



Change Notice

DIRECTIVE AFFECTED: 1237.10
CHANGE NOTICE NUMBER: 1237.10
DATE: 11/24/97

1. PURPOSE AND SCOPE. To highlight the most significant changes in the **Personal Computers, Network Standards Manual**.

2. SUMMARY OF MAJOR CHANGES. In addition to clarifying the differences between true Local Area Network (LAN) standards and suggestions for LAN implementation, the Program Statement describes the establishment of a number of Technical Reference Manuals (TRMs) to assist staff in technical processes.

Currently, the following TRMs are being published on BOPDOCS in conjunction with this Program Statement:

TRM 1205.01	ARCserve 6.1 Installation and Configuration
TRM 1206.01	Novell Internetwork Client for Windows 95
TRM 1207.01	FMIS PC Applications Installation in, a Network Environment
TRM 1208.01	GroupWise 4.x Installation
TRM 1209.01	GroupWise Message Server NLMS
TRM 1210.01	BOP Internet Software - File Server Setup
TRM 1211.01	VTAM Netnames
TRM 1212.01	NETX Novell Client Software
TRM 1213.01	BOP Internet Software - Workstation Setup
TRM 1214.01	NetSoft Gateway
TRM 1215.01	Netsoft Elite Workstation Program
TRM 1216.01	Netsoft Elite Plus Workstation Program
TRM 1217.01	Netsoft Gateway Control Program
TRM 1218.01	Novell/WordPerfect/Corel Shared Code
TRM 1219.01	SimPC Software
TRM 1220.01	Windows 95
TRM 1221.01	WordPerfect 5.1+ for DOS

TRM 1222.01 WordPerfect 6.1 for Windows
TRM 1223.01 WordPerfect 7 (32-bit)
TRM 1224.01 WordPerfect 8

Future TRMs will be published as needed. TRMs will not be published on paper but will be accessible only on BOPDOCS.

4. ACTION. File this Change Notice in front of the **Personal Computers, Network Standard Manual**.

/s/
Kathleen M. Hawk
Director



Program Statement

OPI: OIS
NUMBER: 1237.10
DATE: 11/24/97
SUBJECT: Personal Computers,
Network Standards
Manual

1. PURPOSE AND SCOPE. To establish standards for personal computer networks used in the Bureau. This Program Statement applies to all Bureau Novell/NetWare networks supported by the Office of Information Systems (OIS) or those that are a part of BOPNet. This Program Statement will be amended later to cover additional servers, such as Oracle Database/Application servers.

This Program Statement does not apply to Federal Prison Industries MCS or ADP/Data Services networks. Inmate education networks must adhere to the standards in Chapter 10 and Federal Prison Point-of-Sale (FPPOS) networks must adhere to the standards in Chapter 11.

2. PROGRAM OBJECTIVES. The expected results of this program are:

a. Each Bureau facility will be interconnected via Local Area Networks (LAN) establishing a Wide Area Network (WAN).

b. A standard approach to LAN and WAN configuration and administration will be established throughout the Bureau.

3. DIRECTIVES AFFECTED

a. Directives Rescinded

PS 1237.08 Personal Computers Network Standards Manual
(01/24/94)

b. Directive Referenced

PS 1237.11 Information Security Programs (10\24\97)

4. STANDARDS REFERENCED. None.

5. NETWORK ADMINISTRATORS. Each Bureau personal computer LAN, except those exempted, must have a Network Administrator designated in writing by the appropriate Assistant Director, Regional Director, or Chief Executive Officer (CEO).

Network Administrators shall establish and maintain the computer systems for which they are responsible in accordance with this Program Statement. They are also responsible for informing all new network users about LAN security and data access procedures and for providing refresher training as needed (for example, in annual training).

- On an institution's or regional office's main administrative network, the Network Administrator shall be a member of the Computer Services Department. The CEO may designate another staff member as administrator when the CSM position is vacant.
- On departmental networks, the Network Administrator may be any Bureau employee with training in Novell network management and designated by the CEO.
- A copy of the designation, with the administrator's name, title, and telephone number shall be sent to and kept on file by the Chief of Technical Support, OIS, in the Information, Policy and Public Affairs Division.
- If there is a change in the designated administrator, notification of the change must be immediately forwarded to the Chief of Technical Support, OIS.

