Contractor Add User to DHA Network

NOTE: For instructions on completing form, please see the reverse side.

SECTION I: GENERAL USER INFORMATION*

☐ **Workstation in Place** ☐ **Special Applications/Access** ☐ **Dial-Up Access**

*** If workstation is required or move of a workstation is required, a Network Support Form must be submitted separately.**

Name:		**Date Required:**
Last *First* *MI* *Preferred Name*		
Salutation:	**US Citizen:** ☐ **Yes** ☐ **No** (Non-US Citizen Contractor Employees are not allowed access to the DHA Network or DoD systems)	
Contractor/Organization Name:		**Contract Number:**
Government Organization Supported: *(required for contractors)*		**State of Birth/Keyword:**
Location/Building:	**Suite:**	**Commerical Phone:** *(Include Extension)*

SECTION II: ADD USER ACCOUNT

To add a user to the DHA Network, please fill in all information above, read the Agreements attached and sign these forms. State of Birth /Keyword is mandatory for all new accounts. **I have read and signed the attached Security Agreement and User Agreement**

Name (printed):	**Date:**
Signature:	

SECTION III: NEW USER EQUIPMENT INFORMATION

Equipment: New user for equipment currently in place.

CPU Type:	**System Name:**	**TMA Barcode #:**	**Former User:**	**Monitor Barcode #:**
User's Signature:				**Date:**

SECTION IV: APPROVING AUTHORITY

Contractor Security Manager (required for all contractors):	**SF85P Submitted or Clearance Verified Yes___ No___**	**Date:**
Print Full Name	*Signature*	*Date*
Government Program/Project Manager:	**Approved Yes___ No___**	
Print Full Name	*Signature*	*Date*
DHA OA PSD Representative:	**ADP/IT Security Clearance Verified Yes__ No__**	**Date:**
Print Full Name	*Signature*	*Date*

Comments/Special Notes ***(List Non-Standard Equipment Here):***

SECTION V: FOR INTERNAL USE ONLY

Remedy Ticket Number:

DHA Network Security Agreement

Office of the Assistant Secretary of Defense (Health Affairs)

INSTRUCTIONS

Section I: General User Information

A. Complete this section for all requests.
B. Non-US Citizen Contractor Employees are not to submit an SF85P for Background Investigation.
C. Non-US Citizen Contractor Employees are not to be allowed access to DHA Network or DoD Systems

Section II: Add User Account to the DHA Network

A. Fill out General User Information and Section I.
   1. "Preferred Name" refers to a nickname (i.e. Mike for Michael) – will NOT be used as email address. " State of Birth"/Keyword **required** to verify user's identity
B. Read the Security Agreement below, sign the forms and return them to the Network Support Services IT Call Center
C. Read the User Agreement on the next page, sign the form, and return to the Network Support Services IT Call Center

Section III: New User Equipment Information

A. Fill out General User Information and Section II.
B. Fill out Section A with all information for New User Equipment that is already in place.

Section IV. Approving Authority

A. DHA PSD Representative must sign all ADD requests for Contractors, verifying OPM receipt of form, before the network account can be created.
B. The Contractor FSO must attach a sealed envelop to the Add User Form with a current printout of the JPAS Summary or a separate sheet containing the SSN of the new user. After Gov't Program/Project Manager signoff, fax the Add User Form to the PSD Office at 703-681-3934
C. After PSD Office signoff, the form will be faxed (703 379-3961) to the Network Support Services IT Call Center (itcallcenter@dha.mil) and the account will be added.

As a condition to being granted access to the Defense Health Agency (DHA) Network, I agree to comply with the following security requirements:

For Contractor Personnel:

- I agree to complete and submit information required for a background check (SF85P or SF86) as a prerequisite to being added to the network.
- I agree to complete the IA training, located at https://intranet.tma.osd.mil/IA_training / within seven (7) business days of being added to the network, and understand that my account will be disabled if this is not accomplished.
- I agree to complete the required Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) training, available through MHS Learn, at https://mhslearn.csd.disa.mil/ilearn/en/learner/mhs/portal/home.jsp within 30 days, and understand that my account will be disabled if this is not accomplished.
- I agree to complete the application for Department of Defense Common Access Card DEERS Enrollment (DD1172-2) within seven (7) business days of being added to the network.
- I will comply with Department of Defense (DoD) policies, regulations, and guidelines regarding the protection, handling, processing, transmission, distribution, and destruction of sensitive unclassified information designated "For Official Use Only."
- I will protect sensitive unclassified information from unauthorized access, disclosure, modification, misuse, damage, or theft.
- I will mark all output/media with the applicable security classification markings
- I will observe all policies and procedures governing the secure operation and authorized use of the DHA Network.
- I will disable all wireless capabilities when not in use and/or will disable all wireless capabilities when connected via wired connection
- I will protect all passwords issued to me, and will not disclose them to anyone. I understand that password sharing or the use of another user's ID and password is prohibited. I will change my passwords when required and promptly whenever I suspect that it may have been compromised.
- I will report all security incidents including suspected password compromises and computer viruses to the Network Support Services IT Call Center and my Government Project Manager.
- I will immediately notify the Network Support Services IT Call Center (Customer Assistance Center) when I no longer require access to the network (due to transfer, completion of project, retirement, etc.) and of any changes to my work location or phone number.
- I will use the DHA Network for the processing, transmission, and storage of official U.S. Government related or authorized work only.
- I will not copy or remove copies of licensed software without proper authorization nor will I import or use unauthorized software, firmware, or hardware in the work environment. Only equipment that is owned and maintained by DHA Network may be connected to the network.
- I will not knowingly introduce any malicious code into the DHA Network, nor will I attempt to bypass or circumvent network security features or mechanisms.
- I will not relocate network equipment or software without proper authorization.
- I will use remote access capabilities for official U.S. Government related or authorized work only and protect my password while connecting remotely from all unauthorized users.
- Upon final checkout or departure from Defense Health Agency or a contractor facility I will not have in my possession any sensitive unclassified information in any form nor any government owned equipment, software, storage media (such as diskettes), user manuals, or system documentation.

WARNING: Unauthorized access and/or use of the Defense Health Agency (DHA) Network and services is prohibited and could result in the loss of system privileges and/or civil or criminal penalties. No illegal software will be installed on local and/or network equipment. All software will be inventoried and installed by Network Support Services personnel only. Contact the Network Support Services IT Call Center at 703-681-9411 if you require further assistance. All information placed on this system is subject to monitoring and is not subject to any expectation of privacy.

ALL INFORMATION PLACED ON THIS SYSTEM IS SUBJECT TO MONITORING AND IS NOT SUBJECT TO ANY EXPECTATIONS OF PRIVACY

Name (printed):	**Date:**
Signature:	

STANDARD MANDATORY NOTICE AND CONSENT PROVISION
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 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.

Name (printed):	**Date:**
Signature:	