Army Reserve
Acceptable Use Policy (AUP)
for Access to CLASSIFIED / UNCLASSIFIED Systems

[The proponent agency is G-2/6.]

SECTION I - POLICY

1. Understanding.

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:

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

I understand that I have the responsibility to safeguard the information contained on the Army Reserve Network (ARNet), from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use. I further understand this responsibility extends to any and all Department of Defense information systems (IS) or networks.

2. Access.
Access to the SIPRNet, the unclassified ARNet, or any other DOD IS or network, is for official and authorized use as set forth in DOD 5500.7-R, (Joint Ethics Regulation), AR 25-1 (Army Knowledge Management and Information Technology), and AR 25-2 (Information Assurance).

3. Revocability.
I understand that, lAW AR 380-53, use of any Government owned computer constitutes consent to monitoring for security purposes and to ensure that my use is authorized. I understand that I have no expectation of privacy while using or accessing Government ISs or resources and that access to Government resources is a revocable privilege. I further understand that any information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.

4. Classified Information Processing.

a. I understand that the SIPRNET (Secret Internet Protocol Router Network) is the primary classified IS for the Army Reserve and that it: (1) is a US-only system approved to process SECRET or lower collateral information; (2) is not authorized to process TOP SECRET or higher information; (3) provides communications to external DoD organizations using the SIPRNet primarily via electronic mail and internal networking protocols such as web and ftp.

b. I will not introduce classified information to the NIPRNet or any other network not approved for classified processing. I understand that the introduction of classified information to an unclassified network is a security violation which will investigated and handled as a security violation or as a criminal offense resulting in possible punitive action. If I introduce or am aware of the introduction of classified information to an unclassified network (known as a spillage) I will immediately report the incident to my Information Assurance Security Officer.

c. I will protect my password as SECRET and will not disclose it to anyone, write it down, or transmit it electronically.

d. I will not enter, display, or process classified data where visible to unauthorized personnel.

e. I will protect all information on the SIPRNet as SECRET. Printed material and removable storage media, such as but not limited to diskettes, hard drives, and CDs, will be conspicuously marked and protected in accordance with AR 380-5, Information Security.

f. I will report any changes in my status, such as transfer, change in requirements for “need to know”, or removal of security access) to my Information Assurance Security Officer.

5. Unclassified Information Processing.
The ARNet is the primary unclassified information system for the Army Reserve.

a. The ARNet provides UNCLASSIFIED communication to external DoD and other US Government organizations. Primarily this is done via electronic mail and Internet network protocols such as but not limited to web, ftp, and telnet.

b. The ARNet is approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2.

c. The ARNet and the Internet, as viewed by the Army Reserve, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNet and Internet.

6. Minimum Security Rules and Requirements.
As a Government computer user, the following minimum security rules and requirements apply:

a. I will not be permitted access to any Government owned IS unless I am in complete compliance with the personnel security requirements set forth in DOD 5200.2R, AR 380-67 and AR 25-2.

b. I have completed the DoD Information Assurance Awareness Training module online at https://ia.gordon.army.mil/ia_courses.htm and I will participate in all required training programs directed by AR 25-2.

c. I will protect my CAC PIN, passwords, and pass-phrases lAW AR 25-2. Passwords will consist of at least 14 characters with 2 of each of the following: uppercase letters, lowercase letters, numbers, and special characters. Passwords will not consist of common names, User IDs, call signs, birthdays, phone numbers, military acronyms, or dictionary-based words. Accounts that have not been logged in to (inactive) for 60 days will be disabled. The account that has been inactive for 120 days will be deleted.

d. I will not reveal my CAC PIN, password, or pass-phrase to anyone nor will I store it on any IS or storage media or keep it in written form.

e. I understand that I am responsible for actions performed using my CAC PIN or User ID and password/pass-phrase. If I feel my CAC PIN, password or pass-phrase has been compromised, I will report it to my Information Assurance Security Officer (IASO) immediately.

f. I will use only authorized hardware and software.

g. I will not remove or relocate my computer without permission from my supporting Information Management Officer (IMO) or IASO.

h. I will not download, install or use any personally owned or public domain hardware, software, shareware or freeware on a Government owned computer.

i. I will perform virus-checking procedures before copying, downloading, or accessing information from any website, attachment, system, diskette, compact disk, thumb drive, or other removable device.

j. I will not attempt to access or process data exceeding the authorized classification level for the IS to which I am assigned, nor for which I do not have a "need to know." I understand that computers connected to the NIPRNet are NOT authorized for processing classified information. Under no circumstances will I interchange external media (i.e., CDs, floppy disks, or any other type media) between classified (SlPRNet) and unclassified (NIPRNet) systems.

k. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

l. I will not introduce executable code (i.e., .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

m. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

n. I will not utilize any Government owned IS for commercial or financial gain or illegal activities.

o. I will only permit computer maintenance by technicians authorized by the Army Reserve (i.e., Enterprise Customer Service Center (ECSC), local automation help desk personnel).