The Network Administrator has "supervisory" privileges on the system and is responsible for maintaining network security and reliability. In order to be able to accomplish these tasks, the Network Administrator shall have:

- Full rights to all files stored on the file server.
- Training in Novell NetWare administration.

Network Administrators' technical responsibilities may be found in Chapter 7 of this Program Statement.

6. NETWORK STANDARDS AND TECHNICAL INFORMATION. Technical requirements for operating networks are in the various Sections in this Manual. While general network standards and policy related to networks will be issued in revisions to this Manual as needed, specific technical information and specific staff direction for network implementation and operation of computer software shall be issued in the form of Technical Reference Manuals classified in the 1200 Subject Classification Series.

The TRMs will only be available in electronic form on BOPDOCS. Sensitive information will not be made part of the TRMs on BOPDOCS but will be available through controlled limited distribution. Documents that are deemed to require limited distribution can be obtained from Technical Support in OIS.

7. COMPLIANCE. Any LAN installed after the effective date of this Program Statement shall comply with all standards listed in this Program Statement.

Existing LANs shall be reconfigured to meet these standards within 120 days of the effective date of this Program Statement.

/s/
Kathleen M. Hawk
Director

Chapter 1 - Network Structure

Section 1.0 - Naming Conventions. As the Wide Area Network (WAN) is built, naming conventions are important to make sure that there are no conflicting device names.

- Most of these naming conventions make use of the three character SENTRY codes for each Bureau location (SENTRY ID). Use of this SENTRY ID will assist in ease of tracking locations of advertising devices.
- Some of the naming conventions make use of the three digit allotment code that is the prefix for the property numbers at a location. For the remainder of this document, this number shall be referred to as the ALLOTMENT CODE.
- The naming conventions below indicate that most items have alphanumeric codes as part of their names. In these cases the first such device should be numbered as "1" (or "01", where two characters are required), the second as "2" (or "02"), etc. Existing devices that make use of non-sequential alphanumeric codes are not required to be renamed.
- Many of the naming conventions make use of the underscore character to separate parts of the name. These underscores are used to increase the readability of the names, especially when they appear in long lists. However, there are some devices and software (such as the CD-ROM server software developed by Meridian Data) that do not allow underscores in the device names. Then, the name must follow the published standard without the underscore character.

Any device that advertises itself across the network must have a unique name and shall be registered with the Technical Support staff in the Central Office. This registration can be done over the phone, by written memo or by BOPNet GroupWise e-mail to the Chief of Technical Support, OIS.

Section 1.1 - Basic Information. Any device that advertises itself (i.e., broadcasts its name) across the network must have a name that begins with the three character SENTRY code for the location, followed by an underscore character. If a specific

naming convention for the device is not listed in this Program Statement, the device name must have a length of eight characters (including the SENTRY ID and underscore).

Format: {SENTRY ID} + "_" + {four characters}

Examples: LEX_DV01
NCR_SSS3

Section 1.2 - File Servers - Central and Regional Offices. The name of a file server must be seven or eight characters. The name must begin with:

- SENTRY ID,
- Followed by an underscore, and
- Followed by a unique three or four character string.

Format: {SENTRY ID} + "_" + {three or four characters}

Examples: BOP_OIS
WXR_ISM1

Section 1.3 - File Server - Institutions. The name of a file server must be eight characters. The name must begin with:

- SENTRY ID,
- Followed by an underscore,
- Followed by a three digit description of the server function, and
- Followed by a unique alphanumeric digit that indicates the number of the file server.

If the server function matches any of the functions listed in the table below, then the function codes must be used. In the table below, the word "Administrative" is used to indicate the Novell NetWare file server that Bureau staff use for office automation, and that is not dedicated to a specific purpose, such as Access Control.

<u>Server Function</u>	<u>Function Code</u>
Administrative File Server	ADM
Dedicated Access Control Server	ACE
Psychology File Server	PSY

Format: {SENTRY ID} + "_" + {FUNCTION CODE} +
{alphanumeric ID}

Examples: LEX_ADM1
LEX_ADM2
ALD_PSY3

Section 1.4 - CD-ROM Servers - All Locations. The name of a CD-ROM server must be eight characters long. It must have a name that begins with:

- SENTRY ID for the location,
- Followed by an underscore character,
- Followed by the letters "CD", and
- Followed by a two-digit alphanumeric code.

