Windows NT 4.0
Server Security Guideline
v1.0

May 29, 1998

National Aeronautics and Space Administration
Office of Headquarters Operations
Information Technology and Communications Division

Windows NT 4.0 Server Security Guideline
Table of Contents

1. INTRODUCTION.....1

1.1 PURPOSE.....1
1.2 SCOPE.....1
1.3 OVERVIEW OF WINDOWS NT SECURITY MODEL.....2
1.4 WINDOWS NT AND C2.....3
1.5 HOW TO USE THIS DOCUMENT.....4

2. SERVER INSTALLATION AND CONFIGURATION.....5

2.1 HARDWARE CONSIDERATIONS.....5
2.1.1 Hardware Compatibility List.....5
2.2 PHYSICALLY SECURING SERVER AND SOFTWARE.....5
2.2.1 BIOS and Firmware.....6
2.2.2 Physical Security Configurations.....7
2.3 DISK REDUNDANCY: STRIPE SETS AND MIRROR SETS.....8
2.4 SERVER TYPE: PDC, BDC, SERVER.....9
2.5 USERS.....11
2.5.1 Configuring and Controlling Access to User Manager.....11
2.5.2 User Accounts.....11
2.6 USER ACCOUNT POLICY.....12
2.6.1 Assigning User Rights.....13
2.6.2 Configuring User Account Settings.....18
2.6.2.1 Creating User Templates.....18
2.6.2.2 Built-in User Accounts.....19
2.6.2.2.1 Guest Account.....19
2.6.2.2.2 Administrator Account.....19
2.7 GROUPS.....20
2.7.1 Assigning Users to Groups.....20
2.7.2 Built-in Groups.....21
2.7.2.1 Built-in Local Groups.....21
2.7.3 Global Groups.....22
2.7.3.1 Built-in Global Groups.....22
2.7.4 Special Groups.....23
2.8 SYSTEM POLICY.....23
2.8.1 System Policy Configurations.....24
2.8.2 Implementing System Policies.....24
2.8.2.2 User Rights.....26
2.8.3 Creating System Policies.....26
2.8.3.1 System Policy Troubleshooting.....33
2.8.4 Configuring NT Server to Display Legal Notice.....33

2.9 WINDOWS NT AUDITING....34
2.9.1 Configuring Audit Events....34
2.9.2 File Auditing....35
2.9.3 Registry Key Auditing....36
2.9.4 Print Auditing....36
2.9.5 RAS Auditing....37
2.9.6.1 Searching for Events....41
2.9.7 Archiving Event Logs....42
2.9.8 Audit Log Reporting Utilities....42
2.9.8.1 Crystal Reports....42
2.10 IMPLEMENTING SERVER TCP/IP ADVANCED SECURITY....45
2.10.1 Using Advanced TCP/IP Security at the Server to Mitigate Security Threats....45
2.10.2 Configuring TCP\IP Advanced Security....46
2.11 RECYCLE BIN....47
2.12 ASSIGNING FILE, DIRECTORY, AND REGISTRY PERMISSIONS....47
2.12.1 NTFS Default Configuration....47
2.12.2 Subdirectory Creation....48
2.12.3 The File Protection Model....48
2.12.4 Setting Permissions in Windows NT 4.0....50
2.12.5 Permissions for the Windows NT System Directories....51
2.12.6 Disable POSIX and OS/2 Subsystems....58
2.13 NTFS MOVE/COPY....58
2.14 PROTECTING APPLICATION FILES....60
2.15 DIRECTORY REPLICATOR SERVICE....60
2.16 CONFIGURING PRINTERS....61
2.16.1 User Restrictions....61
2.16.2 Copying Files to the LPT Port....61
2.17 REMOTE ACCESS/DIAL-UP NETWORKING....61
2.17.1 Prohibited RAS Use....61
2.18 PASSWORD-PROTECTED SCREEN SAVER....63
2.19 SERVICE PACK 3....63
2.20 WIPING SYSTEM PAGE FILE....64

3. SERVER ADMINISTRATION....62

3.1 LOG ON/LOG OFF....62
3.2 EMERGENCY REPAIR DISK....62
3.3 LAST KNOWN GOOD CONFIGURATION....63
3.4 LOG ON CREDENTIALS FROM DOMAIN SERVER....63
3.5 PERFORMING SYSTEM SECURITY AUDITS....64
3.6 ADD-INS FOR WINDOWS NT COMPONENTS....64
-....64
3.7 BACKUPS....65
3.7.1 Backup Products....66

3.7.1.1 Legato NetWorker for NT......66
3.7.1.2 ARCserve......66

4. THIRD PARTY SYSTEM AUDITING AND ANALYSIS UTILITIES......69

4.1 KANE SECURITY ANALYST 4.0......69
4.1.1 Software Features......70
4.1.2 KSA Reports......71
4.2 SOMARSOFT DUMPACL......72
4.3 C2 SECURITY MANAGER......72

Appendix A - Acronyms
Appendix B - Windows NT 4.0 Server Security Configuration Checklist

1. INTRODUCTION

This document was created to assist system administrators meet their information protection goals, and to satisfy the policy requirements[1]. **System administrators may need to alter the recommended security configuration where it constrains necessary functionality**. For example, implementing a Web server on NT may require a loosening of the recommendations regarding TCP/IP security. Changes to the recommended Windows NT configuration should be viewed as a risk management decision, and the system administrator and security officer should make every effort to work within the intent of the established policy. Contact the Security Team if you require additional information.

