36. IAO OR APPOINTEE NAME | 36a. RANK/TITLE | 36b. SIGNATURE | 36c. DATE |
| 36d. ORGANIZATION & DEPARTMENT | 36e. OFFICIAL MAILING ADDRESS | | 36f. PHONE |

**PART III – SECURITY MANAGER VALIDATES BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION**

| | | |
|---|---|---|
| 37. TYPE OF INVESTIGATION | 38. DATE OF INVESTIGATION | 39. CLEARANCE LEVEL |

| | | | |
|---|---|---|---|
| 40. IT LEVEL DESIGNATION | ☐ LEVEL I | ☐ LEVEL II | ☐ LEVEL III |

| | | | |
|---|---|---|---|
| 41. SECURITY MANAGER NAME | 41a. RANK/TITLE | 41b. SIGNATURE | 41c. DATE |
| 41d. ORGANIZATION & DEPARTMENT | 41e. OFFICIAL MAILING ADDRESS | | 41f. PHONE |

INSTRUCTIONS

## TYPE OF REQUEST: Completed by the user.

TYPE OF REQUEST. User indicates the type of request he/she requires.
DATE. User enters the date he/she is making the request.
SYSTEM NAME. User enters the name of the system(s) he/she need to access.
SYSTEM LOCATION. The User enters the location(s) of the system(s).

## PART I: Completed by the user.

(1) Name. The last name, first name, and middle initial of the user.
(2) Rank/Title. Rank or Tittle of the user.
(3) Social Security. Last four digit of the user's SSN.
(4) Building #. Building where the user's office is located.
(5) Office #. Room number where the user's office is located.
(6) Phone. Phone number of the user.
(7) Commercial Phone. The commercial phone number of the user.
(8) Position Title. The civilian, military or contractor job title of the user.
(9) Organization. NDU affiliation of the user (such as iCollege, JFSC, etc.).
(10) Badge #. NDU or JFSC badge number assigned to the user.
(11) Primary Email. The user's official e-mail address.
(12) Alternate Email. Optional e-mail address.
(13) Badge Expiration. Date the user badge expires.
(14) Official Mailing Address. The user's official mailing address.
(15) Citizenship. Place an "X" in the appropriate box. IF FN, indicate nation.
(16) CAC User. Place an "X" in the appropriate box. If Yes, indicate the EDIPI. The Social Security Number (SSN) is not the EDIPI. Do not use the SSN.
(17) Account Type. Place an "X" in the appropriate box.
(19) Military Branch. Place an "X" in the appropriate box.
(20) Person Replaced. Type in the name of the person the user is replacing (if applicable). It ensures identical user rights and permissions.
(21) Active Directory Group Membership. Defines access to NDU resources. Contact your local Information Management Officer, Supervisor, Information Owner or Government Sponsor.
(22) Additional Information.
(23) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.
(24) User's Signature. User must sign NDU Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).

## PART II: Completed and endorsed by the user's supervisor or the Government Sponsor.

(25) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
(26) Type of Access Required: Place an "X" in the appropriate box. The "Authorized" category will be used for individual with normal access. The "Privileged" category will be used for those with privilege to amend or change system configuration, parameters, or settings.
(27) User Requires Access To: Place an "X" in the appropriate box. Specify category.
(28) Verification of Need to Know. To verify that the user requires access as requested.
(29) Expiration Date for Access. The user must specify expiration date. If the user is a contractor, then field 32 and 32c are one and the same.
(30) Company Name. If contractor, type the name if his/her company.
(31) Contract Number. If contractor, type his/her company's contract number.
(32) Contract Expiration. If contractor, type the contract's expiration date.
(33) Additional Information. As required.
(34) Supervisor Name. The supervisor or representative prints his/her name to indicate that the information has been verified and that access is required.
(34a) Rank/Title. Rank or Title of the user's supervisor or representative.
(34b) Signature. Supervisor's signature is required by the endorser or his/her representative.
(34c) Date. Date supervisor signs the form.
(34d) Organization & Department. Supervisor's organization and department.
(34e) Official e-mail Address. Supervisor's e-mail address.
(34f) Number. Supervisor's telephone number.
(35) Information System Owner or Appointee Name. The IS owner prints his/her name to indicate that the information has been verified and that access is required.
(35a) Rank/Title. Rank or Title of the IS owner.
(35b) Signature. IS owner's signature.
(35c) Date. Date IS owner signs the form.
(35d) Organization & Department. IS owner's organization and department.
(35e) Official e-mail Address. IS owner's e-mail address.
(35f) Number. IS owner's telephone number.
(36) Information Assurance Officer (IAO) or Appointee Name. The IAO prints his/her name to indicate that the information has been verified and that access is required.
(36a) Rank/Title. Rank or Title of the IAO.
(36b) Signature. IAO's signature.
(36c) Date. Date IAO signs the form.
(36d) Organization & Department. IAO's organization and department.
(36e) Official e-mail Address. IAO's e-mail address.
(36f) Number. IOA's telephone number.

## PART III: Completed by the Security Manager conducting the Certification of Background Investigation or Clearance

(37) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).
(38) Date of Investigation. Date of last investigation.
(39) Clearance Level. The user's current security clearance level (Secret or Top Secret).
(40) IT Level Designation. Select the user's IT designation (Level I, Level II, or Level III) if known.
(41) Security Manager Name. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.
(41a) Rank/Title. Rank or Tittle of the Security Manager or representative.
(41b) Signature. Security Manager or representative's signature.
(41c) Date. Date Security Manager signs the form.
(41d) Organization & Department. Security Manager 's organization and department.
(41e) Official e-mail Address. Security Manager 's e-mail address.
(41f) Number. Security Manager's telephone number.

## DISPOSITION OF FORM

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Form is purposed to use digital signatures. Digitally signed forms must be stored electronically to retain non-repudiation of electronic signature. If pen and ink signature must be applied, original signed form must be retained. Retention of this form shall be IAW DOD and NDU's Record Management regulations and policies. Form may be maintained by the user's Information Assurance Officer and/or Security Manager. Completed forms contain Personal Identifiable Information (PII) and must be protected as such.