Format: {SENTRY ID} + "_CD" + {2 digit alphanumeric code}

Examples: WXR_CD01
LEX_CD55

Section 1.5 - Mainframe SNA Gateways. These standards apply to any gateway that is not located in the Central Office. The name of a mainframe SNA gateway (regardless of the manufacturer) must be eight characters long. It must have a name that begins with:

- SENTRY ID for the location,
- Followed by an underscore character,
- Followed by the letters "GW", and
- Followed by a two-digit alphanumeric code.

Format: {SENTRY ID} + "_GW" + {2 digit alphanumeric code}

Examples: BOP_GW25
WXR_GW15
LEX_GW01

Section 1.6 - Print Servers - All Locations. The name of a print server must consist of:

- The name of the primary file server to which the print server is associated,
- Followed by an underscore character,
- Followed by a two-digit code representing the type of print server, and
- Followed by a two-digit alphanumeric code.

If desired, the print server name may be further expanded with a short description (up to nine characters) that must begin with an underscore.

The two-digit code representing the type of print server must be descriptive of the software or hardware used to service the print server. The table below lists some examples.

<u>Type of Print Server</u>	<u>2 Digit Code</u>
Novell Print Server (PSEVER)	PS
LANSpool Print Server	LS
HP Jet Direct Card	HP

Format: {File server name} + "_" + {2 digit print server code} + {2 digit alphanumeric code}

Examples: BOP_OIS_LS01
WXR_ADM1_HP02
LEX_PSY3_PS01_BUNIT359

Section 1.7 - Novell Disk Volumes. The names for disk volumes on Novell NetWare file servers shall be as follows:

- The primary system volume (that contains the SYSTEM, PUBLIC, and MAIL directories) must be named "SYS".
- The next volume that is created must be named "VOL1". Subsequent disk volumes must be named "VOL" plus a number one up from the previous volume (i.e., "VOL2", "VOL3", etc.).
- This standard applies to all disk volumes except for other types of devices which mount themselves as Novell volumes (such as CD-ROM devices).

Section 1.8 - Novell IPX Network Numbers. Each Novell 3.1x or 4.x file server has an internal IPX network number. Each network cable segment (i.e, each Token-Ring or Arcnet segment) has an IPX network number.

All network numbers must be unique. All network numbers must be registered with the OIS Technical Support Staff and must match the following convention:

- ALLOTMENT CODE,
- Followed by repeating the ALLOTMENT CODE,
- Followed by a unique two-digit alphanumeric code.

The primary network segment for any new administrative networks must use "01" as its unique two-digit alphanumeric code. The two-digit hexadecimal value of "E4" has been reserved for use in the internal IPX network numbers of FPPOS servers. The two-digit hexadecimal value of "E5" has been reserved for use as the IPX network number for the FPPOS cabling segment.

Format: {ALLOTMENT CODE } + {ALLOTMENT CODE} + {2 digit alphanumeric code}

Examples: 10010015
38338301
234234A9

Section 1.9 - GroupWise Domains - All Locations. Each GroupWise (formally known as WordPerfect Office) domain name in the mail system must be unique. The domain name must consist of:

- SENTRY ID,
- Plus the letters "DOM",
- Followed by a unique one-digit alphanumeric code.

Some GroupWise domains may already exist that follow earlier announced standards. In those cases, waivers to continue using the domain name shall be obtained from in writing from OIS Tech Support.

The name of a GroupWise Domain must be in all uppercase characters.

Format: {SENTRY ID} + "DOM" + {1 digit alphanumeric code}

Examples: WXRDOM1
LEXDOM2

Section 1.10 - GroupWise Domains for Dedicated Message Server Domains in the Central Office. There are dedicated GroupWise domains in the Central Office which are hosts to dedicated message servers for routing GroupWise mail.

The name of a GroupWise Domain must be in all uppercase characters.

Format: {SENTRY ID} + "MS" + {2 digit alphanumeric code}

Examples: BOPMS05
BOPMS12

Section 1.11 - GroupWise Post Offices. Each GroupWise post office name must be unique within a domain. The post office name shall consist of the file server name on which the post office resides:

- **Without** any underscore characters that might appear in that file server name.

Some GroupWise post offices may already exist that follow earlier announced standards. In those cases, a waiver to continue using the post office name must be obtained from in writing from OIS Tech Support. The name of a GroupWise post office must be in all uppercase characters.

Examples: BOPOIS
LEXADM1

Chapter 2 - Accounts

Section 2.0 - Network Accounts. There are five basic types of network accounts:

- Regular user accounts
- Supervisor accounts
- Backup accounts
- Task server accounts
- Guest accounts

The requirements for each type of network accounts are listed below.

