Acceptable Use Policy

Purpose

The purpose of the Acceptable Use Policy (AUP) is to establish acceptable practices regarding the use of Department of Defense (DoD) and National Defense University (NDU) information resources in order to protect the confidentiality, integrity and availability of information created, collected, and maintained. It is the responsibility of all personnel to know these guidelines and to conduct their activities accordingly. User consent and acknowledgement is required before accessing any DoD and NDU information resource and system.

Applicability

The AUP applies to authorized personnel who are granted access to DoD and NDU information systems and resources.

1. DoD Notice

The following is DoD's mandated notice and consent for all DoD information system users:

1. You are accessing a U.S. Government (USG) information system (IS) as defined in CNSSI 4009 (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

2. You consent to the following conditions:

a. 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.

b. At any time, the U.S. Government may inspect and seize data stored on this information system.

c. 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.

d. 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.

e. 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:

(1) 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.

(2) 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.

(3) 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.

(4) 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.

(5) 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.

(6) 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.

f. 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.

g. 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 provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

2. NDU Policy

NDU has established the following rules and user responsibilities to protect its personnel, information systems and resources, the DoD, and its partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.1. Acceptable Use

a. Personnel are responsible for complying with NDU policies when using NDU information systems and resources. If requirements or responsibilities are unclear, please seek assistance from the Information Technology Department (ITD).

b. Personnel must use NDU information systems for official use and authorized purposes only in accordance with DoD 5500.7-R Joint Ethics Regulation. Personnel must 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 NDU network, systems, other electrical and non-electrical equipment, or computing devices, if my actions are determined to be deliberate, willful, or malicious.

c. Introducing classified information into an unclassified system or environment is prohibited.

d. Personnel must protect Controlled Unclassified Information (CUI), which includes personally identifiable information (PII) under the Privacy Act, while it is being processed in or accessed from all computing environments.

e. Violating the established security, release, and protection policies for information identified as Classified, Proprietary, CUI, For Official Use Only (FOUO), or Privacy Act-protected during the information handling states of storage, process, distribution, or transmittal of such information and any other actions defined in the DoD 5500.7-R or any other DoD issuances is prohibited.

f. Personnel must sign the AUP every year after receiving NDU access.

g. Personnel are responsible for all actions taken under their NDU account(s) either as an authorized or privileged user and will not attempt to “hack” the network, any connected information systems, or gain access to data which I am not authorized to access.

h. 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 is prohibited.

i. Allowing any user access to NDU information systems or networks or any other connected system without prior approval or specific guidance from ITD Cybersecurity Management is prohibited.

j. Personnel must immediately report any harmful events or policy violations involving NDU assets or information, person suspected of engaging in, or any other 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 NDU Service Desk. Events include, but are not limited to, the following:

- Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to NDU information resources.
- Data incident: any potential loss, theft, or compromise of NDU information.
- Unauthorized access incident: any potential unauthorized access to a NDU information resources.
- Facility security incident: any damage or potentially unauthorized access to NDU owned, leased, or managed facility.
- Policy violation: any potential violation to this or other NDU policies, standards, or procedures.

2.2. Access Management

a. I understand I am the only authorized user of my NDU account.

b. Access to information is based on a need-to-know. Personnel must have requisite security clearance and/or documented authorization approved by their supervisor before accessing NDU information systems and resources.

c. Personnel must not attempt to access any NDU data, programs, or systems for which they do not have authorization or explicit consent.

d. Personnel must connect their Government-issued computer to the NDU network, either physically wired or through the NDU Virtual Private Network (VPN) while conducting NDU work to ensure it receives all necessary security patches and anti-virus updates. **I understand if my Government-issued computer falls out of cybersecurity compliance, my NDU account may be disabled.**

e. Personnel shall not divulge any access information to anyone not specifically authorized to receive such information, including IT support personnel.

f. Personnel must not share their personal authentication information, including:

- Account passwords
- Personal Identification Numbers (PINs)
- Security Tokens (i.e. Smartcard, Common Access Card (CAC))
- Multi-factor authentication information
- Access cards and/or keys
- Similar information or devices used for identification and authentication purposes

g. Access cards and/or keys that are no longer required must be returned to physical security personnel. Lost or stolen access cards, security tokens, and/or keys must be reported to physical security personnel as soon as possible.

h. Personnel must notify their supervisor and the NDU Service Desk when access to NDU information systems and resources are no longer required.

2.3. Cybersecurity Awareness Training

a. All new personnel must complete Joint Knowledge Online (JKO) cybersecurity awareness training prior to being granted access to NDU information systems and resources.

b. All personnel must complete cybersecurity awareness training annually.

2.4. Clear Desk/Clear Screen

a. Personnel should log off from applications or network services when they are no longer needed.

b. Personnel must log off from Government-shared computers prior to leaving the shared computer.

c. Personnel must remove their CAC and log off or lock their computer when their workspace is unattended.

d. CUI must be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.

e. File cabinets containing CUI must be locked when not in use or when unattended.

f. Physical and/or electronic keys used to access CUI must not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.

g. Laptops should be either locked with a locking cable or locked in a cabinet or office when the work area is unattended or at the end of the workday.

h. Passwords must not be posted on or under a computer or in any other physically accessible location.

i. Copies of documents containing CUI should be immediately removed from printers and fax machines.

j. All output (including printed materials, external drives, and media (e.g., compacts disks (CDs) must be appropriately labeled based on information sensitivity.