Windows NT was designed with a uniform security architecture that meets the requirements for a C2 rating by the National Computer Security Center (NCSC). One requirement of the C2 class is the ability to enforce discretionary access control between named users and named objects (e.g., files, programs, printers, etc.) by default or explicit user action. While NT provides the means to enforce controlled access protection, modifications to the default installation configuration are required. System administrators and developers must not assume that the installation of off-the-shelf copies of Windows NT (workstation or server) is sufficient to secure a processing environment. Although many of the initial settings in Windows NT restrict user access by default, changes are required to meet policy and prevent unauthorized access. This document identifies the appropriate values that should be established within the default settings.

1.1 Purpose

This document is intended to provide system administrators the standardized security configuration for NT servers. Absent is a detailed discussion on NT internal processes and specific application information protection guidance. A working knowledge of NT system administration tools and their capabilities is assumed. This document will provide guidance on configuring user accounts, as well as modifying default values for users, groups, file permissions, and access rights.

1.2 Scope

Information in this plan is applicable to the Windows NT Server Version 4.0. This document does not include guidance on configuring office specific or locally developed applications – it is intended to be dynamic with modifications when required.

[1] The following sources were used in the development of this document:

- NSA's *Guide to Implementing Windows NT in Secure Network Environments*;
- Department of State's *Windows NT Security Guide*; and
- Various additional documents on NT security.

1.3 Overview of Windows NT Security Model

Security is an integral part of Windows NT, not an add-on product. Windows NT security affects the entire operating system. The NT security model consists of the:

- Security Reference Monitor (SRM);
- Local Security Authority (LSA); and
- Security Account Manager (SAM).

Each component is interdependent upon the others and performs specific functions. Briefly, the LSA creates access tokens during log on, manages the security policy, controls the audit policy, and logs audit messages to the event file. The SAM maintains the security account database, which contains all user and group accounts. The SRM enforces the policy established in LSA, validates users access to objects, and contains the only access validation code in the system. These components represent a low-level view of Windows NT security and are displayed in **Figure 1.3-1**.

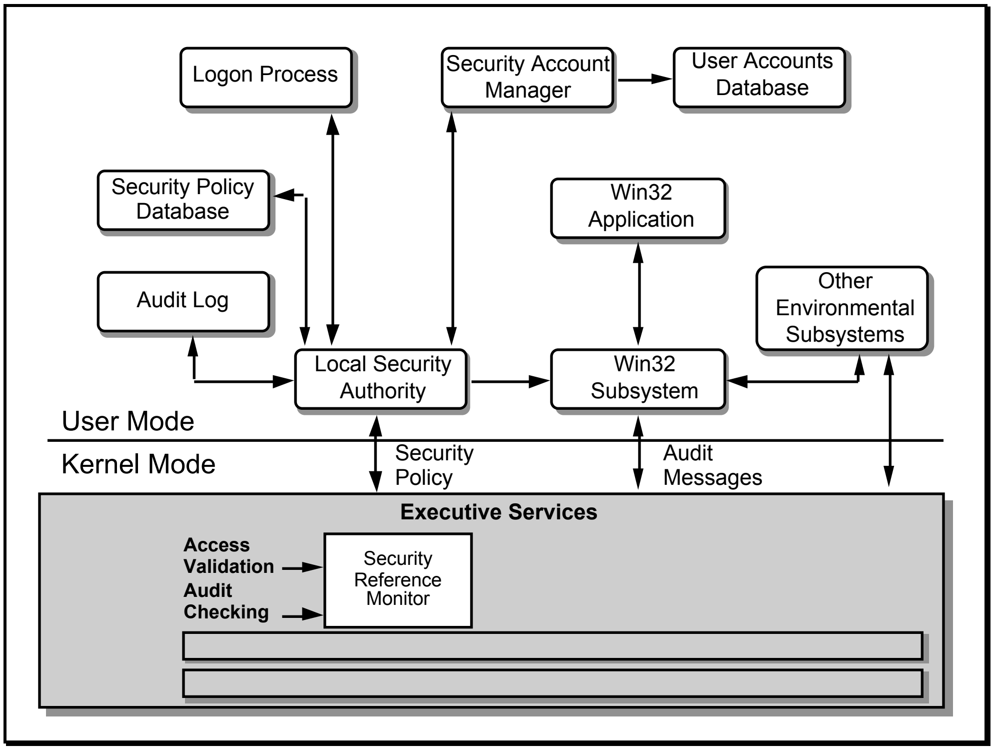


Figure 1.3-1

To Windows NT, all system resources are regarded as 'objects'. Each object can have an associated access control list (ACL) which specifies information to allow or disallow actions based on the subject attempting access. An ACL is composed of access control entries (ACEs), each of which identifies a specific user or group and the permissions designated for that subject to act on the object. The SRM scans an object's ACL entries to see if a subject can access the object, based on permissions listed in ACEs for the aggregate identification of the subject and of what groups the user is a member. The system administrator is provided with several management tools to implement security within NT:

- User Manager – for user account management;
- System Policy Editor – for implementing system policies;
- Windows NT Explorer – for file and directory management;
- Print Manager – for printer management; and
- Server Manager – for server resource management.

Where applicable, guidance has been provided for pre-defined settings within these services.