Section 2.1 - Regular User Accounts. Regular user accounts, used by most staff members, must have the following characteristics and attributes:

- The Netware user name must be three characters. A user's three initials are used. If the initials are already in use, or the user does not have three initials, the Network Administrator must modify the initials to create a unique three character ID. This is usually done by replacing the middle initial with an "X". No special characters (such as punctuation or underscores) shall be used.
- The user account must have a password.
- The user account must have a full name listed in the bindery in the format of "Last, First." The name must be in proper case.
- The user account password must be required to have at least seven characters.
- The user account must have the "require unique passwords" option enabled.
- The user account password must expire at a maximum of 90 days. Smaller values can be used to force the password to be changed more often.
- The user account must have one simultaneous connection. If there is a legitimate need for multiple connections, this need must be requested in writing or by e-mail by the user's department head and kept on file by the Network Administrator.

- The user account must have at most one grace login. (There are some menu systems that require more grace logins. If this is the case, and it can be proven by the menu system documentation, the number of grace logins may be increased to the minimum required by the menu system.)
- The user account must have a time restriction defined that will force the account to be logged out sometime in every 24 hour period. If it is determined that staff member working in a Control Center or other critical area needs access 24 hours a day, the LAN administrator may grant them that access, provided they receive and keep on file written permission of someone in one of the following positions or higher:
 - Warden
 - Deputy Regional Director
 - Deputy Assistant Director
- On an administrative file server, each regular user account must have a home directory in which to store data files. If there are multiple administrative file servers on the network, the home directory is only required to exist on one of them. The name of the home directory must be the same as the user login name. The user must have all trustee rights in this directory except for the SUPERVISORY and ACCESS CONTROL rights. Users must not store executable files in these directories.
- The user account must not have the SUPERVISORY or ACCESS CONTROL trustee rights in any directory.
- Upon logging into the file server, a security banner must be displayed, indicating that the user is consenting to system monitoring and that unauthorized use of, or access to, the system may subject them to criminal prosecution. The exact text of this message can be obtained from SENTRY terminals or the Computer Security Program Statement.

Section 2.2 - Supervisor Accounts. Supervisor accounts are used by Network Administrators or their alternates for system administration of the network operating system and resources. This section refers to not only the default Novell SUPERVISOR

login ID, but also to all login IDs that are made functionally equivalent to the SUPERVISOR ID. Supervisor accounts must have the following characteristics and restrictions:

- The supervisor account must have a password.
- The supervisor account password must be required to have at least seven characters.
- The supervisor account must have the full name field of the bindery filled in with the name of the supervisor in the format of "Last, First" and a notation that it is a supervisor ID. The name must be in proper case. (Example: "Doe, John -- Supervisor Account")
- The supervisor account must have the "require unique passwords" option enabled.
- The supervisor account password must expire at a maximum of 90 days. Smaller values can be used to force the password to be changed more often.
- Upon logging into the file server, a security banner must be displayed, indicating that the user is consenting to system monitoring and that unauthorized use of, or access to, the system may subject them to criminal prosecution. The exact text of this message can be obtained from SENTRY terminals or the Computer Security Program Statement.
- The supervisor account may be used for daily activities by the LAN administrator or a member of Computer Services.
- The supervisor account is exempt from all regular user account requirements, except for those listed above.

Section 2.3 - Task Server Accounts. Task server accounts are login IDs that specific machines use to perform a specific task on the network. Some examples are login IDs for mainframe gateways, CD-ROM servers, GroupWise Message servers. Task server accounts must have the following characteristics and restrictions:

- The task server account must not be a member of the group "EVERYONE".

- The task server account must have only have Read and File Scan (RF) rights in the PUBLIC and LOGIN directories.
- The task server account must have a descriptive name listed in the bindery full name field.
- The task server account must have only the minimum rights in the directories necessary to complete its given task. If the given task is just to boot up a machine, RF rights are sufficient. If the task entails writing data, more rights will be necessary.
- The task server account must have station restrictions so that it can only login from specific LAN stations.
- The task server account must have a limited number of simultaneous connections.
- The task server ID is not required to have a password.
- The task server ID is not required to have a timeout within 24 hours.

