Army Reserve Network (ARNet) Privileged-Level Access and Acknowledgement of Responsibilities Agreement

(The proponent agency is G-2/6)

Privileged Access is the authorized access that provides a capability to alter the properties, behavior, or control of the information system or network. It includes, but is not limited to, any of the following types of access:

- "Super user," "root," or equivalent access, such as access to the control functions of the information system or network, administration of user accounts, and so forth;
- Access to change control parameters (for example, routing tables, path priorities, addresses) of routers, multiplexers, and other key information system or network equipment or software;
- Ability and authority to control and change program files, and other users' access to data;
- Direct access (also called unmediated access) to functions at the operating-system level that would permit system controls to be bypassed or changed; or
- Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems or networks (for example, network or system analyzers; intrusion detection software; firewalls) or in performance of cyber or network defense operations.

SECTION I. AGREEMENT

1. I understand that I have access to the US Army Reserve Network (ARNet) UNCLASSIFIED Army Information System (IS), and that I have and will maintain the necessary clearances and authorizations for privileged-level access to (specify what IS privileges are being granted):

□ **OUAdmin** - *accumulative of all the rights in the sample Field Operating Agency (FOA) Organizational Unit (OU). Additionally controls the test OU. The OU administrator is a member of all other FOA administrative groups.*

□ **SysAdmin** - *manage all member servers within the server OU in the FOA.*

□ **PrtMgt** - *print manager.*

□ **DeskMgt** - *manage all computers within the Laptop and PC OUs in the FOA.*

□ **NameSvr** - *read only all Windows Internet Naming Service/Dynamic Host Configuration (WINS/DHCP).*

□ **UserGrpMgt** - *manage all user accounts and groups in the FOA under ARUser organizational unit.*

□ **GPOMgt** - *administer the Group Policy Objects (GPO) for the sample FOA and the TESTGPO linked to the test OU.*

□ **Helpdesk** - *limited user management permissions such as reset password, disable/enable accounts, and change to properties tab information.*

□ **TrngAdmin** - *manage the training OU computers, users, and groups.*

2. I understand that I am required to perform my responsibilities in accordance with policy and procedures set forth in AR 25-2, Information Assurance, for IA Support Personnel/System Administrators.

3. As a privileged-level user:

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

b. I will NOT share the root, administrator, or superuser account(s) and authenticator(s) entrusted for my use.

c. I will ONLY use the special access or privileges granted to me to perform authorized tasks or mission related functions. I am responsible for all actions taken under my account and understand that the exploitation of this account would have catastrophic effects to all networks for which I have access. I will only use my privileged account for official administrative actions.

d. I will not attempt to "hack" the network or connected ISs, subvert data protection schemes, gain, access, share, or elevate permissions to data or ISs for which I am not authorized.

e. I will protect and label all output generated under my account to include printed materials, magnetic tapes, external media (i.e., CDs, floppy disks, USB drives), system disks, and downloaded files.

f. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of system or network services, illegal or improper possession of content or files, or the actual or possible compromise of data, files, access controls, or systems to my activity Information Assurance Security Officer (IASO) or to the USAR G2/6, Information Assurance Division.

g. I will NOT install, modify, or remove any hardware or software (i.e., freeware/shareware, security tools, etc.) without permission and approval from my activity Information Assurance Security Officer (IASO) or to the USAR G2/6, Information Assurance Division.

h. I am prohibited from obtaining, installing, copying, pasting, modifying, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade-secret, or license agreements.

i. I will not create or elevate access rights of others; share permissions to ISs for which they are not authorized; nor allow others access to IS or networks under my privileged account.

j. I am prohibited from casual or unofficial web browsing and use of email while using the privileged-level account. This account will NOT be used for day-to-day network communications.

k. I am prohibited from accessing, storing, processing, displaying, distributing, transmitting and viewing material that is; pornographic, racist, defamatory, vulgar, hate-crime related, subversive in nature, or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, national, or international law.

l. I am prohibited from storing, accessing, processing, sharing, removing, or distributing Classified, Proprietary, Sensitive, Privacy Act, and other protected or privileged information that violates established security and information release policies.

m. I am prohibited from promoting partisan political activity, disseminating religious materials outside an established command religious program, and distributing fund raising information on activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g., command social-event fund raisers, charitable fund raisers, etc.).

n. I am prohibited from using, or allowing others to use, Army resources for personal use or gain such as posting, editing, or maintaining personal or unofficial home pages, web-blogs, or blogging sites, advertising or solicitation of services or sale of personal property (e.g., eBay) or stock trading.

o. Unless required to perform assigned duties, I am prohibited from employing, using, or distributing personal encryption or decryption capabilities for official electronic communications.

p. I will contact my activity Information Assurance Security Officer (IASO) or the Army Reserve DCS, G2/6, Information Assurance Division if I am in doubt as to any of my roles, responsibilities, or authorities.

q. I will maintain IAVM compliance on all ISs to which I have privileged-user access.

r. I will obtain an account in the Army Training and Certification (ATC) Tracking System located at https://atc.us.army.mil .

s. I will obtain and maintain required certification(s) in accordance with Army policy set forth in AR 25-2 and supplementing Best Business Practice (BBP), Information Assurance (IA) Training and Certification, 05-PR-M-0002, to retain privileged level access and update the ATC Tracking System.

t. I understand that failure to comply with the above requirements is a violation of the trust extended to me for the privileged access roles and may result in any of the following actions:

(1) Chain of command revoking IS privileged access and/or user privileges

(2) Counseling

(3) Adverse actions under the UCMJ and/or criminal prosecution

(4) Discharge or Loss of Employment

(5) Revocation of Security Clearance

u. I understand that the terms of this agreement are in addition to any and all other promises of confidentiality that I may have executed with the government (such as those contained in Standard Form 312).

NAME: ____ DATE: ________________

SIGNATURE: ____

IA Manager (IAM):____________________________________ DATE: __________________

IAM SIGNATURE: ____________________________________

SECTION II. CERTIFICATE OF NON-DISCLOSURE OF PROTECTED OR PRIVILEGED INFORMATION

Whoever, being an officer, employee or agent of the United States or of any department, agency or contractor thereof, publishes, divulges, discloses or makes known in any manner or to any extent not authorized by law, any information coming to him/her in the course of their employment or official duties, which information concerns or relates to the trade secrets or proprietary information of a non-Federal government entity; any information protected by the Privacy Act; any information subject to protection under the Freedom of Information Act; other law, regulation, or policy (including all privileged communications such as doctor-patient, attorney-client, etc.); any information protected under the classification system set forth in AR 380-5; or any other information protected by law or regulation (i.e. IG, AAA, CID); shall, in addition to any penalty imposed by said law or regulation, be subject to UCMJ, administrative, or contract remedy enforcement.

CERTIFICATION

I have read the above provisions. I understand my responsibility not to disclose any matters related to these provisions and the Army Reserve Network (ARNet), except to authorized persons having a need to know. I further acknowledge that failure to comply with these rules could lead to disciplinary action against me.

NAME: ____ DATE: ____________________

SIGNATURE: ____