2.5. Email and Electronic Communication

a. Using NDU-provided identifiers (e.g., email addresses) and passwords for creating accounts on external sites/applications is prohibited.

b Using personal email or other nonofficial accounts to exchange CUI and official NDU information is prohibited.

c. Auto-forwarding electronic messages outside the NDU internal systems is prohibited.

d. Electronic communications should not misrepresent the originator or NDU.

e. Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.

f. Accounts must not be shared without prior authorization from ITD, with the exception of calendars and related calendaring functions.

g. Any personal use of NDU provided email must not:

- Involve solicitation
- Be associated with any political entity
- Have the potential to harm the reputation of NDU
- Participate in chain letters
- Contain or promote anti-social or unethical behavior
- Violate local, state, federal, or international laws or regulations
- Result in unauthorized disclosure of NDU confidential information.
- Violate any other NDU policies

h. Personnel should only send CUI using approved secure electronic messaging solutions.

i. Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.

j. Personnel should use discretion in disclosing CUI or internal information in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

2.6. Hardware and Software

a. All hardware must be formally approved by ITD Management before being connected to NDU networks.

b. Software installed on NDU equipment must be approved by ITD Management and installed by ITD personnel.

c. All NDU IT assets taken off-site should be physically secured at all times.

d. Personnel traveling Outside the Continental United States (OCONUS) and to High-Risk locations, as defined by the US Department of State, must contact ITD for approval five days before traveling with NDU IT assets.

e. Personnel should not allow family members or other non-employees to access NDU information systems or resources.

f. 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 is prohibited. This includes peer-to-peer file sharing software or games and BitTorrent services.

g. Installing, modifying, or removing any hardware or software without written permission and approval from ITD Cybersecurity Management is prohibited. This includes installing unauthorized software (e.g., freeware, shareware, security tools, games, entertainment software) and hardware (e.g., sniffers).

h. Introducing any unauthorized code, Trojan horse programs, malicious code, or viruses into NDU information systems or networks is prohibited.

i. Knowingly writing, coding, compiling, storing, and transmitting or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses is prohibited.

j. Removing or destroying system audit, security event, or any other logs without prior approval from the ITD Cybersecurity Management is prohibited.

2.7. Internet

a. The Internet must not be used to communicate CUI or internal information, unless the confidentiality and integrity of the information is ensured, and the identity of the recipient(s) is established.

b. Use of the Internet with NDU networking or computing resources must only be used for business-related activities. Prohibited activities include, but are not limited to:

- Recreational games
- Streaming media
- Personal social media
- Accessing or distributing pornographic or sexually oriented materials
- Gambling, wagering, or placing of any bets
- Attempting or making unauthorized entry to any network or computer accessible from the Internet
- 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 fund raisers, etc.).
- Or otherwise violate any other DoD or NDU policies

c. Access to the Internet from outside the NDU network using a DoD computer must adhere to all of the same policies that apply to use from within DoD and NDU facilities.

2.8. Mobile Devices and Bring Your Own Device (BYOD)

a. The use of a personally owned mobile device, or BYOD, to connect to the NDU systems and resources is a privilege. NDU reserves the right to revoke personally owned mobile device use privileges in the event that personnel do not abide by the requirements set forth in this policy.

b. All mobile devices must maintain up-to-date versions of all software, applications, anti-virus definitions, and security vulnerability updates.

c. Mobile devices that access NDU email must have a PIN or other authentication mechanism enabled.

d. CUI must only be stored on devices that are encrypted in compliance with the NDU encryption standards.

e. Theft or loss of any mobile device that has been used to create, store, or access CUI must be reported to the NDU Service Desk immediately.

f. Jail-broken or rooted devices should not be used to connect to NDU information systems.

g. ITD Management may choose to execute “remote wipe” capabilities for mobile devices without warning.

h. In the event there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the person’s possession as part of a formal investigation.

i. All mobile device usage in relation to NDU information systems and resources may be monitored, at the discretion of ITD Management.

j. ITD support for personally owned mobile devices is limited to assistance in complying with this policy and may not assist in troubleshooting device usability issues.

k. Use of personally owned devices must be compliant with all other NDU policies.

l. Personally owned devices (laptops, workstations, etc.) are prohibited from connecting to the NDU wired network.

2.9. Physical Security

a. Photographic, video, audio, or other recording equipment, such as cameras and cameras in mobile devices, are not allowed in secure areas.

b. Personnel must display photo ID access card at all times while in the building.

c. Personnel must badge in and out of access-controlled areas. Piggybacking, tailgating, door propping and any other activity to circumvent door access controls are prohibited.

d. Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel at all times.

2.10. Removable Media

Removable media (i.e., USB devices) use is not permitted on NDU IT assets.

2.11. Social Media

a. Creating any public social media account intended to represent NDU, including accounts that could reasonably be assumed to be an official NDU account, requires the permission of the NDU Strategic Communications Department.

b. Communications made with respect to social media must be made in compliance with all applicable DoD policy.

c. Personnel are personally responsible for the content they publish online.

d. Personnel approved to post, review, or approve content on NDU social media sites must follow the NDU MANUAL 8200.19, Standard Operating Procedure: Social Media Site Requests.

2.12. Voicemail

a. Personnel should use discretion in disclosing CUI or internal information in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.

b. Personnel should not access another user's voicemail account unless it has been explicitly authorized.

c. Personnel must not disclose confidential information in voicemail messages.

2.13. Waivers

Waivers for certain policy provisions may be sought by contacting ITD Cybersecurity Management.

2.14. Enforcement

Personnel found to have violated this policy 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 or contract(s)
- Related civil or criminal penalties

2.15. User Acknowledgement

I have read, understand, and will comply with the requirements set forth in this policy.

Name: _____ Date: _____

Signature:

_____