

**National Defense University (NDU) Wireless Internet Gateway USER AGREEMENT**

NOTE: This information may be used to contact a (Wireless System) user in the event of a security incident or an emergency.

**PRIVACY ACT STATEMENT**

**AUTHORITY:** 5 U.S.C. 301; 10 U.S.C. 131. **PRINCIPAL PURPOSE(S):** Identifies the user of the NDU Wireless Internet Gateway 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.

**PART I- PERSONAL INFORMATION**

1. LAST NAME	2. FIRST NAME	3. RANK/GRADE
4. ORGANIZATION	5. BUILDING	6. ROOM NUMBER
7. PRIMARY TELEPHONE NUMBER	8. ALTERNATE PHONE NUMBER	9. SPONSOR ORGANIZATION
10. E-MAIL ADDRESS		

**PART II- INFORMATION ON THE SYSTEM TO BE USED TO ACCESS THE GATEWAY**

BRAND	DESCRIPTION	MODEL	SERIAL NUMBER	MAC Address

11. The following preventive measures are requirements to ensure that use of the above system on the Gateway does not result in the release of DoD information to unauthorized persons.

DoD CIO Memorandum, "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," 9 May 2008 Requirements:

By signing this document, you acknowledge and consent that when you access the NDU Wireless Internet Gateway:  
 -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:
- o The U.S. Government routinely intercepts and monitors communications on this network 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.
  - o Communications using, or data stored on, the Gateway are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
  - o 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

National Defense University (NDU) Wireless Internet Gateway USER AGREEMENT

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 the Gateway if the user intends to rely on the protections of a 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 provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

**Acceptable Use:**

- Users utilizing personally owned mobile devices shall keep their devices up-to-date with anti-virus definitions and security vulnerability updates.
- All NDU Government-issued devices authorized for use on the wireless network must be online and physically connected to the NDU network once a week, for at least 4 hours, between Wednesday and Friday to ensure necessary patches and anti-virus updates are installed.
- Users shall follow security policies that govern the use of this connection. The following activities are prohibited:
  - Transmission of sensitive information (i.e., PII, HIPPA, FOUO, etc.).
  - Transmitting or downloading sexually explicit information, material that could be considered sexually harassing, or obscene language or material.
  - Transmitting or downloading classified information.
  - Attempting to defeat 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).
  - Improperly storing or processing copyrighted material.
  - Transmitting or downloading offensive material, such as racist literature, and any activities for personal or commercial gain.
  - Users are required to report any information systems security incidents to the Information Assurance Manager via the Helpdesk.

By signing this user agreement, I am acknowledging that I accept and will abide by all the terms and conditions described above.

**The Wireless Network Access information that you have been given is confidential and not to be shared with anyone.**

FOR REPORTING PROBLEMS OR TO ASK QUESTIONS, CONTACT:

ITSG Helpdesk: 202-685-3824  
Information Assurance (IA) Team: NDU-IA@ndu.edu

12. Date Signed (YYYYMMDD):

13. Signature of User: