UNITED STATES
NAVAL HOSPITAL OKINAWA, JAPAN

FORM TITLE

ACCEPTABLE USE POLICY FOR USNHO INFORMATION TECHNOLOGY

TYPE OF ACCOUNT: (check one): ☑ **General User** (Review Section I) ☐ **Privileged User** (Review Sections I & II)

I. GENERAL USER

Ref:

(a) DOD 5500.07-R, "Joint Ethics Regulation (JER), Change 7", Chapter 2, Section 3, paragraph 2-301, November 17, 2011

(b) DoDI 8500.1, "Cybersecurity," March 14, 2014

(c) SECNAV M-5510.30 "Department of the Navy Personnel Security Program," June 1, 2006

(d) SECNAV MSG "Internet-Based Capabilities Guidance: Official Internet Posts," DTG 192027Z Aug 10

(e) SECNAV MSG "Internet-Based Capabilities Guidance: Unofficial Internet Posts," DTG 192031Z Aug 10

(f) DoDM 5200.01 (Vol 4) "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012

(g) DoDM 5200.01 (Vol 3) "DoD Information Security Program: Protection of Classified Information," February 24, 2012

(h) SECNAV M-5510.36 "Department of the Navy Information Security Program," June 2006

(i) SECNAVINST 5210.8E, "Department of the Navy Records Management Program," December 17, 2015

(j) NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," current edition

(k) SECNAVINST 5510.30B, "DON Personnel Security Program (PSP) Instruction," October 6, 2006

(l) CJCS M-6510.01, "Cyber Incident Handling Program," July 10, 2012

(m) OMB M-06-16, "Protection of Sensitive Agency Information," June 23, 2006

(n) DoDD 5400.11, "DoD Privacy Program," October 29, 2014

(o) DoDI 1035.01, "Telework Policy," April 4, 2012

(p) SECDEF Memo "Security and Operational Guidance for Classified Portable Electronic Devices," August 19, 2015

1. General Use

a. United States Naval Hospital, Okinawa (USNHO) IT users are every Service Member, civilian, contract support person, or local national with approved access to USNHO IT systems.

b. USNHO IT users must observe all policies and procedures governing the secure operation and authorized use of USNHO IT.

c. Policies, procedures, and restrictions within the SAAR-N are included in this document by reference.

d. Users of systems that impact financial statements will not only follow prescribed internal controls set by policies and procedures governing secure operation and authorized use of USNHO IT, they will also follow internal controls required per Federal Information System Control Audit Manual (FISCAM) audit methodology (available on the Department of Navy (DON) Chief Information Officer (CIO) website: http://www.doncio.navy.mil).

e. USNHO IT resources are provided for official use and authorized purposes only. Authorized purposes may include personal use within the limitations set forth in reference a. Personal use must not adversely affect the performance of official duties or degrade network performance, and must be of a reasonable duration and frequency as determined by commanding officers and supervisors. This includes personal communications from the USNHO IT users that are most reasonably made during the work day (such as checking in with spouse or minor children, scheduling doctor and auto or home repair appointments, brief Internet searches, emailing directions to visiting relatives, conducting on-line banking, distance learning, checking commercial email account, etc.). Non-emergency personal communications shall be made during personal time, such as after duty hours or lunch periods.

f. Users must not use USNHO IT to access inappropriate web sites or applications. Any questions regarding appropriateness of web sites or applications should be addressed to supervisors.

g. Users must not use USNHO IT in violation of the Hatch Act (5 U.S.C. §§ 7321-7326) which limits certain political activities of most federal executive branch civilian employees. Military personnel are similarly affected by DoDD 1344.10, which mirrors the Hatch Act. Any questions regarding prohibited behaviors should be addressed to the designated ethics official. Contractors and local/foreign nationals that are not bound by the Hatch Act are prohibited from using USNHO IT resources in similar manner, except where such guidance is countermanded by contracts or SOFA agreements. USNHO IT users must not:

(1) Engage in political activity while on duty or in the workplace. This includes partisan political social media posts, “likes,” shares, pictures, “tweets,” “re-tweets,” and sending email messages and links, etc., even when using an alias, personal social media account, or personal email account

(2) Send or forward partisan political communications via social media or email to a subordinate at any time.

(3) Engage in political activity in an official capacity at any time, or refer to official titles or positions while engaged in political activities. This includes using an official email account or a social media account created for use in an official capacity to engage in political activity.

(4) Suggest, solicit, or receive political contributions at any time. This includes sending or forwarding invitations to political fundraising events and providing links to partisan political contribution sites or pages.

