Department of the Army
Headquarters, United States Army Reserve Command
1401 Deshler Street SW
Fort McPherson, GA 30330-2000
1 August 2000

USARC Memorandum 25-70

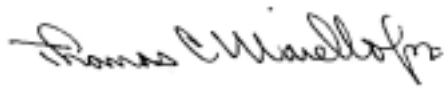
Information Management: Automation

U.S. Army Reserve Command Network Security

For the Commander:

ROBERT B. OSTENBERG
Brigadier General, USAR
Acting Chief of Staff

Official:



THOMAS C. MAIELLO, JR.
Colonel, GS
Army Reserve Chief Information Officer

History. This is the initial printing of USARC Memorandum 25-70.

Summary. This memorandum prescribes network security policy and procedures, as it pertains to the operation, use, and administration of the USARC Headquarters' networks. It also establishes the basis for using network information services and security mechanisms, responsibilities of all persons with network access, and acceptable and prohibited practices and procedures for use of the network and network-accessible resources.

Applicability. This memorandum applies to all assigned or attached U.S. Government and contractor personnel within the Headquarters, USARC, who access or use the government networks and computers.

Suggested improvements. The proponent of this memorandum is the Army Reserve Information Systems Services Directorate (ISSD), Chief Information Office (CIO). Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Commander, U.S. Army Reserve Command, ATTN: AFRC-CIS-S, 1401 Deshler Street SW, Fort McPherson, GA 30330-2000.

Distribution. C

Table of Contents

Chapter 1
Introduction

1-1. Purpose.
This memorandum provides guidance, policies, and procedures pertaining to USARC Network Security with the intent to safeguard the confidentiality, integrity, use, and availability of the network, its components, and the information and data on it. Persons violating policy contained herein may be denied access to the networks and may be subject to criminal, civil, administrative, judicial, or non-judicial proceedings or sanctions. This memorandum will be revised as technical procedures are developed and implemented to safeguard the networks, or to meet new requirements and changing risks. It is available in either hardcopy or electronic format to all network users. The CIO Publications Distribution Center maintains stock of hard copies and the electronic version (Acrobat Reader PDF format) is accessible on the "usarcshared/readonly" drive in the "Hqpubs" folder, as well as through the Intranet using the "Pubs, Forms & Misc Materials" link.

1-2. References.
Required and related publications and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms
Abbreviations and special terms used in this memorandum are explained in the glossary.

Chapter 2
Responsibilities

2-1. Responsibilities of personnel with automated information systems access

a. **All users.** Users (all U.S. Government and contract personnel with access to USARC information systems) are the functional proponents and have primary responsibility for the security implications (OPSEC, INFOSEC, etc.) of their data. Functional proponents are responsible for keeping information on the network, to include Web pages and home pages, timely, up-to-date, as accurate as practical, and for ensuring it reflects the organization's missions and functional needs. ***All users will--***

(1) Read and provide the Information Assurance Network Manager (IANM) with a signed copy of USARC Form 75-R, Information Systems Security Briefing (see USARC Reg 380-2), prior to receiving the initial sensitive but unclassified (SBU) network UserID and Password. Failure to sign this form will result in denial of access. The form is available from the IANM or the designated representatives. It is also available on the "usarcshared/readonly" drive in the "Forms" folder and is accessible through the Intranet using the "Pubs, Forms & Misc Materials" link.

(2) Provide the IANM with a completed AFRC Form 48-R, Classified Network Password Request Form, and sign the Information Systems Security Briefing, to obtain access to the classified network. The form is on the "usarcshared/readonly" drive in the "Forms" folder and is accessible through the Intranet using the "Pubs, Forms & Misc Materials" link.

(3) Maintain up-to-date anti-virus software and comply with established procedures in treating information system (IS) contamination (e.g., computer viruses and hoaxes).

(4) Not attempt to access files, databases, and other information to which they are not granted access.

(5) Not place any classified data or information on the SBU network or computers.

(6) Not conduct or perpetuate an illegal act on networks, nor any activity that can discredit, inhibit, impair, or disrupt the authorized users of networks. Prohibited conduct also includes hacking; attempting to void or avoid network security mechanisms; distributing computer viruses or hoaxes; intentional destruction of official records; and activities that may reasonably be expected to cause embarrassment or bring discredit to the user, the Army, or U.S. Government.

(7) Immediately report to the IANM any known or suspected intrusions or violations of the security policies.

(8) Inform the USARC Customer Service Center whenever a workstation appears to be malfunctioning or may be infected by a computer virus.

(9) Contact the IANM prior to departing or after changing organizations within the Headquarters USARC, to ensure appropriate modification of network permissions.

(10) Back up all mission-essential files on their workstation through the use of diskettes, local back up tape drives, or by copying the files to a network server.

(11) Not respond to any survey conducted by mail, phone or computer, unless specifically authorized by this Headquarters.

(12) Not, at any time, leave a modem or any data transmission device, connected to a telephone line and unattended.

(13) Not write down or share passwords.

(14) Log-off the system and turn off the monitor at the end of the duty day.

(15) Complete the Web-based Information Assurance User Awareness Training located at http://usarcintra/iss within 30 days of receipt of their UserID and password. Complete the annual Information Assurance User Awareness refresher training.

(16) Update anti-virus software and signature files as required by the Information Assurance Office.

(17) Lock the computer whenever out of visual range of the computer (See paragraph 3-6).

(18) Use only CIO-approved hardware and software.

(19) Change their password prior to departing for any extended leave or TDY to preclude user's account from expiring, while user is absent. If leave or TDY is expected to be longer than 6 months, the procedures for "Remote, Dial-In Users" apply.

b. Remote, Dial-In Users. These users include all dial-in users outside the geographic area of the Headquarters, USARC. These users will comply with all the requirements in this memorandum, and must have an organizational sponsor within the Headquarters, USARC. The sponsor is responsible for validating the need for the remote user to access specific SBU network resources. Remote, dial-in users may not change their own passwords. ***All remote, dial-in users will--***

(1) Submit requests for remote access to the USARC network in writing to the IANM. (The IANM will not accept electronic submissions). The request must include the following information:

(a) Requester's full name.

(b) Organization name, to include division, branch, etc.

(c) Mailing address.

(d) Commercial phone number, to include area code.

(e) Fax number.

(f) Electronic mail (E-mail) address (if available).

(g) Two items of identifying information (e.g., mother's maiden name, sister's date of birth, key words, or something probably known only to the applicant).

(h) Justification for access.

(i) Specific access requirements (e.g., E-mail applications, shared files, etc.).

(j) The name and phone number of the sponsor within the appropriate Headquarters, USARC functional area(s) to obtain approval for access to the network files or applications.

(k) Name and telephone number of site Security Manager.

(3) Call the IANM to activate the account, upon receipt of their UserID and password.

(4) Request a new password 3 weeks prior to the expiration of the password to allow time for processing and mailing. (Passwords for remote users expire 6 months (180 days) from issuance.) The user must call the IANM to request a new password. Following confirmation of the user's identity, the IANM will mail the new password to the user. Upon receipt of the new password, the user must call the IANM to activate the new password.

(5) Comply with all requirements listed in paragraph 2-1a upon obtaining access to the network.

c. Government Contractors and Service Providers. Contractors, systems developers, other vendors, and service providers have the same responsibilities as all users (see para 2-1a), plus the responsibility to deliver, develop, install, integrate, test, evaluate, and certify that their hardware, software, and services comply with this memorandum. With prior written approval from the CIO, qualified persons may work with (or for) System Administrators to demonstrate and conduct operations, maintenance, experiments, and tests that would otherwise be in violation of the security policy.

2-2. Responsibilities of information systems security personnel

a. Information Assurance Program Manager (IAPM). The IAPM will establish and implement the IA program (IAP) for all information systems within the Command. For systems within their purview, ***the IAPMs will--***

(1) Oversee the execution of the IA training and awareness program.

(2) Ensure the appointment of appropriate Information Systems Security personnel for each separate information system, group of information systems, or network, as necessary.

(3) Establish an IAP that will provide protection for all information systems and that will ensure all information systems and networks are accredited per this memorandum.

(4) Periodically review the status of all information systems and networks to ascertain that no changes have transpired that affect security and negate the accreditation.

(5) Review threat and vulnerability assessments to enable the commander or manager to properly analyze the risks to the information systems and to determine appropriate measures to effectively manage those risks.

(6) Report security incidents and technical vulnerabilities per this memorandum and AR 380-19. Immediately report all attempts and actual penetrations of Army information systems to the IAPM. In turn, the IAPM will notify the Land Information Warfare Agency (LIWA), who will notify HQ CID and the Army Case Control Office (ACCO) at INSCOM of all successful penetration incidents. Also, notify the local supporting CID and INSCOM office. Implement the Department of Defense Information Systems Security (DoDIIS) Computer Security (COMPUSEC) program and site based accreditation, where feasible.

(7) Establish the scope of responsibilities for information assurance managers (IAMs) using guidance from applicable regulations.

b. Information Assurance Network Manager (IANM). The IANM is responsible for the overall security of the networks, and coordinates the security operations of all Information Systems Security Liaisons (ISSL). In accordance with AR 380-19, the IANM reviews all incident reports, and, in cooperation with other security and investigative personnel, is responsible to advise and report to the Commander. ***The IANM will--***

(1) File reports and coordinate with other appropriate agencies, to include information exchange with HQDA Information Security officials, IAPM, and the Army Computer Emergency Response Team (ACERT) concerning response to perceived threats, increasing vulnerabilities, or observed security violations.

(2) Develop network security implementation procedures for all networks within the Headquarters.

(3) Develop and issue network security guidance and countermeasure implementation instructions to assigned Headquarters information management officials.

(4) Ensure that all networks within the Headquarters, including tenant networks accessing the host infrastructure, are planned, installed, managed, and maintained per the security requirements of this memorandum.

(5) Ensure that all networks within the Headquarters are properly accredited at appropriate sensitivity levels.

(6) Coordinate with IAPM and Network Managers to ensure that all information systems connected to the USARC Headquarters networks are properly accredited and operated to the standards required for connectivity to the network concerned.

(7) Establish and implement a system for issuing, protecting, and changing system passwords. Establish the user account and issue the initial UserID and Password to each person, including remote users, who will access SBU or classified networks.

(8) Monitor, review, and archive network audit trails and resolve discrepancies. Retain archived audit logs for 6 months.

(9) Report actual or suspected security incidents and technical vulnerabilities in accordance with AR 380-19.

(10) Maintain a copy of system security credentials issued to or from other computer systems in an approved security container. (Retain for 6 months after the credential is terminated) .

(11) Maintain a copy of USARC Form 75-R, Information Systems Security Briefing, for each person with network access. Retain forms for 6 months after a person's access to the network expires.

(12) Promptly report automated information system incidents (to include virus attacks, intrusions or attempted intrusions, and technical vulnerabilities) directly to the Land Information Warfare Activity's (LIWA) Army Computer Emergency Response Team Coordination Center (ACERT/CC) and the IAPM. Contact the ACERT/CC by commercial telephone, toll free 1-888-203-6332 (STU-III), non-secure FAX at commercial (703) 806-1003, secure FAX at commercial (703) 806-1004, or E-mail acert@vulcan.belvoir.army.mil. Initial reports should include, at a minimum, the name and location of the reporting unit/organization, system(s) affected, a brief description of the incident, actions taken, and the name and phone number of a point of contact. The ACERT/CC will provide guidance on further reporting requirements, if any. Provide a copy of all information reported to ACERT/CC, written or telephonic, to the USARC DCSINT, ATTN: AFRC-INS. Initially classify reports of technical vulnerabilities at least CONFIDENTIAL and ensure they contain information specified in AR 380-19.

(13) Review and evaluate the security impact of system changes, including interfaces with other information systems.

(14) Ensure that all interconnected systems comply with the security requirements levied within the infrastructure and do not have a negative security impact on any other systems with which they must interact and support.