1.4 Windows NT and C2

According to NCSC's *Trusted Computer System Evaluation Criteria*, a system must meet the following areas in order to meet the C2 requirements:

- Each user must be clearly and uniquely identified;
- The operating system must provide Discretionary Access Control;
- Audit trails must be able to track security-related activities;
- The operating system must protect against object reuse; and
- The operating system must be protected against tampering with either the system files in memory or on disk.

The NCSC rated Windows NT server Version 3.5, with U.S. Service Pack 3 with a C2 level of trust. The rating, however, was only granted in a stand-alone configuration. It did not extend to a networked environment.

✿ Windows NT 4.0 can be configured to implement the changes necessary to achieve a C2 level of trust. As with version 3.5, any system that is connected to any type of network will not be able to achieve a C2 level of compliance. This risk must be taken into consideration and managed[2].

[2] Reference Section 1.5 for description of this symbol.

1.5 How to Use This Document

This document consists of four sections and two appendices. The first section, Introduction, acquaints the reader with the purpose of the document. It alerts the reader to specific icons throughout the document. These icons represent:

★ **Mandatory**. This icon represents specific configuration directions necessary to achieve and maintain the secure NT architecture.

👍 **Recommendations.** This icon suggests recommendations that should be implemented at the discretion of the system administrator.

💣**Warning.** This icon alerts the reader to **use caution** when implementing the requested recommendation. Many of these warnings will appear in connection with the Registry Editor configurations. Using the Registry Editor incorrectly can cause serious, system-wide problems, which may require you to reinstall Windows NT to correct them. **Use this tool with caution.**

✿ **Not Applicable**. Does not apply in the current NASA environment, but may change with future configurations.

Sections 2 and 3 are specific to installation, configuration, and administration of Windows NT 4.0 on **Servers**. Section 4 details Third Party System Auditing and Analysis Utilities to be utilized for security purposes in conjunction with Windows NT 4.0.

Appendices includes a list of acronyms used throughout this document and a checklist of the security configuration for the server. Additionally, an Index is included at the end of the document.

Windows NT 4.0 Workstations Security Configuration Guide is the companion document to the *Windows NT 4.0 Server Security Configuration Guide*.

2. SERVER INSTALLATION AND CONFIGURATION

The security configuration discussed in this document applies to a new or existing installation of Windows NT Server. In most cases, no distinction will be made.

★ Computers running Windows NT (New Technology) must not be configured to run under a second operating system, such as DOS or Windows, to become Dual-Boot systems. Windows NT systems must use only NT file system (NTFS) partitions and not have any file allocation table (FAT) partitions used by DOS or Windows, or any high-performance file system (HPFS) partitions used by OS/2 systems.

2.1 Hardware Considerations

2.1.1 Hardware Compatibility List

👍 **Recommendation:** Only hardware listed on the Microsoft Hardware Compatibility List should be used in a computer running Windows NT. As of the writing of this document, the latest Microsoft Hardware Compatibility List can be found at *ftp://ftp.microsoft.com/bussys/winnt/winnt-docs/hcl/*. If the hardware does not appear on the list, check with the manufacturer to determine whether a Windows NT software driver exists.

💣 Using hardware that does not conform to Windows NT standards may cause serious compatibility problems and have potential security consequences.

2.2 Physically Securing Server and Software

System hardware and software installation disks that have not been physically secured can make the operating system and data stored on hard drives vulnerable. For example, a PC's floppy drive can easily be used to subvert the operating system's controls if certain precautions are not taken. Booting from a DOS floppy and then running a simple shareware program called NTFSDOS.EXE allows the contents of an NTFS formatted hard drive to be read. Likewise, software can be installed and then used to recover an Administrator's password to gain unauthorized control of the operating system. On occasion, the subversion can be unintentional, such as allowing the floppy device to be part of the boot sequence and accidentally booting from a virus infected disk that releases malicious and damaging code.

The four major threats to the physical security of a server are:

1. Removing the hard drives or removing the entire computer for the purpose of obtaining unauthorized access to data stored on the hard drives.

2. Installing software that can be used to compromise or circumvent security, such as: installing a second copy of the Windows NT operating system into another directory and then accessing sensitive data or controlling the operating system; installing a program to create a known administrator's account and then accessing sensitive data or controlling the operating system; or introducing software, such as a virus, that when executed, has damaging and destructive effects.

3. Bypassing the operating system by booting from a floppy and using a simple shareware program such as NTFSDOS.EXE to read sensitive data contained on the hard drive.

4. Using a brute force attack to crack the administrator's password, whereby gaining unrestricted access to sensitive data and control over the operating system.

2.2.1 BIOS and Firmware

✿ Newer workstations include Year 2000 compliant basic input-output system (BIOS) chips with firmware level security provisions. Physical security of the individual workstation, and therefore local-area network/wide-area network (LAN/WAN) resources, can be enhanced by using BIOS password options accessible through the BIOS complementary metal oxide semiconductor (CMOS) setup menu. One or two password choices are offered. If only one password is offered, it is used to protect the system during initial startup by not allowing the operating system to start until the proper password has been entered. A two password system uses one password for initial system startup, while the second is used to protect the BIOS from modification.

✿ Other security provisions provided by the BIOS include removing the floppy devices from the boot sequence or disabling the floppy devices altogether. Removing the floppy drive from the boot sequence reduces the vulnerability to attack by an unauthorized operating system, viruses, sector editor tools, or a LAN sniffer attack from PC-based network card drivers. Disabling the floppy completely will protect against unauthorized software installation that can be used to compromise security, or to prevent the transfer of data from the computer. Enabling these features will enhance the security protection provided by Windows NT.