Section 2.4 - Backup Accounts. Backup accounts are login IDs that are made equivalent to the Novell SUPERVISOR ID, but are used expressly for performing backups of the file server disk storage volumes. The backup account can be viewed as a special type of task server account. The backup accounts must have the following characteristics and restrictions:

- The backup account must be supervisor equivalent.
- The backup account must have a descriptive name listed in the bindery full name field. This name must be in proper case.
- The backup account must have station restrictions enabled so that the ID can only login from the machine(s) connected to the backup device.
- The backup account must have a limited number of simultaneous connections.
- The backup ID is not required to have a password.
- The backup ID is not required to have a timeout within 24 hours.

In addition, the machine that contains and/or controls the tape backup device must be in a secure location (i.e., a computer room as defined in the Computer Security Program Statement).

Section 2.5 - Guest Accounts. The use of generic guest accounts is prohibited. Visiting Bureau staff requiring local network access are to be given accounts that match the standards listed for regular user accounts, with the additional requirements:

- The account must have an expiration date listed in the bindery. This expiration date must be equal to the visitor's last known duty date at the location.

Bureau staff requiring access to their home server may use any unused workstation to perform the login. The TRM gives some suggestions for assisting users to access their home server.

Chapter 3 - Directories

Section 3.0 - Directory Structure Standards. A good directory structure is necessary in organizing the thousands of files that are stored on the file server. A common structure helps everyone who must access the system. All Bureau networks must conform to the following directory structure standards:

- The application software directories, and any supporting file directories, must be placed underneath the directory structure **APPS**, which must be placed at the root of a volume.
- All directories for regular user accounts must be named for the user login name and be placed underneath the directory structure **HOME**, which must be placed at the root of a volume.
- All directories shared by groups of users must be placed underneath the directory structure **GROUPS** which must be placed at the root of a volume.
- Applications the Bureau creates and distributes can be placed either under the APPS directory, or underneath a **BOPAPPS** directory, which must be placed at the root of a volume.

Section 3.1 - Standard Drive Mappings. The drive mappings that are used on a file server may vary from one to another, depending upon how the access methods are established for different applications.

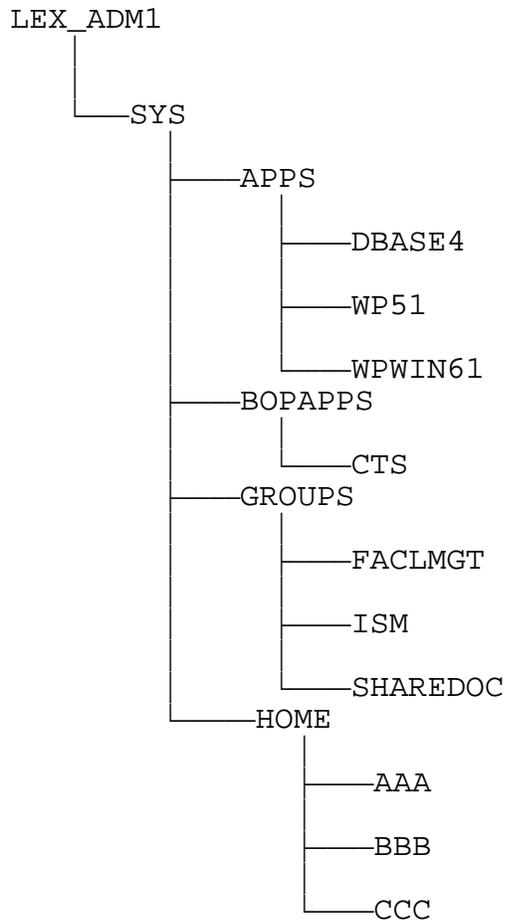
However, all Bureau networks must follow the following drive mapping standards:

- Drive letter H: must be used to map to user home directories.
- Drive letter Z: must be a search drive mapping to the PUBLIC directory of the file server.
- Dynamic search drive mappings for applications must be used as often as possible.

Section 3.2 - Standard Directory Trustee Rights. The directory trustee rights are the key to security on a Novell file server. The following standards apply to regular user accounts and task server accounts. (Note: When the term "full trustee rights" is used, it means all the trustee rights except SUPERVISORY and ACCESS CONTROL.)

- Accounts must have rights only in the directories to which they require access.
- Accounts must not have SUPERVISORY or ACCESS CONTROL directory trustee rights in **any** directory on the file server, including user home directories.