(15) Ensure systems operation and maintenance is in accordance with AR 380-19, USARC Regulation 380-2, and this memorandum.

(16) Ensure managers, system administrators, and users have the appropriate security clearance, authorization, and need-to-know.

(17) Include all personnel associated with IS in system-specific and general awareness security training.

(18) Conduct threat and vulnerability assessments to enable the commander or manager to properly analyze the risks to IS information and determine appropriate measures to effectively manage those risks.

(19) Prepare, distribute, and maintain plans, instructions, guidance, and standing operating procedures (SOP) concerning the security of system operations.

(20) Prepare or oversee the preparation of the certification and accreditation documentation.

(21) Maintain a current network or IS certification or accreditation statement and initiate re-certification and re-accreditation when changes affecting security have occurred.

(22) Ensure that only authorized personnel can gain access to the system.

(23) Ensure appointment of individuals, as needed, for securing each terminal, workstation, computer, or associated group of computers that are not under the direct control of the IANM.

(24) Maintain close liaison with supporting system administrators to promote security at all levels of IS operations.

(25) Ensure the security firewall physically protects the SBU network and restricts administration access to system administrators and specifically designated personnel.

(26) Ensure SBU network resources are protected behind the firewall (workstation and server security, backups, physical security, etc.).

(27) Manage the local security and administration mechanisms of SBU network resources behind the firewall.

(28) Test, evaluate, and ensure there are no backdoors or other entry points that will circumvent or negate the security provisions in this memorandum.

(29) Identify restrictive information flows coming and going out of the SBU network (e.g., retrieving binary files or executables, sending E-mail/ posting to news groups, posting queries) via connections to the Non-classified Internet Protocol Router Network (NIPRNET) and Internet, and internal to the Sensitive but Unclassified (SBU) network.

(30) Review and approve firewall configuration and technologies. Document configuration in writing to the designated approving authority (DAA) and maintain the documented configuration approved by the Commander.

(31) Assist in conducting investigations and preparing reports concerning the use, and possible misuse, of the networks.

(32) Evaluate the security impact of all new software prior to installation.

c. Information Systems Security Liaisons (ISSL). Information Systems Security Liaisons (ISSL), formerly known as Terminal Area Security Officers (TASO), are responsible for implementing risk management procedures and network security mechanisms under direction of the IANM. They oversee the physical features for the hosts and facilities they manage, and implement management directives and awareness programs for the administrators and users of their hosts and facilities. Appointed within each functional area, ***the ISSL will--***

(1) Complete the ISSL training.

(2) Ensure systems within their area of responsibility are operated and maintained according to regulatory requirements.

(3) Ensure all personnel within their area of responsibility complete the Information Systems Security Awareness Training annually.

(4) Prepare or oversee preparation of accreditation documents for all computer systems within their area of responsibility, as appropriate.

(5) Distribute and implement plans, instructions, guidance, and procedures concerning the security of system operations.

(6) Maintain close liaison with IANM to promote security at all levels of automated information systems operations.

2-3. Responsibilities of network management personnel Network management personnel are responsible for operating, maintaining, backing-up and restoring network capabilities, and for the technical implementation of security measures. They advise the IANM on the effectiveness of, and improvement to, existing security measures and respond to emergency events (server failures, computer viruses, etc.) in a prompt, efficient manner. When appropriate, inform users and managers of changes or new developments to the networks.

a. System Administrators (SAs).

(1) The two main goals of the SAs are to keep the information system (IS) operational and the system secure. At all times, each SA also is responsible for judiciously exercising privileges inherent in their duties, to include complying with the Privacy Act, ensuring that appropriate security is established, and that operational procedures are followed to ensure continued system operation and data integrity. ***The SA will--***

(a) Notify the IANM prior to implementing changes to the network architecture.

(b) Ensure the operating system for the IS is configured properly and that the security features appropriate to the intended level of system operation are properly set. Periodically review such settings. These reviews will not involve looking at information or data contained in the files of individual users, other than system configuration files.

(c) Test, evaluate, and demonstrate specific authorized technical capabilities that are outside this memorandum. Document the tests, evaluations, demonstrations, and system and network configurations in writing to the IANM.

(d) Use approved C^2 protect tools to periodically review system security. These may be security utilities provided with network software. At no time use these utilities to review user data, even if the tool is capable of this function. The C^2 protect tools are approved by DISC4.

(e) Periodically check with the operating system manufacturer, the LIWA, or the DISC4 to keep informed of system security problems and patches as they are developed. Apply them as appropriate to maintain IS security.

(f) Ensure audit software configuration is in accordance with this memorandum.

(g) Review file names, length, permissions, and directories. If any of this information leads to suspicion

that an individual user is misusing the system or engaging in other misconduct, notify the IANM and IAPM concurrently. At no time specifically target or track an individual's activities except as part of a properly authorized investigation.

(h) If suspecting an attempt to access the IS by an unauthorized user, take the actions necessary to verify and limit the penetration attempt. Once verified, notify the chain of command, IANM, and IAPM concurrently. The appropriate individual within the chain of command will contact LIWA/ACERT, CI and CID. The SA may make system backups of appropriate log, history files, and user directories. The SA will not in any other manner specifically target, track or attempt to investigate a suspected intruder's activities, except as part of a properly authorized investigation.

(2) The SA does not have unlimited authority in operating the IS. While security of the system is an important component of the SA's job, there are restrictions on actions an administrator may take to accomplish the security function. The SA is not authorized to view, modify, delete or copy data files stored on the IS that are not part of the operating system, *except when*--

(a) Authorized by the user or file owner. The SA will inform the user of any modifications to his or her data access permissions within 24 hours.

(b) Performing system backup and disaster recovery responsibilities.

(c) Performing anti-virus functions and procedures.

(d) Performing actions necessary to ensure the continued operation and system integrity of the IS.

(e) Performing actions as part of a properly authorized investigation.

(3) The SA may intercept, retrieve, or otherwise recover an E-mail message upon written or verbal authorization of the parties involved, or as part of a properly authorized investigation. When the SA must remove an E-mail message that is interfering with the operation of the IS, they will make reasonable effort to notify the originator of the E-mail.

(4) The SA may not browse, modify, or delete user data without either the user's permission. The SA will inform the user of any modifications or deletions to the data via E-mail within 24 hours.

(5) The SA may not transmit sensitive information (e.g. user passwords, configuration data, root passwords, etc.) on the networks. Recommend use of a standalone or classified system to store this type of sensitive information.

(6) The SA may not modify or delete audit information on the status of the networks, except with the permission of the IANM.

(7) The SA is not authorized to use "hacker" techniques in an attempt to penetrate their IS. These techniques include, but are not limited to--

(a) The use of Network Analyzers, "Sniffers," or similar network monitoring systems to monitor the activities of specific system users. The use of these devices is authorized to perform valid system troubleshooting and diagnostics of network problems.

(b) "Keystroke monitoring" software of any kind. This will not be used either resident on the user's computer or by monitoring computer network communications.

(c) The use of keyboarding or automated techniques to exploit or verify vulnerabilities identified by the C^2 protect tools.

(d) Management Searches. In the absence of a user, the SA may grant the user's supervisor temporary access to the user's data files, in order to allow access to data for official purposes. *When such access is granted*--

-- The SA will brief the supervisor as to the limits of accessing the user's data files. This will include a warning to limit the search in scope to those files that could reasonably be related to the objective of the search (e.g., E-mail access would not be reasonable when searching for a word processing file).

-- Limit searches to the time necessary to locate the required data. Such access will not be used to circumvent regulatory or statutory requirements for investigations. The SA may provide technical assistance as requested by the investigating agent, when part of a properly authorized investigation.

b. Network Administrators (NAs). Network Administrators operate under similar broad authority and restrictions as the SA. While it is their responsibility to keep the networking infrastructure operational and secure, they operate under the same constitutional and statutory controls as the SA. These limits represent a balance between the actions necessary to provide a reliable and secure communications backbone for IS, while at the same time ensuring the privacy rights of the users. It is the goal of the NA to ensure the continued operation infrastructure is composed of two major components -- the communications medium (e.g., wiring, fiber optics, etc.) over which the IS communications travel; and the network hardware (e.g., hubs, concentrators, etc.) that makes up the physical equipment of the network. ***The NAs will--***

(1) Ensure proper configuration of all hardware and software components of the network infrastructure and that security features and controls appropriate to the intended level of system operation are properly set. Periodically review such settings to ensure they are set correctly and have not been modified without the NA's knowledge.

(2) Only use approved C^2 protect tools to periodically review network security. These may be security utilities provided with network software. At no time use the utilities to review user data, even if the tool is capable of this function. The general use of these tools will be to map the network and to conduct automated scans of individual machines for configuration errors that could lead to unauthorized access to individual machines or the network. The C^2 protect tools are approved by DISC4.

(3) Periodically check with the maker of the network components, the LIWA or the DISC4 to keep informed of system security problems and patches as they are developed. Apply them as appropriate to maintain the integrity of the network. Use Network Management Systems to monitor the operational status of the network and to collect statistics on bandwidth use and error rates.

(4) If suspecting misuse or misconduct by an individual user, or an attempt to access a system on the network by an unauthorized user, notify the chain of command and contact LIWA/ACERT concurrently. The appropriate individual within the chain of command will contact CI and CID. The NA will not specifically target, track, or attempt to investigate a suspected intruder's activities, except as part of a properly authorized investigation.

(5) Use "Sniffers" or network analyzers only as tools in diagnosing network problems (e.g., to identify the source of bad ETHERNET packets).

(6) Comply with the following restrictions in the normal performance of their duties:

(a) The NA is NOT authorized to view, modify, delete, or copy user data files in transit on the network or stored on an IS, unless one of the following apply:

-- Authorized is granted by the user or file owner.

-- It is incidental to performing diagnostics functions to correct network problems.

-- It is incidental to performing actions that are necessary to ensure the continued operation and system integrity of the network.

(b) The NA is NOT authorized to use "hacker" techniques in an attempt to penetrate their networks. These techniques include, but are not limited to--

-- The use of Network Analyzers, "Sniffers," or similar network monitoring systems to monitor the activities of specific system users. The use of these devices is authorized only to perform valid system troubleshooting and diagnostics of network problems.

-- "Keystroke monitoring" software of any kind. This will not be used either resident on the user's computer or by monitoring computer network communications.

-- The use of keyboarding or automated techniques to exploit or verify vulnerabilities identified by the C^2 protect tools.

(c) The NA may provide technical assistance as requested by the investigating agent, when part of a properly authorized investigation.

2-4. Responsibilities of Customer Service Center (CSC)

a. The Customer Service Center is responsible maintaining the hardware, software and security configuration of all the desktop and portable computers within the Headquarters, USARC in accordance with established regulations, policies, and guidelines.

b. The CSC will:

(1) Install and configure all approved software.

(2) Install and maintain hardware configurations.

(3) Maintain the security configuration.

(4) Create new user accounts and assist users in changing their passwords on the sensitive but unclassified network as required.

2-5. Responsibilities of Webmasters

a. The Webmaster is responsible for ensuring that information on the Web site is kept up-to-date and clearly reflects the stated purpose of the service. The Webmaster will coordinate site development with the IANM and USAR Webmaster prior to implementation.

b. Webmasters will ensure their staff Director or Chief prepares an appointment letter to identify the Webmaster and an alternate. The CIO will train these personnel as required.

c. Each USARC Web site must have an identified Webmaster. The Webmasters will--

(1) Develop and maintain professional appearance of their Web pages.

(2) Establish procedures for required updates to page content.

(3) Verify all files (messages, data, images, or programs) are virus free, in accordance with AR 380-19, prior to posting to the Web site.

(4) Establish procedures to ensure that classified information, or information that could enable the recipient to infer classified information, either from individual segments of the information or from the aggregate of the information, is not posted to the Web Site.

(5) Be responsible for the information content on their Web sites.

(6) Keep information on Web pages current and accurate.

(7) Keep within the format and content guidelines specified in DOD, DISC4, DA, and USARC policy. (Limit content to official government information only.)

(8) Obtain approval from the CIO prior to implementing an Internet Web site.

(9) Maintain current links with all USARC approved Intranet home pages.

(10) Develop and maintain their specific Web sites by using the "development server" - USARCINTRADEVA. The development server root is currently restricted for USARC Webmaster use only. Upon completion of Web site development or updates to a specific Web page, Webmasters will submit their request for publication ticket to the USARC Intranet Webmaster for action using ARWeb (Remedy).

c. The USAR Webmaster will maintain links to all USARC-approved Command Internet home pages.

Chapter 3
Network Security and Personal Accountability

3-1. Intent

This chapter provides policy and guidance to help reduce risks to the networks from untrustworthy automated data processing (ADP) practices, processes, and services, especially risks that can arise by way of the SBU network connections to NIPRNET and the public Internet. This memorandum includes operational, physical, procedural, and information security mechanisms that are intended to meet or exceed the operational requirements of the area of control, and to safeguard the information resources of the network.

3-2. Personal accountability

All persons are responsible for understanding and complying with the policies and procedures in this memorandum before receiving network access. All persons

accessing the networks must follow safe computing practices, and remain cognizant of the security requirements (OPSEC, INFOSEC, etc.). ***Each person is personally accountable for his or her behavior and actions.***

3-3. Using the USARC networks

a. Individual User Identification and Password.

(1) Each USARC network user will logon using his individual user identification (UserID) and Password. ***Publicizing or sharing a UserID and Password with any other person is a security violation and is prohibited.***

(2) Each person will obtain the initial UserID and Password in person (without exception) from the IANM or the designated representative. Prior to getting the initial Password, each person will read and provide the IANM a personally signed copy of the Information Systems Security Briefing (USARC Form 75-R).

(3) Each SBU network user will change their password at least twice a year by using the NT Workstation "Change Password" utility (option button on the "Security" dialog box that appears on the monitor when the CTL-ALT-DEL keys are pressed simultaneously). Personnel who will be on extended absences (e.g., TDY, Leave, etc.,) should contact the IANM for guidance.

(4) The IANM will issue all passwords to the classified network. The classified network passwords will expire every 3 months.

(5) Immediately report any lost, misplaced, or possibly compromised passwords to the IANM. Users who forget their passwords will seek assistance, in person, from the IANM.

(6) Users must memorize their passwords. Passwords will not be written down or stored in a function key, logon script or communications software. Under no circumstances will passwords be shared.

3-4. Files and data

Classified information will **NOT** be processed, transmitted, or stored on the SBU network. ***Each person is accountable for the proper security classification of data, and will ensure that classified data is NOT placed on SBU network.***

3-5. Data transfers between the classified and SBU systems

Each user will--

a. Treat all files and data coming from the classified network (to include hard copy printouts) as SECRET until downgraded or declassified by the agency security manager. (b. Mark or label all materials with the proper security classification.

c. Avoid saving classified information to diskette. If classified information must be transferred to diskette from the USARC classified network or any computer accredited to process classified information, the user will mark the diskette SECRET and handle accordingly.

d. Never use a classified diskette in any unclassified or SBU systems. Use only SBU diskettes, files, and data in a workstation connected to the SBU network.

e. Never transfer any file from a classified network or a classified diskette to an unclassified or SBU network, regardless of the classification of the data. If transfer of unclassified or SBU information from a classified file to the unclassified or SBU network is necessary, the user will obtain written authorization from the agency security manager, who will ensure that no classified data is introduced into the unclassified or SBU network. The user will maintain a copy of the security manager's authorization to transfer the data.

f. Immediately run the virus checking software against a diskette every time it is transferred between the classified and SBU networks or any other computer system.

g. Report a security violation if any classified diskette, file, or data is in an SBU network workstation, or if any classified information displays on a workstation not approved for processing classified information.

h. Run Norton Utilities DISKWIPE 3 times on a diskette to DECLASSIFY a CLASSIFED diskette. This destroys all data. After the agency security manager verifies that no classified information remains on the diskette, the user may re-label the diskette. (DISKWIPE is available at the USARC Customer Service Center.) Contact the USARC Deputy Chief of Staff, Intelligence if there is any doubt or concern about the security classification or how to perform security downgrading or re-grading.

3-6. Log-off and lock workstations

a. When leaving the immediate area of the workstation, the user will either log-off or lock workstation. Workstations are locked by using the NT Workstation "Lock Workstation" utility (option button on the "Windows NT Security" dialog box that appears on the monitor when the Control-ALT-DEL keys are pressed simultaneously). Locking the workstation hides the user window, until the user types the log-in password and presses enter. It is a security violation to leave the workstation without logging off or locking the workstation, as an active workstation makes the user's account available for use by others.

b. Users will log-off the workstation at the end of the duty day. Log-off terminates all user work and closes the network session.

c. When available, an automatic log-off will terminate user programs and log the user off the network automatically after 30 minutes of non-use.

3-7. Network monitoring and audit trails

a. Information on workstations and servers is property of the U.S. Army. ***The user has no right to privacy on the USARC network.*** All activity, to include E-mail transmissions, file transfers, and access to the World Wide Web is subject to monitoring and auditing at all times. Using the network and computer systems constitutes consent to ADP and telecommunications security monitoring.

b. During monitoring or auditing, information might be copied, generated, or used for official purposes. Network and computer systems are monitored by authorized personnel or automated means to ensure that the use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify

security procedures. Monitoring includes authorized tests or verification to ensure the security of systems from unauthorized use. Evidence collected during monitoring may be provided to appropriate authorities for administrative, criminal, or other judicial or non-judicial actions.

c. Audit trails may record any information, E-mail, or data that transits the system. Users will NOT attempt to access, alter, or delete audit logs and audit files.

3-8. Terminating or disabling access

a. The IANM will review user accounts quarterly. After 60 consecutive days, the IANM will disable an unused account until the user reconfirms the need for access, through their functional proponent. The IANM will delete disabled accounts after 30 days.

b. The IANM will delete a user account when any of the following occurs:

(1) Sponsorship is rescinded by the USARC functional proponent.

(2) On direction of the Commander (e.g., security violation).

(3) Need for access expires.

(4) User does not access network for 90 consecutive days.

3-9. Network permissions

a. The IANM provides users access to network files and folders strictly on a need-to-know basis. Only the owner or functional proponent of the data may authorize access.

b. Users requesting access to network files must obtain access permission from the functional proponent of the data. The functional proponent will notify the IANM, via E-mail, to authorize access to the data. The E-mail must include the name of the user or group to be granted access, the specific location (servers, folders, and file names) of the data, and the type of permission (read, write, execute, change, etc.) to be granted.

3-10. Authorized and unauthorized use

a. Authorized use of an information system is defined as those activities authorized to be performed by an individual in accordance with this memorandum and DOD 5500.7-R (change 2, para 2-301).

b. Unauthorized use includes any activity that is illegal or is prohibited by this memorandum; disrupts or prevents authorized use; compromises privacy of other users; performs an unauthorized release of information; or impairs the integrity of information processing, storage, or transmission capability. Examples of unauthorized use include: introducing computer viruses; compromising the technical or administrative security mechanisms of the networks; making information on networks available to the World Wide Web; making SBU information available to unauthorized persons; E-mailing "chain letters;" or accessing pornographic material.

c. Under NO circumstances will any individual place games on network servers.

3-11. Reasonable and prudent precautions

Each person using or supporting use of the networks will take reasonable and prudent precautions to ensure--

a. The availability and integrity of network resources.

b. Information on government computer systems or networks is not disclosed to the World Wide Web and is transmitted ONLY TO authorized persons over Non-secure Internet Protocol Router Network (NIPRNET) and the public Internet.

3-12. Computer security

a. Special emphasis on data security is essential because of the configuration and proximity, of classified computers and SBU computers. The proper security classification label (e.g., SF 710) must be on every diskette and data media. Users will NOT place any electronic media in any SBU network workstation if the media is suspected to contain classified information, or if the media has a security label which exceeds SBU.

b. Network resources must provide the highest possible assurance that information made available to, or received from, interfaces to the public Internet, NIPRNET, and other network connections, maintains network integrity, timeliness, functionality, and accuracy. It must ***NOT*** impede, restrict, or disrupt the operation of networks. Every IS user will practice safe computing and remain alert to the possibility of intrusions, computer viruses, computer hoaxes, and other threats to security.

Chapter 4
NIPRNET, Internet, and World Wide-Web

4-1. NIPRNET, Internet, and World Wide Web

The SBU network has access to the NIPRNET, Internet and World Wide Web (WWW). The Internet is an efficient and effective means for users to share accurate, relevant, and timely mission-related information, and to provide value-added information services among SBU network users; Army activities; other Service and Joint organizations; and other Federal, State, and Local agencies. Network security will block features that are known or likely to be security risks in connecting with outside networks like NIPRNET and the public Internet.

4-2. Release of information to the public

The SBU network will NOT be used to release information to the general public, World Wide Web, or the public Internet. Users having information for public release will contact the USARC Public Affairs Office and will prepare that information for release on the USAR Internet Home page.

4-3. Contact with the media and Congress

All official contacts with the media concerning USAR matters must be made through the appropriate USAR Public Affairs Office and all contacts with Congress concerning USAR matters must be made through the Office of Congressional Liaison.

4-4. Internet access

a. Users will not access commercial services (such as CompuServe, America on Line, or Prodigy) using government-owned facilities or equipment ***unless a government-acquired subscription to such services is in place and the access is for official business only.*** If the connection is made via an individual modem, the computer must be logged off the LAN and operating in a standalone mode.

b. **Users will limit use of the Internet from government-owned or leased computers to unclassified, official government business, and those authorized purposes as set forth in DOD 5500.7-R.** Government access to WWW sites is permitted to obtain professional literature that is job related; acquiring public domain information of value to the organization; to send official U.S. Government E-mail; to correspond with learning institutions for job-related continuing education purposes; and for other official government business.

c. Authorized (as opposed to official) purposes include brief Internet searches, when the supervisor (commissioned officer or GS-11 or above) grants permission after determining the following:

(1) Such communications do not adversely affect the performance of official duties by the DOD employee or by the DOD employee's organization.

(2) Such communications are of reasonable duration and frequency and, whenever possible, made during the DOD employee's personal time such as after duty hours or lunch periods.

(3) Such communications serve a legitimate public interest (such as educating the DOD employee on the use of the Internet; enhancing the professional skills of the DOD employee; job searching in response to federal government downsizing).

(4) Such communications do not put federal government communications systems to use that would reflect adversely on DOD or the USARC (such as uses involving pornography; chain letters; unofficial advertising, soliciting, or selling -- except on bulletin boards established for such use; violations of statute or regulations; inappropriately handled classified information; and other uses which are incompatible with public service).

(5) Such communications do not overburden the communications system and creates no significant additional cost to DOD or USARC.

d. All USAR information systems with servers (including Web servers) that are connected to unclassified publicly accessible computer networks, such as the Internet, will employ a combination of access and security controls (firewalls, routers, etc.) to ensure the integrity, confidentiality, and availability of DOD information systems and data.

e. In accordance with AR 380-19, the designated approving authority (DAA) must accredit and authorize all systems ***prior*** to being put into operation. The IANM will conduct a network risk analysis as part of the overall network security plan to determine the appropriate level of security. All USAR wide area network and LAN systems security accreditations must reflect the addition of, or existence of, a Web server or other Internet information server.

f. Information residing on a server with a ".army.mil" domain or server, may be interpreted as reflecting official Department of the Army, or Department of Defense policies or positions.

g. There is no such thing as a personal or unofficial home page on a ".mil" server. These servers and the information they contain are only for official business and use in an official capacity.

