# NAVY MEDICINE OPERATIONAL TRAINING CENTER
# VPN USER AGREEMENT

**FOR PERSONNALLY-OWNED COMPUTER DEVICES**

(INCLUDES PERSONAL DIGITAL ASSISTANT, LAPTOPS, DESKTOPS, PALM PILOTS, AND ANY OTHER PERSONALLY OWNED ELECTRONIC DEVICE)

| NAME (printed): | COMMAND: | DEPT CODE: | BLDG/ROOM NUMBER: |
|---|---|---|---|
| | | | |

## DESCRIPTION

| COMPUTER MAKE: | MODEL: | OPERATING SYSTEM: |
|---|---|---|
| | | ❑ Windows XP Home<br>❑ Windows XP Professional<br>❑ Windows 2003<br>❑ Windows Millennium Edition<br>❑ Other:_____ |
| INTERNET CONNECTION:<br>❑ DSL<br>❑ CABLE<br>MODEM BRAND:_____ | IS A WIRELESS ROUTER USED:<br>❑ YES<br>❑ NO | |

| Justification for remote access to the NMOTC unclassified network: | ANTI-VIRUS SOFTWARE USED: |
|---|---|
| ❑ TELEWORK<br>❑ TAD/TDY<br>❑ OTHER:_____ | ❑ Norton<br>❑ McAfee<br>❑ Symantec<br>❑ Other:_____ |

**RULES AND RESPONSIBILITIES FOR PERSONALLY OWNED ELECTRONIC DEVICES USED FOR PROCESSING/ACCESSING GOVERNMENT DATA AND E-MAIL**

I agree to the following provisions and will:

(1) Handle, store, maintain and destroy all unclassified information in accordance with DoD/DoN and NMOTC policies.

(2) Immediately notify the command of any information loss, theft or suspicious behavior.

(3) Protect the confidentiality, integrity and availability of e-mail systems and information at all times.

(4) Complete all required training.

(5) Install, configure, maintain and update required security software, hardware, PKI certificates and current anti-virus files by updating them at least weekly or when prompted.

(6) Not use public access computers, such as those in college computer labs, public kiosks, libraries, etc., to access NMOTC unclassified e-mail accounts.

(7) At the completion of a session:

- (1) Close all e-mail files
- (2) Clear the web browser's cache
- (3) Exit and close the browser
- (4) Immediately turn off the computer. "Sleep" and "Standby" modes are not acceptable

(8) Install and use approved anti-virus protection and personal firewall software. Approved software is available to all DoD employees at no cost from the Defense Information Systems Agency (DISA) website at http:/www.disa.mil/infosec/iaweb/default.html, under the DoD enterprise license. Additional approved products may be found on the National Information Assurance Partnership (NIAP) validated product list at http://niap.nist.gov/niap/services/validated-products.html.

(9) Ensure that no other wireless or LAN connection exists for the duration of the session. Any other existing connections must be disabled for the duration of the session.

(10) Ensure that appropriate security settings are configured into the wireless router to ensure adequate network security is established.

| The undersigned accepts the responsibilities to user their personally owned hardware/software for Government use. | |
|---|---|
| OWNER SIGNATURE: | DATE: |

**DEPARTMENT/DIRECTOR**

**I have evaluated this request for validity and approve its use as essential for mission accomplishment.**

| | | |
|---|---|---|
| ❑ APPROVED ❑ DISAPPROVED | SIGNATURE: | DATE: |
| ❑ APPROVED ❑ DISAPPROVED | SIGNATURE: | DATE: |

**MANAGEMENT INFORMATION DEPARTMENT (NMOTC 09IS)**

**NMOTC VPN account has been established.**

| | | |
|---|---|---|
| ❑ APPROVED ❑ DISAPPROVED | SIGNATURE: | DATE: |