👍 **Recommendation**: If BIOS passwords are to be implemented, the passwords must be managed by the same systems staff who assign and distribute passwords for Windows NT users. BIOS passwords must be created with the same procedures and format as other system passwords, and must be different from Windows NT user IDs or passwords.

★ BIOS must be Year 2000 Compliant.

2.2.2 Physical Security Configurations

The recommended precautions to safeguard hardware and the Windows NT operating system are:

- Physically restrict and limit access to hardware, particularly any configured as Windows NT Servers. Servers should be housed in the computer room.
- Physically secure the hard drives by locking them in place, or locking the case to prevent unauthorized removal of the media.
- Force Domain Administrators to log on to any Windows NT Server locally.
- Disable the floppy drives through the BIOS to prevent it from being used as a boot device, and to prevent unauthorized installation of software.
- Password protect the BIOS to prevent the floppy drives being activated without authorization.
- Physically secure software, particularly the Windows NT installation disks and CDs.

👍 **Recommendation**: Management and system administrators should implement all precautions listed above for servers, since they present a larger target to be penetrated maliciously, and can cause the most disruption to users if done so.

★ Virus scanning software must be installed and regularly used to detect and remove viruses.

2.3 Disk Redundancy: Stripe Sets and Mirror Sets

To better protect data on a Windows NT Server from loss if a hard drive fails, it is recommended that some form of disk redundancy be implemented. By copying or distributing data over multiple disks, the data can be quickly and accurately recovered if a hard drive fails. Implementing fault tolerance using redundant array of inexpensive disks (RAID) methods can also provide improved data transfer performance to and from the disk.

👍 One of the following methods of disk redundancy should be used.

- **RAID 1 -** Disk mirroring. Two drives store identical information so that one is a mirror of the other. The system writes identical information to both disks. The dual write operations can degrade system performance. **By using duplexing, where each mirror drive has it own host adapter, performance can be improved**. The mirror approach provides good fault tolerance. However, because only half of the available disk space can be used for storage while the other is used for mirroring, it is relatively expensive to implement.

- **RAID 5 -** Disk striping with parity. This method of providing fault tolerance uses from three to 32 disks. Data is distributed, or striped over multiple disks. The check data, or parity data is striped across all disks in the group. The primary fault tolerant benefit of RAID 5 is that any failed disk in the group can be replaced and the data regenerated without loss. **The performance benefit of the RAID 5 distributed check data approach is that it permits write operations to take place simultaneously and multiple reads to take place simultaneously**. Additionally, it is efficient in handling small amounts of information.

RAID Hardware Considerations:

- RAID 1 can be implemented using a minimum of one disk controller and two hard drives of similar size. To use the duplex method, two disk controllers are required and two hard drives of similar size.
- RAID 5 can be implemented using a minimum of three hard drives of similar size. However, a special hard drive controller card designed for multiple reads and writes will be needed.

👍 **Recommendation:** When possible, implement disk redundancy. Be sure to use disk redundancy hardware that conforms to Microsoft's Hardware Compatibility List and to the specifications of other computer manufacturer's equipment.

2.4 Server Type: PDC, BDC, Server

When installing Windows NT, the choice between three types of servers must be made:

- Primary Domain Controller (PDC);
- Backup Domain Controller (BDC); and
- Server.

A domain in a Windows NT environment consists of a logical collection of computers sharing a common user accounts database and security policy. A domain also provides log on validation to ensure that domain user accounts and security policies are enforced within the domain.

Within each domain, all domain controllers that run Windows NT Server comprise a single administrative unit to manage all aspects of user-domain interactions. They share one directory database to store security and user account information for the entire domain. Domain controllers use the information in the directory database to authenticate users logging on to domain accounts.

There are two types of domain controllers. The PDC tracks changes made to domain accounts and stores the information in the directory database. Therefore, central processing unit (CPU) resources are used to process logons and replicate the security database to BDCs. A domain has one PDC. The BDC maintains a copy of the directory database, which is periodically synchronized with the directory database on the PDC. A domain can have multiple BDCs and a BDC can be promoted to a PDC.

Once a PDC or BDC is installed in a particular domain, it is committed to that domain. Because a unique identifier, called a security identification (SID), is created during installation and used for all accounts on the domain, **neither can be moved to another domain without reinstalling Windows NT**.

The domain structure provides the following advantages for maintaining a secure network:

- Single Log on Procedure. Network users can connect to multiple servers by logging on to a single domain.
- Universal Resource Access. The user needs only one domain user account and password to use network resources.
- Centralized Network Administration. A centralized view of the entire network from any workstation on the network provides the ability to track and manage information on users, groups, and resources in a distributed network. This single point of administration for multiple servers simplifies the management of a Windows NT Server-based network.

Five different levels of security can be set for user actions on the domain as a whole:

1. The Account Policy controls how user accounts use passwords.
2. The User Rights Policy controls access rights given to groups and user accounts. User rights are applied at the domain level and affect overall domain security.
3. The System Policy creates profiles that control the Windows NT environment.
4. The Audit Policy controls the types of events the security log records.
5. The Trust Relationships Policy controls which domains are trusted and which domains are trusting. A trust relationship requires two or more domains.

Details on establishing and maintaining these policies are described in more detail throughout this section and in Section 3, Server Administration.