4-5. Internet monitoring

This Headquarters monitors Internet use. Use of a government computer serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized. Use of such systems is not anonymous. For example, for each use of the Internet over a government system, the name and computer address of the employee user is recorded by the Government and also by the locations searched.

4-6. USARC *Internet* Web site

a. The USARC Internet Web site is at http://www.usarc.army.mil or http://160.136.109.3. USARC network resources are not accessible from the USAR Home page.

b. The USAR Web sites and organizational Web pages use information from functional proponents (users). Functional proponents are responsible for--

(1) Information content on Web pages.

(2) Keeping information current and accurate.

(3) Keeping within format and content guidelines specified in the USARC Public Affairs Office policy.

Content is limited to official and unofficial information of military value to the operations of the USAR. For example, home page and Web site information will NOT contain personal or Privacy Act Information (such as family member names, personal photos and addresses, home phone numbers, career history, resumes, previous assignments, awards, or schooling). Information that extends beyond the duties and responsibilities of the person's organization, commercial advertising, and product endorsement is prohibited.

4-7. USARC *Intranet* Web site

a. The USARC Intranet Web site is at Uniform Resource Locator (URL) "*http://usarcintra*" or IP address "*http://55.124.130.176.*"

b. The USARC Intranet Webmaster, within the USARC CIO, is responsible for the USARC Intranet Home page. Staff sections are responsible for designating, by appointment letter, Webmasters for their respective Web pages. Intranet Webmaster responsibilities are in paragraph 2-5 of this memorandum.

c. Access to the USARC Intranet is available only to authorized WAN users. Appropriate access and security controls (firewalls, restriction by IP address, etc.) are in place to ensure data integrity. Material provided on the USARC Intranet is for official use only and will not be

made available to the public at large without the written approval of the PAO.

d. Hyperlinks from NIPRNET and Internet sites to USAR Intranet sites are prohibited.

Chapter 5
Modems, Remote Access Services, and Software Standards

5-1. Modems and data transmission devices (dial-in, dial-out)

a. The USARC strictly prohibits the connection of any unauthorized modem or any data transmission device to any computer within this Headquarters. Data transmission devices pose an unacceptable risk of bypassing network security mechanisms. Network level modems are available on the SBU network that supports the network security system.

b. The USARC DAA must approve all individual communications devices. Instructions for obtaining approval for data transmission devices are found in USARC Regulation 380-2. Upon approval from the USARC DAA, users will--

(1) Ensure that information is transmitted via data transmission device that meets communications security standards found in 380-19 and AR 380-40. If in doubt as to the information's sensitivity level, consult the originator of the information or the USARC Deputy Chief of Staff, Intelligence (DCSINT).

(2) Disconnect the computer from the network before using the individual data transmission device.

(3) Turn off or disconnect the data transmission device when not in use.

c. Under NO circumstances will users permit dial-in access to their computer via the individual modem, without specific written permission from the IANM.

5-2. Remote Access Service (RAS)

a. Remote access service (RAS) to the SBU network is available for all authorized users. Remote access to the classified network is prohibited.

b. Remote access users will not use the save password feature within the logon dialog box. This feature will be disabled on all government owned computers. In the event the computer is lost or stolen, use of this feature allows an intruder to automatically logon and access network resources.

5-3. Terminal Server Access Controller System (TSACS)

a. Managed by the Army Signal Command, through local Service Providers, the TSACS was designed for true Army-wide common-user access to the Internet when users were out of the office and required access; e.g., TDY.

b. Submit requests for access to the TSACS using the USARC Form 94-R, USAR Terminal Server Access Controller System (TSACS) Registration Form. Provide completed forms to the AFRC-CIS-S, USAR CIO TSACS Service Provider. This form is in FormFlow format on the "usarcshared/readonly" drive in the "USARC" subfolder of the folder named "Forms."

5-4. Software standards

a. In order to maintain integrity and compatibility across the network, only software that has been specifically developed, approved for use, purchased, or leased by the USARC CIO may be used on workstations or servers. The list of USARC-approved software is published by the USAR CIO and is available on the USAR CIO Web page. Go to http://usarcintra, click on "Directorate Links", then "CIO," and click on "Policy and Guidance." Then on the "CIO Policy Index" Web page, scroll to the appropriate memorandum. The CIO, AFRC-CIS-S, must approve deviations from the standards, in writing, prior to implementation.

b. Users will ***NOT*** install or use any non-government licensed, privately owned, public domain, shareware, or non-standard software on government-owned equipment without written approval from the CIO Information Systems Services Directorate (ISSD). Submit requests to use these types of software through the agency Director or Chief, to CIO, ISSD.

c. The CIO will not provide technical support for public domain, shareware, or privately purchased software.

5-5. Push-pull technology prohibition

The use of all commercially available software that provides the capability to pull non-official information feeds into government computers is prohibited. Examples of these "automatic push-pull data gathering applications" include Pointcast Network Client, Pointcast I-Server, Freeloader, Intelliserv, Internet Explorer 4.0 Active Desktop, and Ticker.

5-6. Electronic mail

a. The USAR E-mail system is only for official and authorized use, as described in DOD 5500.7-R. Unauthorized use is prohibited. Violations will be dealt with as appropriate.

b. To conserve bandwidth and maximize network efficiency, users will--

(1) Not use the "Return Receipt" E-mail feature as a matter of routine. Use only on official E-mail when receipt must be positively verified (e.g., where the E-mail has a direct bearing on the mission).

(2) When using the "Reply" and "Reply to All" E-mail feature, avoid quoted or in-line replies (e.g., complete E-mail strings) to the maximum extent possible. Limit the use of "cc:" addressees as much as possible.

(3) Limit the number of addressees on E-mail messages. The maximum number of addressees is 200.

c. Limit official subscriptions to newsgroups to the absolute minimum required to support command missions and functions. This Headquarters strongly discourages personal subscriptions to newsgroups that are not mission related.

d. Keep large E-mail attachments to a minimum. Users can place documents on shared network servers or Web servers and provide directions to access the documents. To

the maximum extent possible, compress all large E-mail attachments to conserve bandwidth. The maximum attachment size is 9MB for Intranet message traffic and 5 MB for Internet message traffic. When message addressees include both Intranet and Internet recipients, the maximum attachment size is 5 MB

e. The maximum mailbox size is 10MB. Requests for exception will be submitted, in writing, to the CIO for approval.

5-7. Proprietary software

a. Without the specific written permission of the software licenser, no user has the right to make or distribute copies of copyright material. The only exception is the user's right to make a backup copy for archival purposes, if the manufacturer does not provide one. Unauthorized duplication of software is a Federal crime.

b. Individuals installing upgrades to commercial software packages must properly dispose of the superseded software media. Unless vendor license agreements specify disposal procedures for obsolete software, the obsolete diskettes will either be appropriately destroyed or purged and reformatted. If not destroyed, the most recent version of the obsolete software must be securely stored (see USARC Regulation 380-2, para 8-1).

c. Personnel who violate copyright laws may be subject to criminal prosecution, civil and criminal penalties, and disciplinary or adverse action.

Chapter 6
Workstation and Network Server Configurations

6-1. Hardware standards

a. In order to maintain integrity and compatibility across the network, the CIO must approve all hardware prior to use. The USARC hardware standards are in USARC Regulation 25-1. The CIO, AFRC-CIS-S, must approve any deviations from these standards, in writing, prior to implementation.

b. Users will ***NOT*** install or use any non-government or privately owned hardware on government-owned equipment without written approval from the CIO ISSD. Submit requests to use these types of hardware through the agency Director or Chief, to CIO, ISSD.

c. The CIO will not provide technical support for privately purchased hardware.

6-2. Trusted domains or networks

Establishment of trusts will be in accordance with the USARC Information System Architecture. The DAA must approve the establishment of trusted relationships with any other domains or networks ***prior to*** implementation. The DAA has authority to direct the dissolution of an established trust relationship in the event of a known or suspected compromise.

6-3. User passwords

a. The configuration of the SBU network and unclassified, stand-alone workstations requires each person to change their password at least every 6 months. It also provides a warning notice at one or more logons at least 10 working days prior to expiration and requires each password to be no less than 8 random characters and contain characters from at least 3 of the following 4 classes:

Description	Examples
1. Upper Case Letters	A, B, C, ... Z
2. Lower Case Letters	a, b, c, ... z
3. Numbers	0, 1, 2, ... 9
4. Non-alphanumeric (special characters)	For example, punctuation and symbols. ({}[]<>,;.:'"?/|\`~!@#$%^&*()_-+=)

b. Passwords may not contain any part of the user's name or any word out of the dictionary. The SBU network will also prevent passwords from being reused within the past 24 password changes.

c. The classified network and stand-alone workstations are configured to:

(1) Require users change passwords at least every 3 months.

(2) Provide a warning notice at one or more logons at least 10 working days prior to expiration.

(3) Require each password to be no less than 8 random characters.

(4) Prevent the re-use of passwords within the past 24 password changes.

d. Generic password assignment is prohibited (e.g., using "password" as the password for all newly created user accounts).

6-4. System passwords

a. System passwords will follow the same rules as user passwords. Additionally, at a minimum, the appropriate administrator will change every default or initial password for the operating system, application software, and network software whenever--

(1) Software is installed, upgraded, or replaced.

(2) A person having access to the password departs, or no longer has an operational need or functional responsibility to know the password.

(3) A known or suspected security violation may have caused a password compromise.

(4) Competent authority (e.g., ACERT, IAPM) orders a password change.

b. Network operations accounts (those network accounts created for operations and maintenance purposes) will not have dial-in access.

c. To ensure the availability of important system data, written documentation of system passwords and parameters, and the procedures for changing them will be secured in a security container, under the control of the Chief of the Network Operations Center (NOC).