(5) Forward partisan political emails received by a government account to anyone or any place other than their own personal email accounts.

h. USNHO IT users may not use official email addresses to sign up for non-official online services (e.g., adult content, newsletters, non-official social media accounts, etc.)

i. Information Technology Department (ITD) shall ensure required background investigations are completed commensurate with the level of USNHO IT access a user requires, per references b and c.

j. All USNHO IT users shall have approved DON system authorization access requests (SAAR-N) on file prior to being granted access to USNHO network.

k. USNHO IT users must not bypass, stress, or test cybersecurity (CS) or computer network defense (CND) mechanisms (e.g., firewalls, content filters, proxy servers, anti-virus programs, intrusion-prevention systems, etc.).

l. Users must not introduce or use unauthorized software, firmware, or hardware on any USNHO IT resource.

m. Users must not relocate or change equipment or the network connectivity of equipment without authorization from the Information Assurance Manager (IAM).

n. Users must not use personally owned hardware, software, shareware, or public domain software for official DON business without written authorization from the IAM.

o. Users must not upload or download executable files (e.g. .exe, .com, .vbs, .js, .bat, or .ps1) onto USNHO IT resources without the written approval of the IAM.

p. Users must not use USNHO IT to participate in or contribute to any activity resulting in a disruption or denial of service.

q. Users must not use USNHO IT to write, develop, compile, store, transmit, transfer, or introduce unauthorized or malicious software, programs, or code.

r. Users must not use USNHO IT resources in any way that would reflect poorly on the DoD, DON or USNH Okinawa. Such uses include, but are not limited to: pornography; chain letters; unofficial advertising; soliciting or selling (except on authorized bulletin boards established for such use); violation of treaty, statute, regulation or policy; inappropriate handling of classified information, personally identifiable information (PII) or personal health information (PHI); and other uses that are incompatible with public service.

s. Users must follow the specific guidance in references d and e to properly safeguard controlled unclassified information (CUI), including PII, PHI, and for official use only (FOUO).

t. Users must report all security incidents, including PII and PHI breaches immediately.

u. Users must not place data onto UNSHO IT resources whose security controls are insufficient to protect that data (i.e., data classified Secret may not be placed onto an unclassified network/asset).

v. Users must protect DoD/DON/USNHO Information and IT to prevent unauthorized access, compromise, tampering, exploitation, unauthorized or inadvertent modification, disclosure, destruction, or misuse.

w. Users must protect authenticators (e.g., passwords and personal identification numbers (PIN)) required for the logon authentication at the same classification as the highest classification of the information accessed.

x. Users must protect authentication tokens (e.g. common access card (CAC), alternate smart card logon (ASCL), personal identity verification (PIV), national security systems (NSS) tokens) at all times. Unattended tokens must be properly secured.

y. Users must virus-check all information, programs, and other files prior to uploading them onto any USNHO IT resource.

z. Users must access only that data, classified and unclassified controlled information, software, hardware, firmware for which they are authorized access, have a need-to-know, and have the appropriate security clearance. Users must assume only those roles and privileges for which they are authorized.

2. Training Requirements

a. Users must complete Cyber Awareness Training and HIPAA training for the current fiscal year prior to provisioning of their USNHO IT account. Refresher training must be completed annually. Failure to provide current training to USNHO SEAT or ITD will result in revocation of USNHO IT access.

b. USNHO IT users must complete derivative classification training prior to being granted initial access to USNHO classified IT and biennially thereafter.

3. Service Requests

a. Any request for service or support from authorized USNHO users to ITD must be submitted via Remedy through the Defense Health Agency (DHA) Global Service Center (GSC).

b. Technical support of an emergent nature that has a direct, immediate and unavoidable impact on patient care may bypass GSC ticketing by approval of the user's director or director-equivalent only. At no time, shall requests for password resets, account creation, or on-boarding be considered emergent needs under this clause.

c. Employees of ITD are not permitted to work on technical support issues that do not have a GSC ticket number without the express prior approval of the Department Head, ITD.

4. E-mail Use

a. Users must digitally sign e-mail messages requiring either message integrity or non-repudiation using DoD Public Key Infrastructure (PKI) or other approved method. All e-mails containing an attachment or embedded active content must be digitally signed.

b. Users must encrypt CUI/PHI/PII contained in e-mail in accordance with reference f. Examples of this are attachments that contain personal identity or budget information.

c. Use of commercial e-mail with unclassified content that does not require encryption for official government business is only permitted under the following conditions:

(1) Preapproval requirements:

(a) To meet an urgent operational requirement(s) wherein the user will not have access to unclassified USNHO IT systems (e.g., NIPRNET). This method is not authorized as a routine means.