A Windows NT Server that is not configured as a PDC or BDC is defined as a Server. **The distinguishing characteristic of a Server is that it does not process domain logons**. The server allows the system administrator to mix and match security – accounts may be created in the local security database and assigned to local resources. Any of the domain accounts (and accounts from trusted domains) can be assigned to local resources if the server is a member of a domain. **Also, a server is easier to move to a different domain and can change its domain membership without reinstalling Windows NT**.

2.5 Users

2.5.1 Configuring and Controlling Access to User Manager

There are three tiers of user administration within Windows NT: user accounts, local groups, and global groups. The User Manager program is the primary tool used to create, modify, and delete user accounts and manage group security for domains and computers in Windows NT. A domain is a collection of computers that share a common accounts database and security policy. Each domain has a unique name.

★ Access to the User Manager utility in both stand-alone and domain environments must be restricted to authorized system staff.

2.5.2 User Accounts

A user account must be established for each person requiring access to Windows NT. All of the information that defines a specific user to the operating system is contained within the user's account.

★ The following must be used when creating and managing user accounts:

- **The system administrator must establish an account for every individual requiring access to NT workstations or server resources**. Users must not share accounts. Accounts used for services or proxies must be unique to the service.
- Each user account must be included in only those groups assigned permissions and/or rights to those resources required operationally by the user.
- Do not assign a user account to a new user by changing the user name and other properties of an existing user account.
- **System and domain administrators are required to maintain at least two user accounts. User accounts that are members of the Administrative group must be used only for performing administrative functions**. Normal processing must be done with a non-privileged account.

2.6 User Account Policy

User accounts operate within the parameters of the established individual account and *user rights* policies established for a domain or workstation in the User Manager program. The *account policy* applies to all users on the particular domain or workstation, and determines the password length, age, uniqueness, and whether users must log on to change their password. It also controls the number of invalid log on attempts to accept before locking the user account and whether remote users will be forcibly disconnected from the server when log on hours expire.

★ The settings listed in **Figure 2.6-1** must be established within the Account policy:

Maximum Password Age	Set to Expire in 90 days
Minimum Password Age	This is an optional field, as a knowledgeable user can cycle through whatever number is set for password uniqueness, and end up keeping their original password.
Minimum Password Length	Must be 6-8 characters in length. Under no circumstances are blank passwords permitted.
Password Uniqueness	The default value of five provides a sufficient rotation period.
Account Lockout	Must be selected. The following are the minimum required settings. System administrators may implement a more restrictive lockout policy if required by their operational environment. ■ Lockout after 3 bad log on attempts ■ Reset count after 30 minutes ■ Lockout duration set to Forever (until admin unlocks)
💣 Forcibly Disconnect Remote Users When Logon Hours Expire	✿ NT Server Only. Use this box judiciously. While it may be desirable, forcibly logging off a user may cause a loss of data.
Users Must Log On to Change Password	Leave unchecked. When unchecked, allows users to change their expired passwords without notifying an administrator. (Note: This is optional. Password changing may be handled manually by the system administrator.)

Figure 2.6-1

2.6.1 Assigning User Rights

User rights refer to the ability to perform certain functions on the system. Unlike assigning a user permission to an object, rights apply to the system or domain as a whole. User rights should be assigned to groups, not individuals. **User rights assigned on the domain controller affect every domain controller in the domain. User rights assigned on a non-domain controller server or a workstation affect that machine only**. The user rights policy is changed in User Manager for Domains (Policies, User Rights, click Show Advanced User Rights checkbox). Server Manager, an administrative utility, can be used to force the PDC to replicate its database/sync its database with that of any or all BDCs in the same domain.

★ NT includes several advanced user rights that are used by the system and should not be assigned to any user or group. The system administrator must ensure the recommended changes listed in **Figure 2.6.1-1** are made, and that no users (non-administrators) are assigned user rights marked with ☒.

Legend: Italicized groups appear in the user rights of NT Workstations and non-domain controller servers only.
Bold groups appear in the user rights of domain controllers only.
"⇨" Indicates an advanced right.
Rows containing changes to be made to the default settings are shaded.

User Right	Allows	Initially Assigned To	Recommended Change
Access this computer from the network.	A user to connect to the computer over the network.	Administrators, Everyone, *Power Users*	Revoke this right from Everyone and Power Users. Add only groups that need to access this computer from the network. Revoke this right from Administrators to force Administrators to log on locally. (optional).
⇨☒Act as part of the operating system.	A process to perform as a secure, trusted part of the operating system. Within the operating system some sub-systems are granted this right.	(None)	No change
☒Add workstations to the domain.	A user to add workstations to a particular domain. This right is meaningful only on domain controllers.	(None)	No change
☒Back up files and directories	A user to back up files and directories. This right supersedes file and directory permissions, including "No Access".	Administrators, Backup Operators, **Server Operators**	No change
⇨Bypass traverse checking.	A user to change directories and to access files and directories, even if the user does not have access to the parent directories.	Everyone	No change
Change the system time.	A user to set the time for the internal clock of the computer.	Administrators, *Power Users,* **Server Operators**	No change
⇨☒Create a pagefile.	A user to crate new pagefiles for virtual memory swapping.	Administrators	No change

Legend: Italicized groups appear in the user rights of NT Workstations and non-domain controller servers only.
Bold groups appear in the user rights of domain controllers only.
"⇨" Indicates an advanced right.
Rows containing changes to be made to the default settings are shaded.