p. I will remove my CAC card and use screen locks to prevent unauthorized access to IS during periods of temporary non-use and will log off (NOT power off) when departing the area and at the end of the duty day.

q. I will report any suspicious output, files, shortcuts, links, or system problems to the ECSC, local automation help desk personnel, or supporting IASO, and will cease using the system immediately.

r. If I observe anything on the system I am using that indicates inadequate security, I will notify my IASO.

s. I will address any questions regarding policy, acceptable use, and my responsibilities to my IASO or to the USAR DCS G2/6 Information Assurance Division.

t. I understand that each IS is the property of the Army and is provided to me for official and authorized uses.

u. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

v. I understand that DOD and Army Reserve policy states that Federal Government communication systems and equipment, including but not limited to Government-owned or provided: computer hardware; firmware; peripheral equipment; software; media; telephones; facsimile machines; Internet connectivity; e-mail; and access to Internet services, when use of such systems and equipment is paid for by the Federal Government, will be for "official use" and "authorized purposes" only.

(1) I understand that: AUTHORIZED USE is any official or personal activity authorized to be performed by an individual in accordance with DoD Regulation 5500.7-R, Joint Ethics Regulation (JER), AR 25-2, Information Assurance, and AR 25-1, Army Knowledge Management and Information Technology Management.

(2) I understand that OFFICIAL USE is the activity directly related to the discharge of an employee's duties in the performance of the US Army Reserve (USAR) mission.

(3) I understand that UNAUTHORIZED USE is any use that: is illegal or prohibited by DoD and Army policy; would adversely reflect on DoD or the Army; disrupts or prevents authorized use; compromises privacy of other users; performs an unauthorized release of information; or that impairs the integrity of information processing, storage, or transmission capability. I understand that the following activities define unacceptable uses of an Army IS and that I will not --

(a) Use systems in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army, or violates standards of ethical conduct.

(b) Use systems for commercial purposes or in support of "for-profit" activities or in support of outside employment or other business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services), including using Government equipment or services to assist relatives, friends, or other persons in such activities.

(c) Intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (spam) communications to include sending sexually explicit e-mail or accessing sexually explicit web sites, pornographic images, or virtual computer generated or otherwise pornographic images.

(d) Introduce computer viruses to the system, send "letter bombs" (repeatedly mailing to an individual to deny that person access to mail service); create, copy, transmit or retransmit chain letters or other mass mailings (such as virus warnings, hoaxes, and chain letters) regardless of the subject; forward greeting cards, video, sound, or other large file attachments; engage in indiscriminate use of the "reply to all" feature in Outlook; visit inappropriate Internet sites; and load automatic data gathering technology on the internet and other continuous data streams (i.e., RealAudio, PointCast, CNN Live, WeatherBug), that degrade the performance of the entire network.

(e) Participate in on-line gambling or other activities inconsistent with public service.

(f) Use Government systems as a staging ground or platform to gain unauthorized access to other systems, or circumventing or compromising the security mechanisms of the network.

(g) Create, download, view, store, copy, or transmit materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities.

(h) Use Government equipment or service for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

(i) Engage in any fund-raising activity not authorized in accordance with JER, section 3-210, participate in any lobby activity, engage in any partisan political activity, or conduct the business of any non-Federal entity.

(j) Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that contradicts the agency's mission or positions or that could create the perception that the communications was made in one's official capacity as a Federal Government employee, unless appropriate agency approval has been obtained.

(k) Participate in the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data that includes privacy information; material that is copyrighted, trade-marked, or with other intellectual property rights (beyond fair use); proprietary data; or export controlled software or data.

(4) I understand that limited personal use of Government resources and communication systems by employees during non-work time may be authorized by the first supervisor who is a commissioned officer or civilian above GS/GM-11 when such use: involves minimal additional expense to the Government; is performed on the employee's non-work time; does not interfere with the USAR mission or operations; is reasonable in duration and frequency; serves a legitimate public interest; does not reflect adversely on Department of the Army or the United States Army Reserve; does not over burden the communication systems; and does not violate the JER. I understand the privilege to use Government resources and communication systems for non-Government purposes may be revoked or limited at any time by the first supervisor as defined above or any superior of the first supervisor. Some examples of authorized personal uses are:

(a) checking in with spouse or minor children;

(b) scheduling doctor, auto or home repair appointments; and

(c) brief Internet searches or e-mailing directions to visiting relatives.

(5) I understand that unauthorized use of Government equipment or services could result in any or all of the following sanctions: loss of use or limitations on use of equipment or services, disciplinary or adverse actions, criminal penalties, and employees being held financially liable for the cost of unauthorized use.

SECTION II - ACKNOWLEDGEMENT

I have read the above requirements regarding use of U.S. Government information systems and I understand my responsibilities regarding use of these systems and the information contained in them.

Command/Activity: _____

Name (Last, First, MI): _____

Grade/Rank: _____ Phone #: _____

Signature: _____ Date: _____