6-5. "Risky" protocols, services, and file extensions
The CIO will—

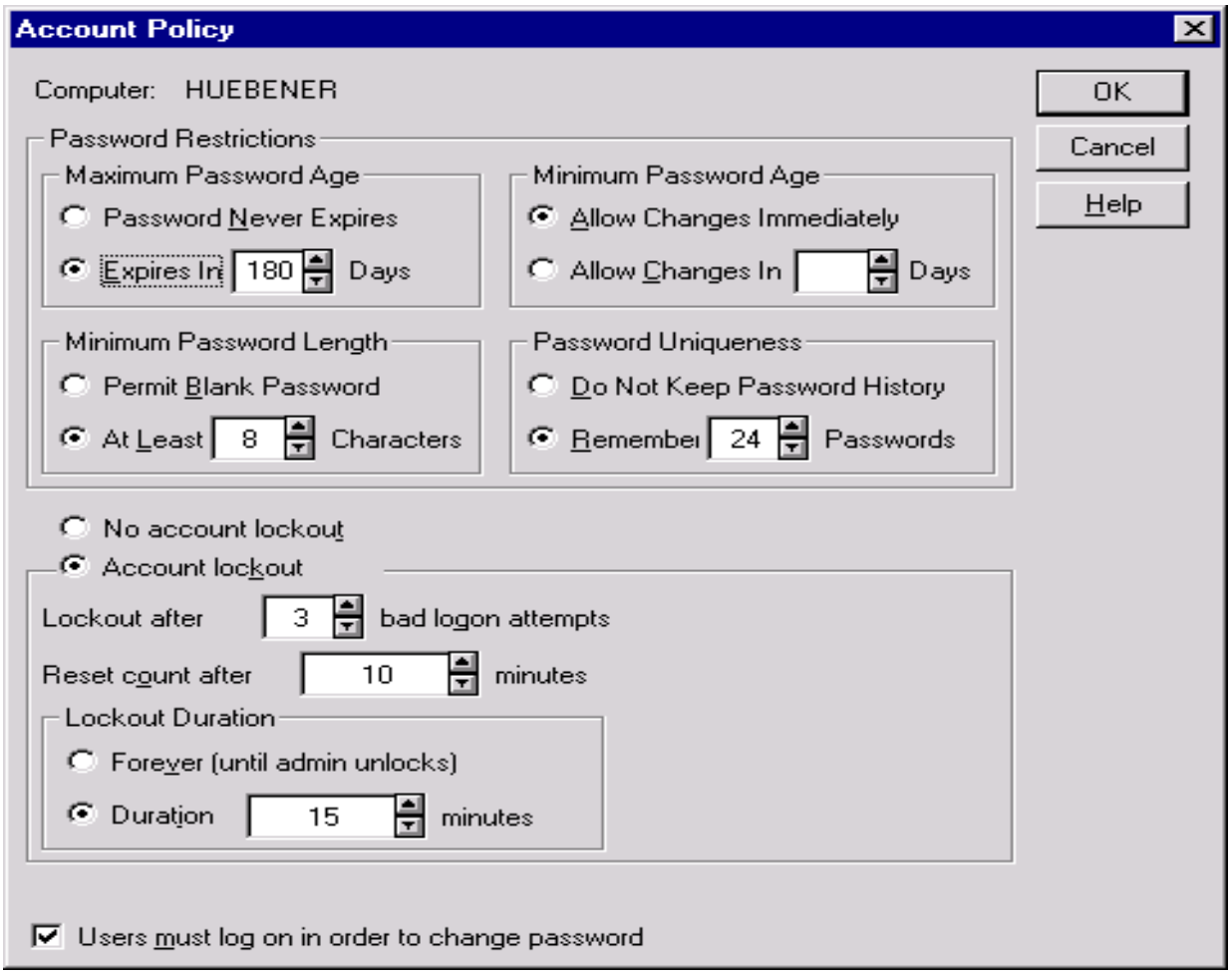
a. Wherever possible, isolate or map files and directories with .lnk, .dat, .cmd, .bat, .url, or .exe files so that they only access information resources specific to that service, protocol, or public access partition. .Bat, and .cmd files will not be used as CGI scripts. To minimize the risk that a security breach in one service can expand to other parts of SBU network, wherever possible, the CIO will store such files completely within a single directory or partition. For example, partitions accessible to the public will not contain .lnk, .dat, .cmd, .bat, .url, or .exe files, except those that are expressly required for the proper functioning on software applications that reside in the partition function; and the contents of those files will not map to access files or information outside the partition.

b. Disable NetBIOS over TCP/IP.

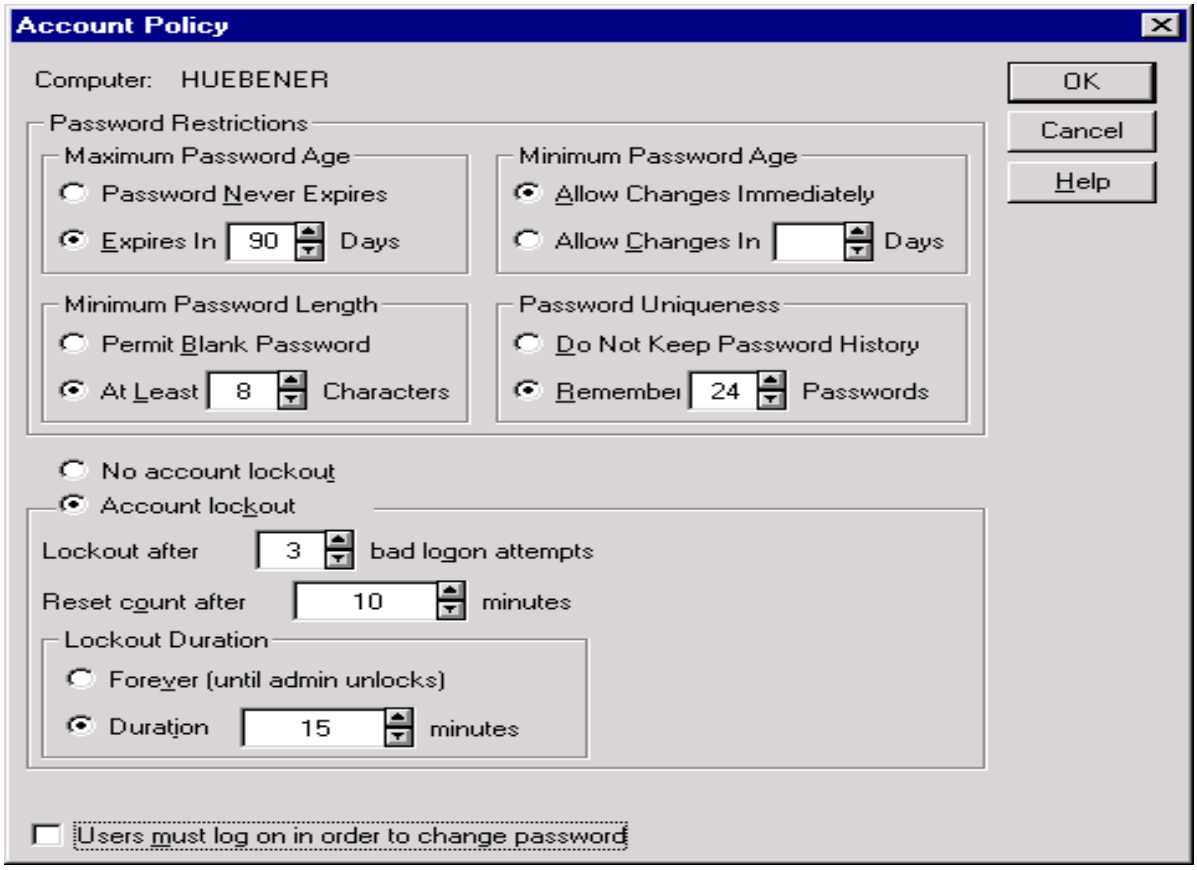
c. Remove unused protocols to prevent the possibility of unauthorized exploitation.

6-6. Workstation configuration
The CIO will ensure workstation configuration complies with the following:

a. SBU Workstation User Account Policy Values.
The following are the required values for the User Account Policy on SBU workstations:



b. Classified Workstation User Account Policy Values. The following are the required values for the User Account Policy on classified workstations.



c. Workstation default accounts

(1) Upon installation of a workstation or server, the CIO **must** change passwords on all default accounts (e.g., Administrator, ISSO, Sysadmin, and BIOS). Where the workstation employs both the classified and SBU subsystems, the passwords for these accounts **must not** be the same. Additionally, the CIO must rename the Administrator account and disable the Guest, ISSO and Sysadmin accounts. The naming conventions and passwords for these accounts is available from the USARC Customer Service Center.

(2) The Administrators account is for emergency system management only. Individuals assigned responsibility for the Administrators account must have a separate logon for daily operations.

6-7. Workstation Event Log settings

The CIO will ensure workstation Event Log settings comply with the following:

a. The Event Viewer Log Settings on workstations **must** read as follows:

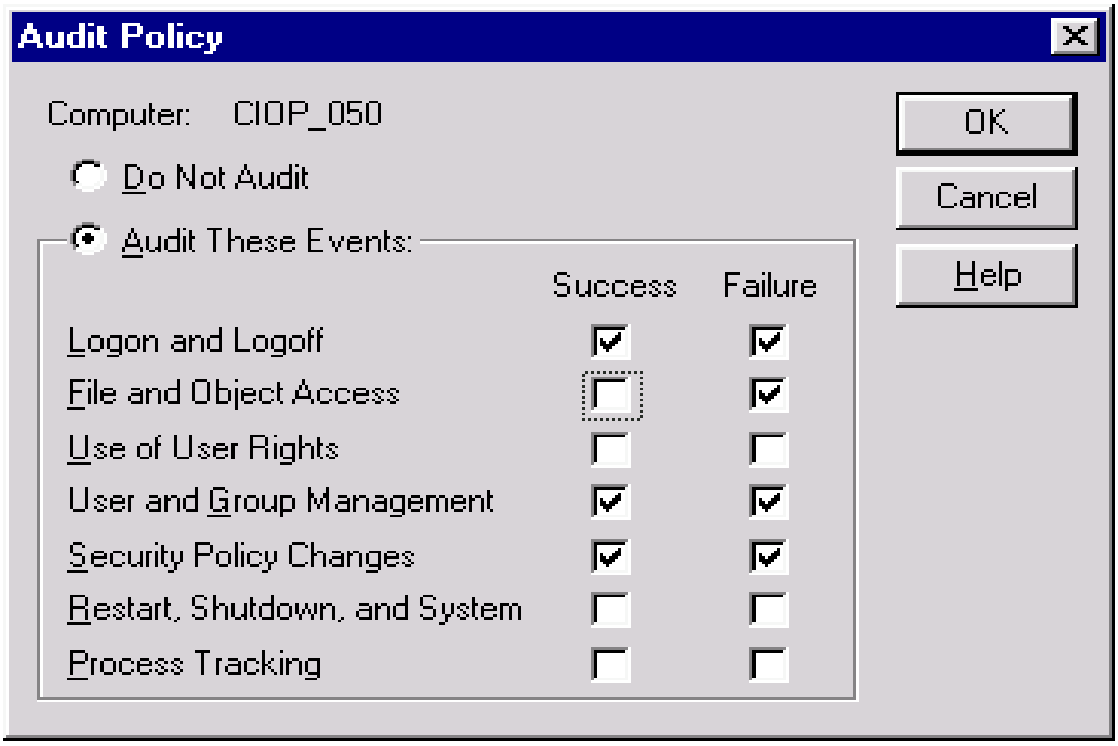
Application Log	Overwrite Events Older than 15 Days
Security Log	Overwrite Events Older than 30 Days
System Log	Overwrite Events Older than 15 Days

b. In the event of a security incident, maintain the logs until the incident is resolved.

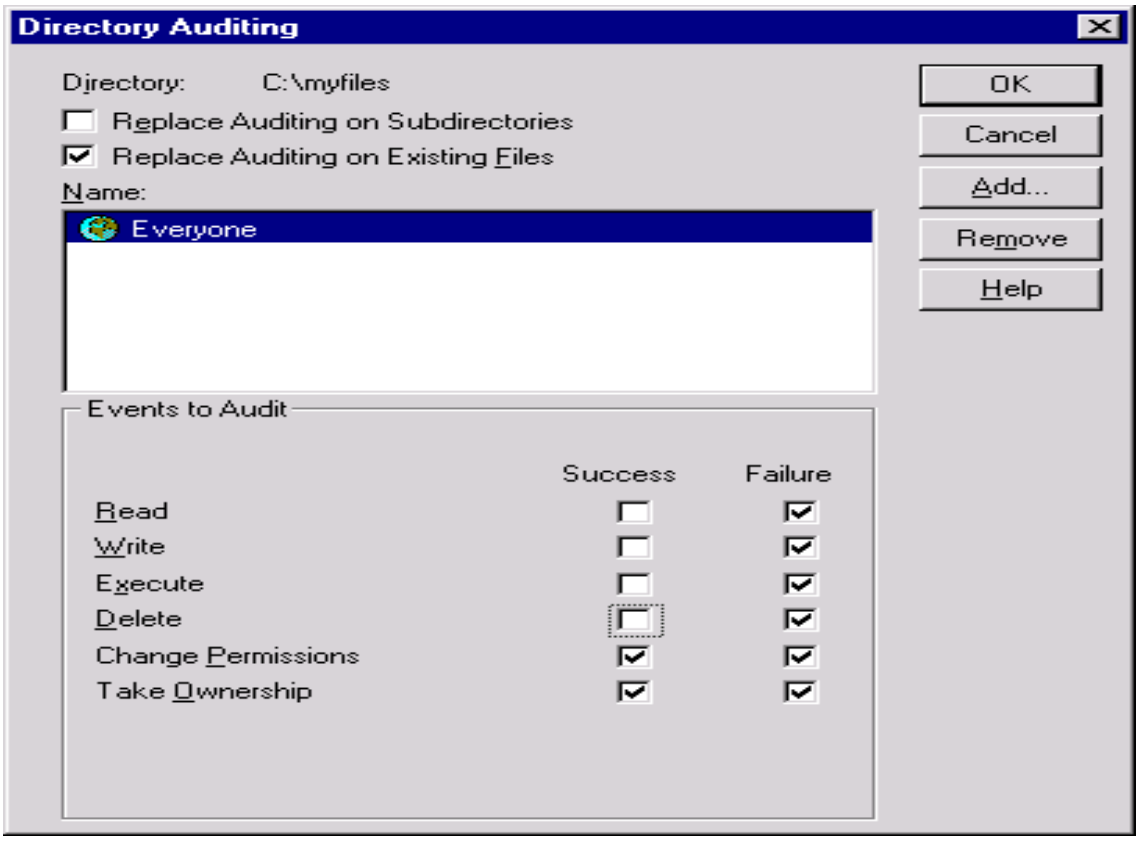
6-8. Workstation auditing

The CIO will ensure audit mask settings are set for "Everyone." The following tables display the recommended, minimum audit requirements for the workstations:

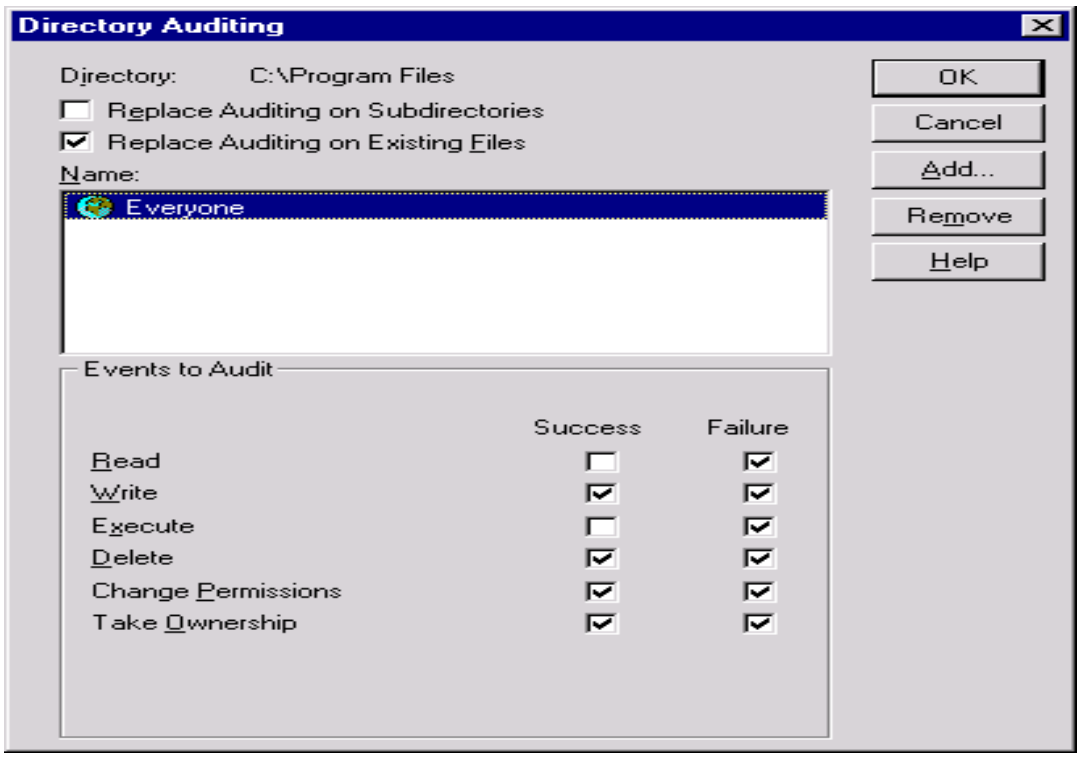
a. Audit Mask for Workstations.



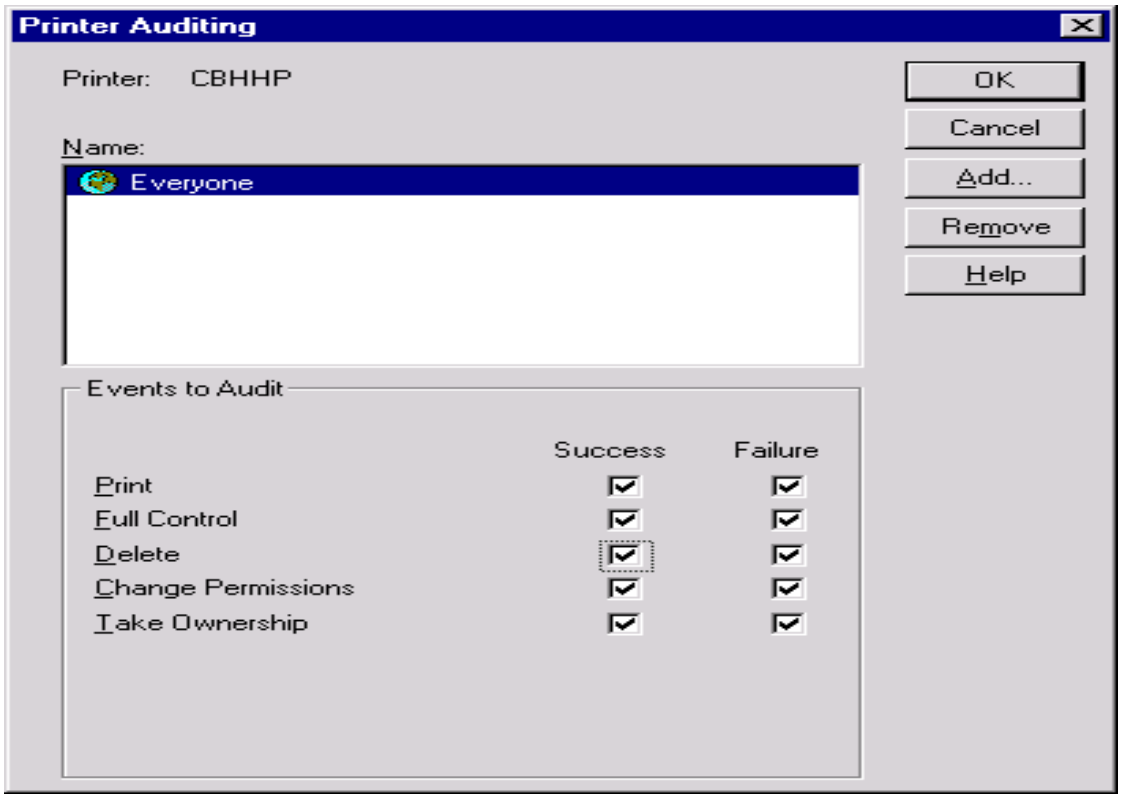
b. Audit Mask for User Directories and Subdirectories.



c. Audit Mask for all other Directories.



d. Audit Mask for Printers on Classified Systems.



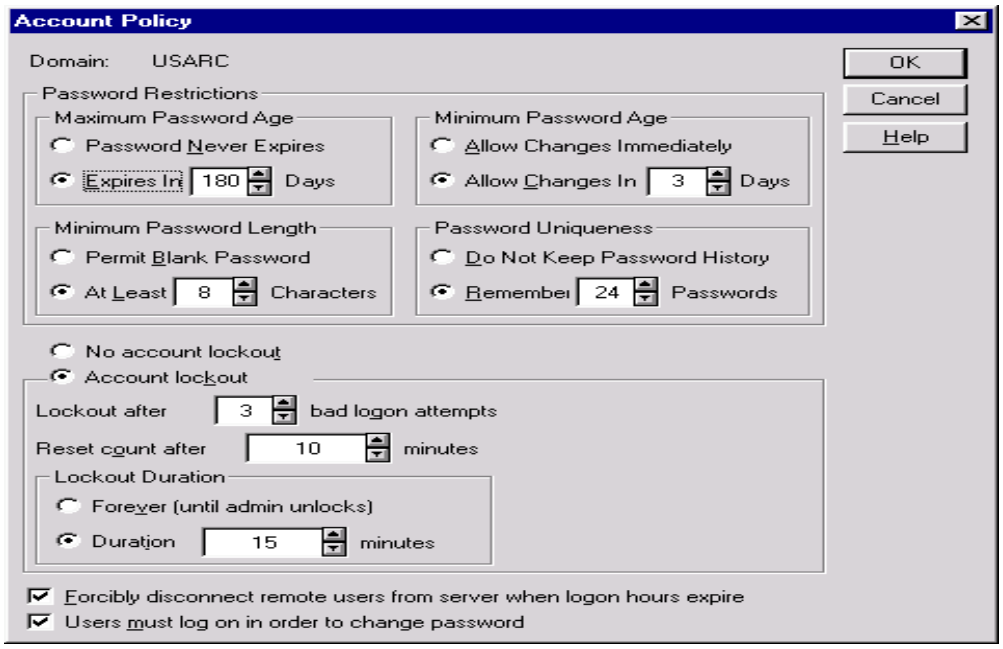
6-9. File system standard
The installed file system on all NT platforms will be the NT File System (NTFS). No system will use the File Allocation Table (FAT) file system format used by Disk Operating System (DOS). All workstations will boot into NT Workstation. Exceptions must be approved in writing by the IANM.

6-10. Patches and upgrades
The CIO will apply system upgrades and patches immediately.

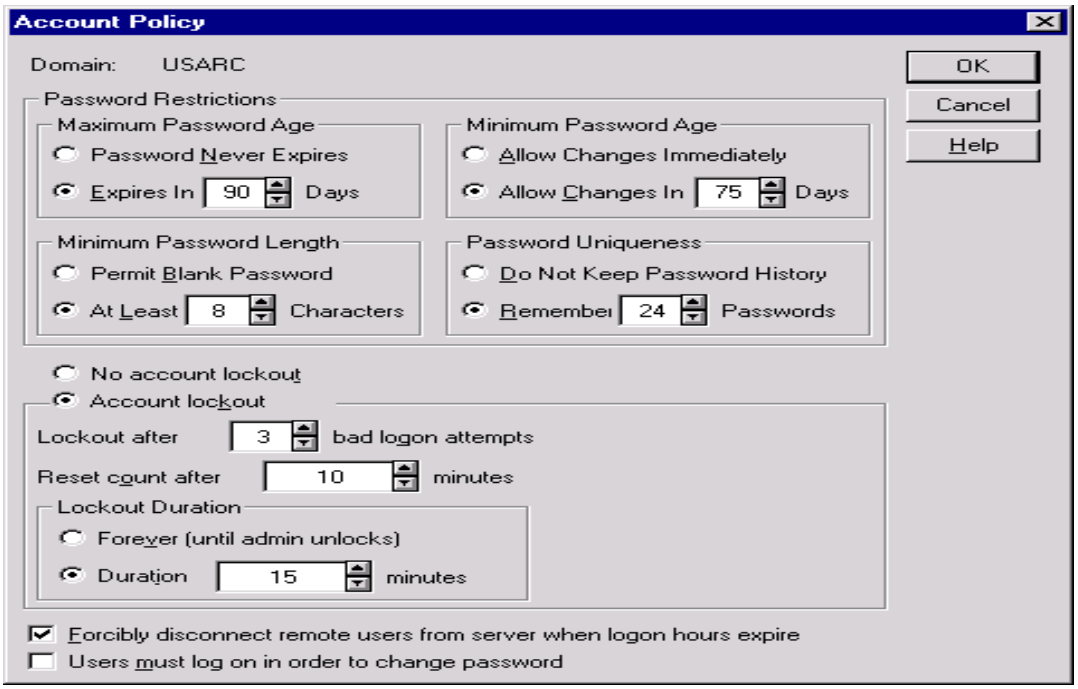
6-11. Disable last logon UserID display
The CIO will disable the Windows NT feature that saves the last logon UserID when a user logs off the workstation.