User Right	Allows	Initially Assigned To	Recommended Change
⇨☒Create a token object.	A process to create access tokens. Only the Local Security Authority should be allowed to do this.	(None)	No change
⇨☒Create permanent shared objects.	A user to create special permanent objects such as //Device.	(None)	No change
⇨☒Debug programs.	A user to debug various low-level objects such as threads. This right is not auditable and therefore must not be assigned to any user, including the system administrator. In a production environment, there is no apparent operational requirement for users to debug programs.	Administrators	Revoke this right from Administrator on domain controller and non-domain controller servers.
☒Force shutdown from a remote system.	A user to shut down a Windows NT system remotely over a network.	Administrators, **Server Operators**	No change
⇨☒Generate security audits.	Allows a process to generate security audit log entries.	(None)	No change
⇨☒Increase quotas.	This right has no effect in current versions of Windows NT.	Administrators	No change
⇨☒Increase scheduling priority.	A user to boost the execution priority of a process.	Administrators, *Power Users*	No change
☒Load and unload device drivers.	A user to install and remove device drivers.	Administrators	No change
⇨☒Lock pages in memory.	A user to lock pages in memory so they cannot be paged out to a backing store such as PAGEFILE.SYS.	(None)	No change
⇨☒Log on as a batch job.	Nothing. This right has no effect in current versions of Windows NT.	(None)	No change

Legend: Italicized groups appear in the user rights of NT Workstations and non-domain controller servers only.
Bold groups appear in the user rights of domain controllers only.
"⇨" Indicates an advanced right.
Rows containing changes to be made to the default settings are shaded.

User Right	Allows	Initially Assigned To	Recommended Change
⇨☒Log on as a service.	A process to register with the system as a service. This user right should only be assigned to accounts specifically created to run a Windows NT service.	(None)	No change
Log on locally.	A user to log on directly at the computer.	**Account Operators,** Administrators, Backup Operators, **Print Operators, Server Operators,** *Users*	On domain controller and non-domain controller servers, revoke this right from everyone *except* Administrators and Operators.
☒Manage auditing and security log.	A user to specify what types of resource access (such as file access) are to be audited and clear the security log.	Administrators	No change
⇨☒Modify firmware environment variables.	A user to modify system-environment variables stored in non-volatile RAM on systems that support this configuration.	Administrators	No change
⇨☒Profile single process.	A user to perform profiling (performance sampling) on the system.	Administrators,	No change
⇨☒Profile system performance.	A user to perform performance sampling on the system.	Administrators	No change
⇨☒Replace a process-level token.	A user to modify a process's security-access token. This is a powerful right, used only by the system.	(None)	No change
☒Restore files and directories.	A user to restore backed-up files and directories. This right supersedes file and directory permissions, including "No Access".	Administrators, Backup Operators, **Server Operators**	No change

Legend:	Italicized groups appear in the user rights of NT Workstations and non-domain controller servers only. Bold groups appear in the user rights of domain controllers only. **“⇨”** Indicates an advanced right. Rows containing changes to be made to the default settings are shaded.		
User Right	**Allows**	**Initially Assigned To**	**Recommende d Change**
Shut down the system.	Shut down Windows NT.	Administrators,	On domain controllers and non-domain controller servers, revoke this right from everyone except Administrators.
⇨☒Take ownership of files or other objects.	A user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions on objects including “No Access”.	Administrators	No change

Figure 2.6.1-1

2.6.2 Configuring User Account Settings

2.6.2.1 Creating User Templates

Recommendation: The configurations included in **Figure 2.6.2.1-1** are provided for establishing user account settings.

Administrator User Properties	**Parameters**
User Name	Must be configured in accordance with the *NASA Standard Naming Conventions.* The required format is **[FIRST INITIAL][LAST NAME]**, with an eight character maximum**.** (Example: ASmith).
Full Name	Follow naming conventions.
Description	Should include the individual's job title, e.g., ADM clerk or Secretary
User Must Change Password at Next Logon	Should be selected unless the system administrator chooses to handle password changes manually.
Users Cannot Change Password	Should not be selected.
Passwords Never Expire	Policy requires that users' passwords change every 90 days. Using this feature, the system administrator can force a user's password to expire at the end of twelve months automatically. Alternatively, the administrator may elect to handle this process manually.
Account Disabled	Do not select for normal users. Could be used to temporarily turn off an account, or for TDY accounts.
Groups	The system administrator or systems security officer must create an NT group plan, logically dividing all users into functional areas. Users must be assigned only to those groups that they need for access to resources required to perform their job duties.
Profile	See Section 2.8.2, Implementing System Policies. Login Scripts: In the \winnt\system32\repl\import\scripts directory. Should be stored on an NTFS partition. NT permissions to login scripts must be restricted to execute for users (this is the default). Login scripts may be configured to connect users to those resources required to perform their assigned duties. Additionally, the login script may be used to synchronize the workstation's clock with the primary domain controller. This is achieved by adding a "net time" statement to the beginning of login scripts as follows: `net time "\\name of the primary server" /set /yes` Home Directory: The default home directory \USERS\DEFAULT is located on the local drive of an NT workstation. To ensure that all data files are being backed up, system administrators may change the default home directory to a sub-directory of a shared network directory on a server. All home directories must reside on an NTFS drive.
Hours	By default, users are permitted to access NT at any time. The system administrator must establish reasonable hours of operation for the system and ensure that access to the network outside of normal business hours is monitored. This option can be modified for individuals requiring access after normal business hours on an as-needed basis.