(b) User must submit a request in writing and have it approved by both the IAM and the first field-grade officer in the user's chain of command, prior to using commercial email. The request must include the urgent operational requirement(s) and validation of compliance with the requirements in subparagraph (2) and (3) below.

(c) The CO and XO are considered sufficiently senior to pre-approve use of personal email when the conditions cited in (1)(a) above apply. However, they must still ensure compliance with the requirements in subparagraphs (2) and (3) below.

(d) A copy of the approval must be provided to the Deputy Under-Secretary of the Navy for Policy (DUSN(P)) Security for reference.

(2) Records generated:

(a) Once approval has been obtained per requirements in paragraph (i) above, USNH Okinawa personnel must include their official government email address on all email transmissions containing USNH Okinawa unclassified information. Transmitted USNHO unclassified information to any other commercial email address is prohibited.

(b) If unable to copy their official government email address, users must forward complete copies of the information to their official government email address within 20 days of the original creation or transmission of the record.

(3) Authorized (only when digitally signed and encrypted):

(a) Unclassified official government information that does not require safeguarding and dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies.

(b) Unclassified//For Official Use Only (U//FOUO) information, which is a type of controlled unclassified information (CUI). This includes FOUO information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended.

(4) Prohibited:

(a) Classified Information

(b) All other current types of CUI, such as Department of State Sensitive But Unclassified, Drug Enforcement Administration Law Enforcement, Unclassified Naval Nuclear Propulsion Information, Unclassified Critical Nuclear Weapons Design Information, National Geospatial-Intelligence Agency unclassified imagery or geospatial information, unclassified Technical Documents with Distribution Statement F or X, etc.

d. Users must not auto-forward official email from their official email accounts to commercial email accounts

5. Remote Access

a. Commanding Officer, USNHO, shall control remote access to USNHO IT.

b. USNHO ITD shall provide government-furnished computer equipment, software, and communications with appropriate security measures as the primary means for remote access for any regular and recurring telework arrangement that involves CUI.

c. USNHO ITD will ensure all remote access to DoD information systems and networks, including telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Use of encryption to protect the confidentiality of the session is required, per reference b.

d. USNHO ITD must ensure authentication and confidentiality requirements for remote access sessions use National Institute of Standards and Technology (NIST)-approved COMSEC and DoD PKI certificates for unclassified systems.

e. USNHO ITD will, when appropriate, require the use of Virtual Private Networks (VPNs) to protect and control internal and external access to USNHO information systems and networks, if a mission need for remote access is established. VPNs are the preferred method when using government-furnished or government-contracted equipment.

f. USNHO ITD and users must ensure all computers used for remote access have DoD-approved antivirus and firewall protection that includes the capability for automated updates per references b and j. The most current definitions and updates for these applications must be loaded before a remote access session is established.

g. USNHO IT administrators/privileged users must comply with the following requirements when accessing USNHO IT from outside of the enclave:

(1) Once USNHO ITD determines the mission need for remote access, they must establish approved VPN connections using government-furnished equipment under their user-accounts (with user privileges).

(2) After establishing a secure connection, elevate permissions to the appropriate level for conducting administrator tasks.

(3) Terminate connection when administrator tasks are complete.

(4) Safeguard information (i.e., do not access or display in an area where unauthorized persons are present) and control the equipment after connection termination per reference p.

6. Violations

a. Any violations of this policy may result in immediate termination of the user's account, at discretion of the IAM and/or CIO. In such cases where network access is a condition of employment, this may result in termination.

b. Any violations of this policy may result in revocation of the user's security clearance, at discretion of the adjudicating authority. In such cases where that clearance is a condition of employment, this may result in termination.

II. PRIVILEGED USER

1. Understanding and Consent. I understand, acknowledge and consent to the following:

a. I am responsible for all requirements stated in Section I above

b. I am responsible for all actions taken under my administrative, root, or superuser account(s) and understand that the exploitation of this account would have catastrophic effects to all networks for which I have access. I will only use the privileged access granted to me to perform authorized tasks for mission related functions. I will use my general user account at all other times.

c. I will protect the administrative, root, or superuser account(s) and authenticator(s) to the highest level of data or resource it secures.

d. I will not share the administrative, root, or superuser account(s) and authenticator(s) entrusted for my use.

e. I will not create or elevate privileged rights of others, share permissions to information systems not authorized, nor allow others access to information systems or networks under my privileged account

f. If I work in a capacity where I have rights to remotely log into users' systems, I will ensure they are positively informed of my presence prior to taking any actions on their system.

III. REQUESTOR

LAST NAME, FIRST NAME, MI	RANK/GRADE	DATE
SIGNATURE	**ORGANIZATION**	**TELEPHONE**