6-12. Network server configuration
The CIO will ensure network configuration complies with the following:

a. SBU Network User Account Policy Values. The following are the required values of the User Account Policy for the SBU network:



b. Classified Network Account Policy Values. The following are the required values of the User Account Policy for the classified network:

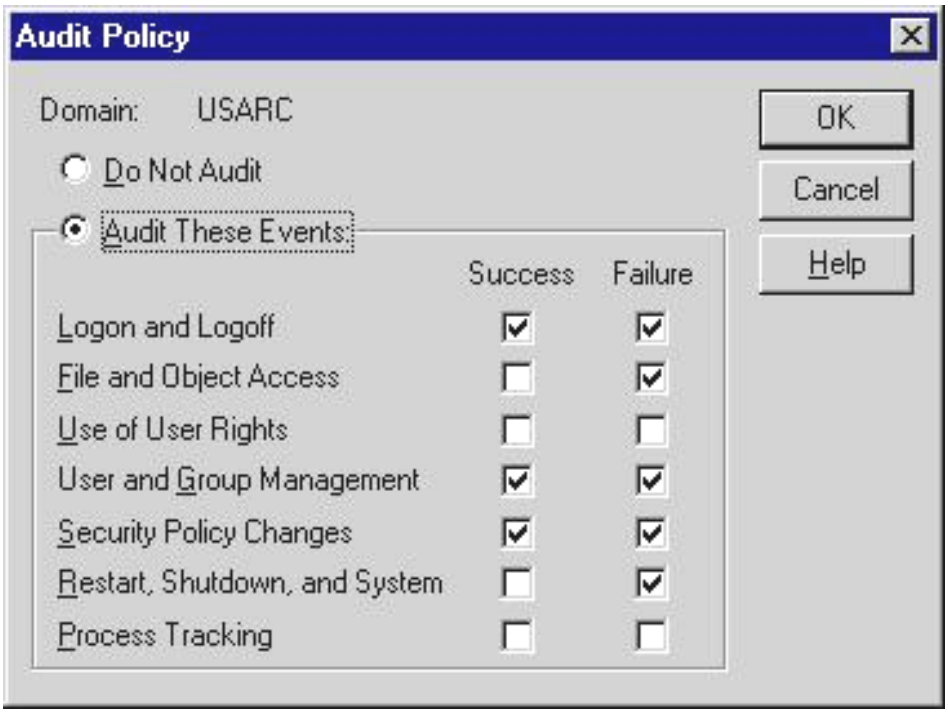


c. Server Default Accounts. See paragraph 6-5b.

d. Server Event Log Settings. See paragraph 6-5c

e. Server Auditing. The following table displays the minimum audit requirements for servers:

Audit Mask for Servers



f. File System Standard. See paragraph 6-8.

g. Patches and Upgrades. Network management personnel will apply system upgrades and patches immediately, and will maintain a log detailing when and where they are applied.

Chapter 7
Network Services

7-1. Outgoing Services

The following outgoing services are available:

Service						
User Type	SMTP	FTP	Telnet	DNS	NNTP	HTTP
Directly Connected	Yes	Yes	Yes	Yes	Yes	Yes
Dial-In	Yes	Yes	Yes	Yes	Yes	Yes

7-2. Incoming Services

The following incoming services are available:

Service						
User Type	SMTP	FTP	Telnet	DNS	NNTP	HTTP
Directly Connected	Yes	Yes*	Yes*	Yes	Yes	No
Dial-In	Yes	No	No	Yes	Yes	No
*Available for Authenticated Users only.						

7-3. Proxy services

a. Resources internal to SBU network (inside the firewall) will use Simple Network Management Protocol (SNMP). SNMP queries through the firewall are not permitted.

b. Hypertext Link Protocol allows SBU network users unrestricted viewing of WWW using an Internet browser. The public will only be able to view information approved for public viewing on the WWW server.

c. Simple Mail Transfer Protocol (SMTP) provides the E-mail application gateway service to the Microsoft Exchange Server.

d. File Transfer Protocol (FTP) allows SBU network users to query and obtain information from other hosts outside SBU network. It may be necessary to provide an electronic security advisory to the remote FTP host(s), because there is a possibility that the SBU network FTP daemon can be compromised. (When the Windows NT proxy server intercepts the user's FTP UserID and Password, Windows NT generates a UserID and Password that is proxied to the remote host.)

7-4. Network audit data

a. Safeguards are in place to ensure that each person having access to an IS may be held accountable for his or her actions. For all IS, except stand-alone systems, a security audit trail will provide a continuous documented history of IS use.

b. The audit trail will be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise or damage should a security violation or malfunction occur. The IANM or designated network security personnel will review the audit data once per week, as a minimum, but should review the network audit data daily.

c. If documentation from the audit trail includes suspected or actual security relevant events which become part of a body of evidence supporting an ongoing investigation, it will be retained by CIO according to the Uniform Code of Military Justice (UCMJ). The USARC will maintain audit records for 6 months, unless the IANM or Commander determines that suspicious activity merits keeping them for a different time period. At the end of the specified period, they will be erased.

7-5. Services not covered in this memorandum

The minimum services essential to the missions and functions of SBU network users are in this memorandum and its appendices. The IANM will obtain appropriate approval from the DAA to implement new requirements, capabilities, or to correct security weaknesses as they are identified.

7-6. Malicious Code management

a. Malicious Code is program code introduced into an IS that intentionally, or unintentionally, causes a disruption of normal operations through the destruction or modification of data, or through the denial of service.

b. Virus protection is the responsibility of the individual user. Users must be extremely careful when redistributing files to a large number of users or placing them in shared folders. Use particular caution with the following types of files:

(1) ALL files received as electronic mail attachments.

(2) ALL files downloaded from outside Internet hosts.

(3) ALL files received on Information Storage Media (e.g., floppies, CDs, etc.)

c. Each user will ensure that--

(1) The latest version of the anti-virus software is installed and working on their computer.

(2) The latest version of the anti-virus definition file(s) is(are) installed on their computer.

(3) The latest version of the anti-virus software and definition file(s) is(are) run automatically, if possible, at least weekly against the entire local hard drive(s); that it checks all files; and, if possible, removes (disinfects) any viruses detected.

(4) If viruses are detected and removed, they inform their local ISSO/ISSM of the viruses encountered.

(5) If viruses are detected that could not be removed, they inform their local ISSO/ISSM of the viruses encountered and--

(a) Write down the exact path to the infected file.

(b) Make a note of where the infected file came from (if known).

(c) Notify one of the following individuals immediately:

-- Customer Service Center, USARC CIO, (404) 464-9350, Helpdesk@usarc-emh2.army.mil

-- Information Assurance Program Manager (IAPM), Mrs. Pat Benny, (404) 464-8450, bennypat@usarc-emh2.army.mil

-- Information Assurance Manager (IAM), Mrs. Suzanne Kreisher, (404) 464-8452, kreisher@usarc-emh2.army.mil

-- Information Assurance Network Manager (IANM), Mrs. Carol Huebener, (404) 464-9386, huebener@usarc-emh2.army.mil

*[**NOTE:** Users **WILL NOT** share anything on their computer (e.g., send attachments or save to network drives) until the system has been cleaned and cleared by authorized personnel.]*

d. The local network administrator will--

(1) Ensure that the latest version of the anti-virus software is available on the network.

(2) Ensure that the latest version of the anti-virus definition files are available on the network.

(3) Whenever possible, automatically update all user's anti-virus software and anti-virus definition files when updates become available.

(4) Inform users when these updates become available on the network.

e. Virus infections on USARC computer systems are CONFIDENTIAL information. Do not discuss them with others that do not have a need to know. Avoid using the networks to discuss these matters.

7-7. Sanitizing procedures

a. General.

(1) In cases of compromise, immediately disconnect and secure compromised equipment and media. Physically disconnect **ALL** affected workstations and servers from the network by unplugging the network cable or by logging off and powering down the equipment. These servers and workstations must remain disconnected from the network until they have been sanitized and certified.

(2) Report the compromise to the Information Assurance Program Manager. Detailed reporting instructions are in AR 380-19, paragraph 2-27.

(3) Identify all backup media from the affected equipment, mark it as classified, and store in a GSA container approved for storage of classified information.

(4) When the compromise involves passing classified information via unsecured E-mail determine the scope of the compromise.

(a) The originator of the E-mail must provide a complete list of all addressees to whom the classified E-mail was sent. If feasible, initiate an attempt to recall the E-mail.

(b) Personally contact identified addressees to ensure their workstations are isolated (removed from the network) to preclude further compromise. If an addressee forwarded the classified E-mail, obtain a complete list of those addressees and contact each one. Continue until each addressee of the E-mail has been personally contacted.

(c) If an addressee is outside the area of responsibility of the originating command, provide immediate notification of the compromise to the Information Assurance Manager and Information Management Office at that addressee's command.

(d) If the classified E-mail is sent to an address outside DOD (e.g., AOL or Prodigy, commercial or corporate entities), ***DO NOT*** notify them of the incident. Under no circumstances should a commercial or corporate agency be alerted to the possibility of classified information residing on their servers.

b. Sanitizing Workstations.

(1) Delete all classified data from the computer's hard drive.

(2) Visually review, each user-created file intended to be reloaded. If the file is determined to be SBU or unclassified, it may be backed up for reloading to the hard drive. The Commander assumes the risk of reloading invisible data trailer information, which may be accessible to a sophisticated intruder.

(3) Back up the SBU and unclassified user-created data files (.doc, .ppt, xls, etc.) to tape, disk, or CD. Select files to be backed individually, not by directories, to preclude the possibility of including classified temporary files on the back up media.

(4) Purge the workstation by over writing the hard drive three times. Army Regulation 380-19, appendix F (Clearing, Sanitizing and Releasing Computer Components), allows the use of any tool that is capable of ***verifiable, three-time, overwriting*** of the hard drive.

(5) Reload the operating system and application software.

(6) Restore the SBU and unclassified user-created data files.

c. Sanitizing Servers.

(1) Delete all files identified as classified.

(2) Perform complete backup of the server.

(3) Physically break the array and put the hard drives into a different configuration.

(4) Low level format all drives three times.

(5) Initialize the reconfigured array.

(6) Restore from the SBU and unclassified backup tapes.

d. Alternative Procedures for Exchange Servers.

(1) All users on the affected Exchange server must remove all E-mail messages from their Inbox, Outbox, Sent Items, and Deleted Items folders. Users may save items identified as unclassified to personal folders located on their workstations. Make sure the users understand this step. If they save classified data to their workstation, that workstation will have to be purged.

(2) Delete all messages with classified information from the Inbox, Sent Items, and Deleted Items folders. If the information must be retained, print it or save it to disk. Mark and store the classified document or disk in accordance with AR 380-5.

(3) The IM personnel must certify that mailbox resources for each user is "0". The DAA must provide a certifying statement to CIO indicating that the command accepts the potential risk involved with not purging the exchange servers.

(4) When the classified information is an attachment to an E-mail message and, ***IF*** the classified attachment was not opened, the E-mail and classified attachment may be deleted from the user's inbox and deleted items. Since, temporary files are created only if the attachment is opened, the recipient's workstation and exchange server need not be purged.

e. Verification. Provide the USARC DCSINT and CIO Information Assurance Office a memorandum listing all the affected computers (by serial number) verifying completion of the above procedures and the DAA's acceptance of the potential risk of collateral compromise.