Logon To	The system administrator may use this option to specify the workstations from which a user can log on to using this domain account.
Account	Account Expires: The system administrator may choose to create an account with an expiration date (for example, a TDY user account). Normal accounts should never expire (this is the default). Account Type: All accounts should be global (this is the default).

Figure 2.6.2.1-1

2.6.2.2 Built-in User Accounts

2.6.2.2.1 Guest Account

Upon installation, the guest account has a blank password. On NT Servers the default for the guest account is disabled. However, on NT Workstations the default is enabled. Its profile cannot be changed from the default user profile and the account cannot be deleted.

★ **The guest account must be disabled** to deny anonymous access to network resources. All user accounts must specifically identify an authorized user.

2.6.2.2.2 Administrator Account

The Administrator Account has complete access and control over the entire system. At installation time, the account is created automatically with a password selected by the installer.

★ Following installation, the system administrator must rename and assign a 6-8 character password to the Administrator Account. Note: The name cannot contain the following characters: “”/ \ [ ] : ; | = , + * ? < >

★ The Administrator Account must be used only by the system administrator or delegated alternates for administrative functions. The system administrator must create a second (personal) account for non-administrative functions.

👍 **Recommendation**: **It is strongly recommended that the password for this account be stored in writing and secured in accordance with policy. If only one user account has administrative privileges and the password is lost, the account can only be restored by reinstalling NT or using the Emergency Repair Disk (ERD), if it is up to date**.

2.7 Groups

2.7.1 Assigning Users to Groups

A *group* is a collection of Windows NT user accounts, created in User Manager. The system administrator should not simply accept the default groups installed by Windows NT. Divide the Windows NT LAN into logical groups of users by virtue of their functional needs.

To protect resources on an NT system or domain, objects such as files, directories, and printers have *Access Control Lists (ACL).* The ACL for any object contains a list of *Permissions* which apply to individual users, and/or groups of users. **ACLs should never contain individual user accounts. Groups should be used to manage security**.

👍 **Recommendation**: Use the following rule of thumb to manage security using groups:

- Devise a Windows NT group architecture based on functional/operational needs.
- Create the user accounts and add them to these functional/operation groups.
- Apply NTFS permissions against functional/operational groups by adding only groups to the ACLs for objects (e.g., files and printers).

Creating a group architecture may be as general as stating that all staff in the Headquarters Accounting Division are members of a group called ACCOUNT. Alternatively, it may be broken down to the degree that Cost and Commercial Accounts Branch members are in a special group called ACCTCOST, and Personal Services Branch members are in the ACCTPERS group. Users may be members of more than one group, as needed. For example, a user can be a member of both the ACCTCOST and ACCTPERS groups, each granting access to a particular set of resources.

★ The system administrator must follow the principle of least privilege when assigning users to groups. Membership in a group must be determined by the user's need to access the collective resource permissions and system rights of the group. All groups must be created by the system administrator, and possess only those privileges required by the group to perform assigned duties.

2.7.2 Built-in Groups

NT provides several default built-in local and global groups. By default, these groups have been granted specific access rights and privileges. The default access rights can be modified, whereas the built-in privileges cannot. Therefore, caution is urged when adding users to the built-in groups. For each built-in group, the system administrator must modify the group's access rights as noted, and implement the following configurations.

2.7.2.1 Built-in Local Groups

★ The configurations listed in **Figure 2.7.2.1-1** must be followed with respect to built-in local groups.

Administrators	Membership in this group results in the user account gaining superuser attributes. This group must include only the designated security officer, System Administrator, and authorized system staff. General users must never be assigned to the Administrators group. The username "Administrator" must not be listed as a member of this group (this vulnerability is removed by implementing the recommendations contained in the section on built-in user accounts).
Backup Operators	This group must include only those system staff assigned backup duties, if they are not already members of the Administrators group. No excess user access rights have been assigned to this group. However, it is important to note that any user assigned access to this group will be able to backup all files on the system regardless of the permissions established on the files.
Everyone	This group encompasses all local workstation and domain users, and all users from other domains. **Note:** By default, many NTFS permissions on objects allow the Everyone group *Change* access (Read, Write, Execute, and Delete) or *Full Control* access (Change access with Take Ownership and Change Permissions access added). This is completely opposite to the principle of least privilege. Changing this default must be addressed aggressively by the system administrator. (See Assigning User Rights and Assigning File, Directory, and Registry Permissions sections.)
Guests	Username "Guest" must be disabled. Anyone authorized to sign-on to a computer resource must be fully identifiable through user account credentials.
Users	This group should provide a template for locally devised common functional/operational user groups.

Figure 2.7.2.1-1

In addition to the above listed groups, Windows NT Server contains the built-in local groups as listed in **Figure 2.7.2.1-2.**

Replicator	If directory replication is configured, this group should contain the directory replicator service account.
Account Operators	This group should not be used. Its features are reserved for system administrators and all necessary privileges already are contained in the Administrators group.
Print Operators	Includes only those individuals authorized to maintain print queues and printers. Assign judiciously for section level print operators.
Server Operators	This group should not be used. Its features are reserved for system administrators and all necessary privileges already are contained in the Administrators group.