SAMPLE TREE STRUCTURE



- Accounts must have no directory trustee rights at the root level of a volume.
- Accounts must have no directory trustee rights at the APPS or BOPAPPS level of a volume.
- Accounts must have no directory trustee rights at the HOME level of a volume.

- Accounts must have no directory trustee rights at the GROUP level of a volume.
- Accounts must have no directory trustee rights in the SYSTEM directory.
- Accounts must have only READ and FILE SCAN rights in the PUBLIC directory.
- Accounts must have full trustee rights in the home directory corresponding to the account, if such a home directory exists.
- If a user account is a member of a group that has an associated group directory, the account may have full trustee rights to that group directory. However, the trustee rights may be limited to give that user less rights if deemed necessary.
- Accounts shall have the default rights (everything except Access Control and Supervisory) for the automatically created MAIL directories created by the NetWare operating system. The NetWare operating system uses these directories to store user specific information.

Section 3.3 - User Access to Home Directories. Home directories are meant to be private. However, it is sometimes necessary that one user have trustee rights to another user's home directory.

There are two ways that this may be accomplished:

1. The owner of a home directory can request access for other users to his or her home directory or subdirectory thereof. This request must be given in writing and kept on file by the system administrator.

2. If the owner of the home directory is unavailable and it is deemed an emergency to gain access to files in the home directory, the supervisor can grant access to another user only with the written permission of someone in one of the following positions or higher:

- Warden
- Deputy Regional Director
- Deputy Assistant Director

The System Administrator must keep this request and forward a copy to the Bureau's Computer Security Program Manager. Once the files have been retrieved from the directory, the Network Administrator shall reinstate the original access restrictions.

Section 3.4 - Group Directories. Group directories are directories that are shared by one or more users. Group directories may be used for sharing files, accumulating data, or other purposes.

Each group directory must have a primary person or point of contact responsible for who should or should not have access. This point of contact may be the Network Administrator. Any access additions or changes must be submitted in writing or BOPNet GroupWise e-mail and kept on file by the Network Administrator. Users may have no access, partial access or full access to the group directory. All group directories must be created underneath a master GROUP directory off of the root of a volume.

Chapter 4 - Software

Section 4.0 - Application Software. Since software revisions change with a great deal of frequency, publishing standard directory locations and user directory trustee rights for each application program is not practical. Suggestions for directory names and rights for some common applications are given in the technical reference material published by OIS Tech Support. However, the standards listed below must be met by all application software, unless the application program requires otherwise. If that is the case, any deviation from the standard must be supported by program documentation or information provided by OIS Tech Support.

- All application software directories, and supporting file directories, must be placed underneath the directory structure **APPS**, which must be placed at the root of a volume. The exception are applications that the Bureau creates and distributes. These applications may be placed either underneath the APPS directory or underneath a **BOPAPPS** directory. If used, the BOPAPPS directory must be placed at the root of a volume.
- The name of the application software directory must be descriptive of the program name.
- Users must have only Read and File Scan trustee rights in the main application software directory. Additional rights can be granted for certain sub-directories of the application software directory, such as those that contain data or configuration files.
- DOS based applications must have batch files created to automate access to the application, including the mapping of whatever drives are needed by the applications. These batch files must use dynamic mapping of search drives whenever possible.

Section 4.1 - GroupWise. GroupWise is (or will become) the primary means of exchanging electronic mail and scheduling information between the different Bureau locations. Therefore, it is necessary to have more standards for GroupWise directory locations and trustee directory rights than with other applications.

The GroupWise installation must meet the following standards:

- If the file server contains a GroupWise domain, the domain directory must be named the same as the domain and be located underneath the **APPS** directory. These names must follow the requirements listed above.
- If the file server contains a GroupWise post office, the post office directory must be named either the same name as the post office or "**OFF4**" and located underneath the **APPS** directory.
- The "Default Security Level" setting of all GroupWise post offices shall be set to "High."
- User trustee rights and task server rights must follow the information listed in the GroupWise section of the OIS LAN Technical reference documentation.
- The client software must be installed in the default locations (OFWIN40 and OFDOS40) underneath the post office directory.
- If the Domain has an NLM based message server, the message server delivery for that domain must be set to "server always."
- Passwords attached to a GroupWise mailbox must not be shared.
- If proxy rights are assigned to a GroupWise mailbox, the proxy rights must not include the ability to read private messages.
- A user must not have more than one personal mailbox. The user may have access to one or more functional mailboxes.
- Any object (resources, groups, etc.) which do not need to be seen outside of the local system shall have visibility set to "Domain" or "Post Office" or "None." Any object which needs to be seen nationally may have visibility set to "System." Complexes which have multiple GroupWise domains may need to set certain objects to "System" visibility.