7-8. Warning banners

All networked and stand-alone government and contractor computer systems require a logon warning banner in accordance with USARC Regulation 380-2. The banner will display prior to entry into a host or gateway process. If the banner does not display, contact the Customer Service Center.

a. The following is the required content of the logon warning banner for networked systems:

ATTENTION

This is a DOD computer system. Before processing classified information, check the security accreditation level of this system. Do not process, store, or transmit information classified above the accreditation level of this system. This computer system, including all related equipment, networks and network devices (including Internet access) are provided only for authorized US government use. DOD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for all lawful purposes.

b. The following is the required content of the logon warning banner for stand-alone systems:

ATTENTION!

This is a DOD computer system. Before processing classified information, check the security accreditation level of this system. Do not process or store information classified above the accreditation level of this system. This computer system, including all related equipment, is provided only for authorized u.s. government use. DOD computer systems may be monitored for all lawful purposes. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for all lawful purposes.

7-9. Web browser configuration

Web browsers will access the Internet via the proxy server. The browser will be configured to--

a. Set Internet security mode to High.

b. Warn the users before sending information over an open connection.

c. Warn the user if changing between secure and unsecured mode.

d. Warn the user before accepting "cookies."

e. Enable all cryptography settings and prohibit saving secure pages to disk.

7-10. Continuity of Operations (COOP)

a. The USARC Network Operations Center (NOC) will conduct and maintain back up and archival functions as outlined in the Network Standing Operating Procedures. Labeling of back up and archival tapes will be in accordance with AR 380-19.

b. Outages may occur as the result of natural disasters, fire and smoke, climate, water, lightning, or other causes. However, the most likely outages are due to "hard" failures in equipment, communication lines, and electrical power, or "soft" failures caused by software errors, administrative errors in setting up software, computer viruses, or intrusions.

c. The NOC is responsible for developing, coordinating, maintaining, and checking the written procedures for computer operators, system and network administrators, and backup site personnel to start-up, manage, re-boot, and restore the system configuration, system start-up files, servers, and network.

d. The NOC will follow the Network Standing Operating Procedures to assess the technical impact of outages and will advise the chain of command of the estimated time to restore services. Where practical, maintenance and repair work will begin as soon as possible. The NOC will notify users of outages and, in the event that the outage is estimated to be longer than 1 duty day, the NOC will attempt to notify all agencies concerned by official message of the estimated time of repair. As necessary, the CIO and IANM will also coordinate assistance from other Information Management agencies.

e. If extended network disruption occurs (estimated over 24 hours), users will continue work in their functional areas. When users require access to external systems (e.g., Internet, NIPRNET), CIO will attempt to connect modems, for temporary use, on a limited number of common user workstations and will physically disconnect those workstations from the SBU network. When network functions are restored, CIO will remove the modems before re-connecting those workstations to the SBU network. Persons using the stand-alone workstations with modems will comply with all provisions of this memorandum.

f. If circumstances cause the network to relocate, a temporary unclassified network may be implemented at the alternate site. Until it becomes practical to install a temporary network at the site, the USARC will provide a limited number of common user workstations with modems for dial-out access to systems. Users will NOT set up or permit dial-in access. Persons using workstations with modems will comply with all provisions of this memorandum and will also be responsible for backing up their data and files onto diskettes.

Appendix A
References

Section I
Required Publications

AR 380-5
DA Information Security Program. (Cited in para 7-7d(2).)

AR 380-19
Information Systems Security. (Cited in paras 2-2a(6), 2-2b, 2-5c(3), 3-3c(1), 4-4e, 5-1b(1), 7-7a(2), 7-7b(4), and 7-10a.)

AR 380-40
Policy for Safeguarding and Controlling Communication Security (COMSEC) Material. (Cited in para 5-1b(1).)

USARC Regulation 25-1
Information Resources Management Program. (Cited in para 6-1a.)

DOD 5500.7-R
Joint Ethics Regulation (w/Chg 2). (Cited in paras 3-4a, 4-4b, 5-6a.)

Section II
Related Publications

(A related publication is merely a source of additional information.)

AR 25-1
DA Information Resource Management Program

AR 25-55
Army Freedom of Information Act Program

AR 340-21
Army Privacy Act Program

AR 360-5
Public Information

USARC Regulation 25-10
Telecommunications Management Program

USARC Regulation 380-2
Information Systems Security

USARC Pamphlet 25-1
Information Managers Handbook

USARC Memorandum 380-1
Information Systems Security

Section III
Referenced Forms

USARC Form 75-R
Information Systems Security Briefing for Users of Unclassified Computers or Local Area Networks

USARC Form 94-R
USAR Terminal Server Access Controller System (TSACS) Registration Form. (Prescribed in para 5-3b.)

AFRC Form 48-R
Classified Network Password Request Form

SF 710
Unclassified Label or ADP Media

Glossary

Section I
Abbreviations

ACERT
Army Computer Emergency Response Team

CID
Criminal Investigation Division

DAA
designated approving authority

DNS
Domain Name Service

DOD
Department of Defense

FTP
File Transfer Protocol

HTTP
hypertext transfer protocol

IAPM
Information Assurance Program Manager

IANM
Information Assurance Network Manager

INFOSEC
information security

IS
Information system

ISSL
Information Systems Security Liaison

LAN
local area network

LIWA
Land Information Warfare Agency

NIPRNET
Non-classified Internet Protocol Router Network

NNTP
Network News Transport

OPSEC
operations security

PAO
Public Affairs Office

SBU
Sensitive but Unclassified

TCP/IP
Transmission Control Protocol/Internet Protocol

WWW
World Wide Web

Section II
Terms

Accreditation
The formal declaration by the DAA that the IS is approved to operate in a particular security mode using a prescribed set of safeguards.

Browser
A browser is a computer application that allows a user to view information on the World Wide Web. At a minimum, browsers are able to display information they receive in the hypertext markup language. The browser provides two basic navigation operations: to follow a link or to send a query to a server.

Compromise
A violation of the security policy of a system such that unauthorized disclosure of sensitive information may have occurred.

Cookie
A cookie is a handle, transaction ID, or other token of agreement between cooperating programs. "I give him a packet, he gives me back a cookie." Something passed between routines or programs that enables the receiver to perform some operation; a capability ticket or opaque identifier. Especially use of small data objects that contain data encoded in a strange or intrinsically machine-dependent way (e.g., on non-UNIX operating systems with a non-byte-stream model of files, the result of "ftell" may be a magic cookie rather than a byte offset; it can be passed to "fseek," but not operated on in any meaningful way). The phrase "it hands you a magic cookie" means it returns a result whose contents are not defined but which can be passed back to the same or some other program later.

Daemon
Pronounced “demon.” A process that runs in the background and performs a specified operation at predefined times or in response to certain events. Typical daemon processes include print spoolers, E-mail handlers, and other programs that perform administrative tasks for the operating system.

Domain Name Service (DNS)
Domain Name Service is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.microsoft.com would be translated to 198.105.232.4. You can see that they're the same by substituting the number for the name in the URL http://www.microsoft.com and entering it in a Web browser. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

File Transfer Protocol (FTP)
A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network.

Firewall
A dedicated gateway machine with special security precautions on it, used to service outside network, especially Internet, connections and dial-in lines. The idea is to protect a cluster of more loosely administered machines hidden behind it from crackers. The typical firewall is an inexpensive, microprocessor-based UNIX machine with no critical data, with modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster. The special precautions may include threat monitoring, call-back, and a complete iron box keyable to particular incoming IDs or activity patterns.

Home page
The top-level Web document relating to an individual or institution. This often has a Uniform Resource Locator (URL) consisting of just a hostname. All other pages on a server are usually accessible by following links from the home page.

Hypertext Transfer Protocol (HTTP)
The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.

Information system
Computer hardware, software or firmware used to collect, create, communicate, disseminate, process, store, and control data or information.

Intranet
A network based on TCP/IP protocols belonging to an organization accessible only by the organization's members, employees, or others with authorization. An Intranet Web site looks and acts just like any other Web site, but the firewall surrounding an Intranet fends off unauthorized access.

Intranet server
Refers to a server that uses security or access controls to strictly limit access to authorized users by employing security features such as firewalls to control access to other Internet and Intranet servers and authorized Intranet users.

Internet
A collection of a worldwide "network of networks" that uses the transmission control protocol/internet protocol (TCP/IP) for communications. The Internet is the largest internet in the world. It is a three level hierarchy composed of backbone networks (e.g. ARPAnet, NSFNet, MILNET), mid-level networks, and stub networks. These include commercial (.com or .co), university (.ac or .edu) and other research networks (.org, .net) and military (.mil) networks and span many different physical networks around the world with various protocols including the **Internet Protocol.**

Internet Host
An Internet host is any computer or computer network that serves as a repository for services available to other computers on the Internet. Internet hosts typically offer services such as E-mail, file transfers protocol, Web, or text search services.

Intrusion
Any unauthorized attempt to gain access to networks, workstations, files or services.

Network News Transport Protocol (NNTP)
NNTP is the protocol used to post, distribute, and retrieve USENET messages.

Sensitive but Unclassified (SBU) Information
Information for which loss, misuse, unauthorized modification, or unauthorized disclosure could affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code; but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

Transmission Control Protocol/Internet Protocol (TCP/IP)
The de facto standard Ethernet protocols incorporated into 4.2BSD UNIX. TCP/IP was developed by DARPA for internetworking, encompassing both network layer and transport layer protocols. While TCP and IP specify two protocols at specific layers, TCP/IP is often used to refer to the entire DOD protocol suite based upon these, including Telnet and FTP.

Telnet
An Internet capability that allows a user to connect to another Internet computer and use that system remotely.

Uniform Resource Locator (URL)
A standard for specifying an object on the Internet, such as a file or a newsgroup. URLs are used extensively on the World Wide Web. They are used in HTML documents to specify the target of a hyperlink. Examples of URLs are:

ftp://www.usarc.army.mil/USARCForms
http:// www.usarc.army.mil/index.html

The part before the first colon specifies the access scheme or protocol. The part after the colon is interpreted according to the access scheme. In general, two slashes after the colon introduce a hostname (host:port is also valid, or for FTP user:passwd@host or user@host). Schemes include: FTP, HTTP (World Wide Web) or WAIS. The "file" scheme should only be used to refer to a file on the same host, but is often used incorrectly as a synonym for FTP. For an HTTP or FTP URL the next part is a pathname that is usually related to the pathname of a file on the server. The file can contain any type of data but only certain types are interpreted directly by most browsers. These include HTML and images in GIF or JPEG format. The file's type is given by a MIME type in the HTTP headers returned by the server (e.g. "text/html," "image/gif") and is usually also indicated by its filename extension. A file whose type is not recognized directly by the browser may be passed to an external "viewer" application; e.g. a sound player. The last (optional) part of the URL may be a query string preceded by "?" or a "fragment identifier" preceded by "#". The latter indicates a particular position within the specified document. Only alphanumeric, reserved characters (:/?#"<>%+) used for their reserved purposes and "$", "-", "_", ".", "&", "+" are safe and may be transmitted unencoded. Other characters are encoded as a "%" followed by two hexadecimal digits. Space may also be encoded as "+". Standard SGML "&<name>;" character entity encodings (e.g., "é") are also accepted when URLs are embedded in HTML. The terminating semicolon may be omitted if “&<name>” is followed by a non-letter character.

Web page
A page of information typically presented using the hypertext markup language (HTML) and accessible using Internet technology. Web pages may present a variety of information sources from text to a combination of sound, graphics and video.

Webmaster
The person responsible for the development and maintenance of the Web pages at a Web site.

Web Server
The collection of hardware, software and data using World Wide Web technology and hypertext markup language as the means to navigate between Web servers and the documents and resources available on these servers.

World Wide Web
The World Wide Web is an Internet service that permits users to weave information and resources together by using hypertext links. On the WWW, information is represented to the user as a hypertext object in HTML format. Hypertext links refer to other documents by their URLs. These can refer to local or remote resources accessible via FTP, Gopher, Telnet or news, as well as those available via the HTTP protocol used to transfer hypertext documents.