Chapter 5 - Servers

Section 5.0 - Server Organization

Section 5.1 - Server Documentation File. Emergencies sometimes make it necessary for someone to fill-in or replace a Network Administrator. In order to give a common location for this information, the Network Administrator must create a documentation file that list pertinent information about the file server and the software that it contains. Printed copies must be placed in the following location: with the tape backup media, with the tape backup off-site storage location, with the Contingency Plans and in the appropriate Associate Warden's office. The requirements for this file are listed below:

- The file name must be the name of the file server with a "DOC" extension.
- The file (and any other supporting, secondary documentation files) must be stored in a SRVDOC directory that must be created underneath the SYSTEM directory of the file server.
- The file must be in ASCII text format, WordPerfect 5.x format or WordPerfect 6.x format.

The file must contain (at a minimum) the following items. If necessary, the items may be listed in separate secondary files.

If this is necessary, the secondary files must be stored in the same locations as the primary file, and the primary file must contain the names of any and all secondary files.

- The file must contain the contents of the file server STARTUP.NCF and AUTOEXEC.NCF files.
- The file must list the disk driver(s) used by the server, along with any needed settings or parameters.
- The file must list the network interface card driver(s) used by the server and the network segment numbers associated with them, along with any needed settings or parameters.
- The file must list any passwords necessary to boot the file server or perform administration functions. This does NOT include Novell passwords. This does include,

but is not limited to the following: power on passwords, password for GroupWise administration (if the password has been enabled), etc.

- The file must list the name of any print servers the file server uses and the software and/or hardware.
- The file must have a section for every application or utility program loaded on the file server, listing the following information about each application:
 - The directories the program uses.
 - The Novell group used to control access to program (i.e., that has trustee rights assigned to it).
 - The license metering method used to control access to the program. This could be that it is licensed by file server, the number of licenses owned is equal to or greater than the number of users who have access, the application is self-metering, a metering program, etc.
 - The name and location of any batch files used to launch the application.
- The file must list the name of the menu system being used. The name and location of any menu files must also be listed.
- The file must list the name and location of any non-standard utilities or programs that are used to access applications. A description of how the utility or program is being used must be included.
- The file must the name and location of any custom written software being used on the network. Program documentation, source code and the name and version of the compiler used must also be included.
- The file must include complete instructions for performing a partial restoration of files from the tape backup.

- The file must include complete instructions for performing a full restoration of file from the tape backup.
- The file must include a list of the normal backup schedule.

Chapter 6 - Gateways

Section 6.0 - Gateway Considerations. Systems Network Architecture (SNA) gateways allow access to the mainframe via terminal emulation software on LAN workstations. As far as physical security, a gateway PC must be treated with the same security concerns as a cluster controller. In addition, the following items apply to the gateway hardware and software:

- Gateway logical units (LUs) must not be shared and must be associated with a unique physical machine. Pooling of LUs and associating LUs with user login IDs are not allowed.
- If the gateway control program (the software that controls the functions of the gateway PC itself) is stored on the file server, it must be stored in the directory APPS\GATEWAYS\{gateway name}.
- The gateway name must match the naming conventions listed in Section 1.5.
- The task server account for the gateway PC must only have Read and File Scan trustee rights to the APPS\GATEWAYS\{gateway name} directory. Users must have no trustee rights to this directory.
- If the NSA Elite workstation client software is stored on the file server, it must be stored in APPS\GATEWAYS\ELITE directory. Users must only have Read and File Scan rights to this directory.
- If the NSA Elite Plus workstation client software is stored on the file server, it must be stored in the APPS\GATEWAYS\ELITEP directory. Users must only have Read and File Scan rights to this directory.
- CFG3270E and CFG3270P must be taken out of ELITE and ELITEP directories and placed into another directory called APPS\GATEWAYS\ELCFG. User accounts must have no trustee directory rights to this directory.
- If the NSA Dynacomm Elite workstation client software is stored on the file server, it must be stored in the APPS\GATEWAYS\DE3270 directory. Users must have only READ and FILE SCAN rights in this directory.

There is a technical support document available discussing how to secure gateway sessions. This document has limited distribution and must be requested directly from OIS Technical Support.

Chapter 7 - Network Administrators

Section 7.0 -Network Administrator Responsibilities. The Network Administrator's responsibilities include ensuring (at a minimum) the following:

- All standards in this document are adhered to, or a written waiver has been obtained from OIS Tech Support and placed on file.
- The file server is backed up to tape daily. The file server must have a full backup at least twice a week, with at least incremental backups on the remaining days. Backups on weekends and holidays can be incremental backups.
- Tape backups are labeled and stored as required in the Computer Security Program Statement.
- The appropriate security background check has been scheduled before new users are added to the network, as required by the Computer Security Program Statement.
- User accounts are removed in a timely manner, as required by the Computer Security Program Statement. User files for departed staff must be backed up and stored as required by the Computer Security Program Statement.
- Users must be informed of the issues relating to remote support operations that require remote control software. Users must give consent before remote control software may be used.
- The network file server is scanned for viruses and any viruses that are found must be removed and reported in accordance with the Computer Security Program Statement.
- Users are trained in network security and in proper login/logout procedures
- All software on the network file server is legally licensed and is being properly metered for simultaneous use.
- Shared printers on the network are created, maintained, and deleted when necessary.

- Network hardware components and peripherals must be maintained. Any contractors performing hardware maintenance and/or repair must be supervised.
- Software on the network is properly installed and the appropriate access rights are assigned.
- All task server machines must be properly installed, configured, and maintained. These include, but are not limited to, print servers, mainframe gateways, CD-ROM servers, fax servers, etc.
- Any staff performing supervisor functions on the network must have sufficient training to complete those tasks.

Chapter 8 - Network Requirements

Section 8.0 - Network Requirements

- An unrestricted supervisor equivalent ID must be established for each current member of OIS Tech Support. This ID will only be used for emergency assistance and troubleshooting. The names of the OIS Tech Support staff and associated network IDs can be obtained from OIS Tech Support.
- An unrestricted supervisor equivalent ID must be established for the appropriate Regional Computer Services Manager.
- Local Area Network used by staff for administrative functions must use the Token-Ring network topology. Locations that have Arcnet networks for administrative staff may continue to use Arcnet while planning and installing Token-Ring networks.
- Users must not install software on the file server. Furthermore, the user home directories shall not contain executable programs. The users shall be instructed that any software that is distributed via e-mail or other automated sources shall be saved to their local hard drive or to diskette.
- The network protocol used on LANs must be IPX. Any use of IP must have prior written approval by OIS Tech Support.
- A menu system is required for accessing network applications. This requirement may be met by a version of Microsoft Windows running on individual workstations.

Chapter 9 - Workstations

Section 9.0 - Workstation Requirements

- The Novell 16-bit DOS client software (NETX or VLM) must be located in a directory off of the root of the C: drive with a descriptive name, such as C:\NET, C:\NWCLIENT or C:\NOVELL.
- External network adapters (i.e., those that plug in to an external port on a PC, such as a parallel port or a PCMCIA slot) must be treated with the same security concerns as external modems as required in the Computer Security Program Statement.

Chapter 10 - Inmate Education Networks

In addition to the standards contained in the Computer Security Program Statement, any LAN used for inmate education purposes must also follow these standards:

- The inmate education LAN must not be interconnected with the institution administrative LAN in any way.
- Inmate education networks must not use the Token-Ring topology.

Chapter 11 - FPPOS Networks

The Federal Prison's Point-of-Sale networks are special systems set up and controlled by the Trust Fund branch of the Administration Division of the Central Office. Since they serve a specialized purpose, they are not subject to the same requirements as administrative networks. However, any FPPOS network which is connected to the Bureau wide area network must meet the following requirements.

- The FPPOS file server name shall be:
 - "FPPOS"
 - Followed by an underscore, and
 - Followed by the SENTRY ID

Format: "FPPOS_" + {SENTRY ID}

Examples: FPPOS_LEX
FPPOS_MAN

- Any FPPOS device or resource that advertises itself over the network (such as a print server) must not duplicate the name of any other BOPNet device. Furthermore, this name shall contain the SENTRY ID in some part of the name to identify its location.
- FPPOS networks must follow the standard numbering convention for Novell IPX network numbers listed in section 1.8. The two-digit hexadecimal value of "E4" has been reserved for use in the internal IPX network numbers of FPPOS servers. The two-digit hexadecimal value of "E5" has been reserved for use as the IPX network number for the FPPOS cabling segment.