Figure 2.7.2.1-2

2.7.3 Global Groups

Global groups are defined in Windows NT Domains, i.e., at least one Windows NT Server configured as a Primary Domain Controller exists within the network. Global groups enable group lists to propagate across multiple NT computers (servers and workstations) in a domain, as well as any trusting domains. This enables the system administrator to assign permissions to groups that are not local to his/her domain or workstation without incurring the overhead of locally managing the membership of those groups.

👍 **Recommendation**: The rule of thumb for using global groups is:

- Add users to global groups on the domain.
- Add the global groups to local groups.
- System administrators in other domains or users on peer NT workstations apply permissions locally against these local groups.

2.7.3.1 Built-in Global Groups

There are two built-in global groups in Windows NT: Domain Admins and Domain Users.

★ Membership in the Domain Admins group must be limited to administrators.

👍 **Recommendation:** Domain Users should be considered a template for creating global groups comparable to the Users local group.

2.7.4 Special Groups

Windows NT contains five groups that are created by the system for special purposes, being Network, Interactive, Everyone, Creator Owner, and System. Membership to these groups cannot be assigned by the system administrator. Instead, users are either members by default or become members of one of these groups based on their network activity. System administrators will note the appearance of these groups when establishing the permissions on files, directories, and printers. For specific modification of default permissions assigned to these groups and general guidance on modifying these groups permissions see Section 2.12, Assigning File, Directory, and Registry Permissions.

2.8 System Policy

Policy requires that access to the operating system and application software be limited. Only authorized users can have special privileges to access the operating system, access application software, modify security parameters, and perform sensitive system functions such as backups. Access to the operating system and application software by general users must be controlled to provide the least amount of privileges. Along with granting access privileges, user profiles must be established and structured to limit access. Windows NT 4.0 System Policy Editor and System Policies allow Administrators to create system profiles to control user's Windows NT workstation environment. Establishing system policies enables the Administrator to:

- Implement and manage a consistent computing environment from a central location.
- Secure workstations from unauthorized software and hardware changes.
- Minimize the threat of computers being used for internal intrusion.

Defined policies affect desktop settings, log on access, network access, and printer access for both users and computers. **Using the System Policy Editor, an administrator can create a default user and computer configuration that will be automatically downloaded at each log on**. Similarly, policies for groups can be created and applied. Built-in flexibility allows the administrator to create a custom profile for an individual and computer suitable to the business needs.

2.8.1 System Policy Configurations

Recommendation: The following are recommended configurations for implementing system policies.

- Apply “Access this Computer from the Network” right to the appropriate domain group that includes all users without administrative privileges.
- ✿ Use System Policies instead of User Profiles.
    - System policies are applied in the following order:
        1. User
        2. Group
        3. Default User
        4. Computer
        5. Default Computer
- Once implemented, all users and computers that access a domain controller from the network will be affected by the system policy. **Establishing system policies at the time of workstation installation will provide best results.**
- Installation of Service Pack 2 (at least) on the domain controller is required.
- The Default Computer and Default User should be the most restrictive. Add Groups, Users, and Computer to provide the appropriate level of restrictions.
- Policies set using the System Policy Editor affect the following registry keys:
    - HKEY_LOCAL_MACHINE
    - HKEY_CURRENT_USER
- Rank groups in priority. In the event of a policy conflict, the policy of the group with the highest ranking takes precedence.
- Policies are taken from a user’s logon domain.
- To ensure proper application of policy changes, users must log out, and in some cases, restart the computer.
- **System policies are not effective for systems running Windows 95, because booting from a floppy or running in Safe Mode will circumvent them**.
- System policies have no affect on Windows 3.x users and MS-DOS users.

2.8.2 Implementing System Policies

Two conditions must exist for system policies to be properly implemented. **Users must have roaming profiles and must belong to a group, preferably the group Domain Users, that has the right “Access this Computer from the Network” applied at the domain controller**. Users, not Administrators, should have roaming profiles setup. Having roaming profiles allows the system administrator to delete the local user profile after the user has logged off the system. Should the server not be available, a default profile stored on the workstation will be used.

Being a member of a group that has the "Access this Computer from the Network" right initiates the application of system policies to a user and computer. By excluding Administrator accounts from the group, system policies will not be applied allowing administrators full access to the system. As a precaution, however, administrators should only be able to log on at the server.

Roaming profiles can easily be created using User Manager for Domains as listed below:

1. Open the User Manager for Domains and open the user account.
2. Select the **Profile** button.
3. Within the **Profile** dialog box, add the user profile path using the following convention: \\domain server name\share name\profile name. For example, if the PDC is located on a server called *HQPDC1*, the share name is *Profiles*, and the profile name is *RSmith*, the path would be \\HQPDC1\PROFILES\RSMITH. **Note:** Windows NT creates a directory <winnt root>\profiles where the default user's profile is stored. Share this directory. Check "Replace Permissions on Existing Files". Set the security permission as follows:
    - Administrators – Full
    - Creator Owner – Full
    - Remove the group Everyone.
    - Add the group Domain Users or the name of the group that contains all users. Change the permission to be Change.
    - Server Operators – Change
    - System – Full
4. Click OK twice to save the new settings. The new profile directory will automatically be created the first time the user logs on.

2.8.2.2 User Rights

Recommendation: All users without administrative privileges should be included in the group Domain Users. The group Domain Users should have the user right "Access this Computer from the Network" applied using the User Manager for Domains. This right should only be applied to non-administrator groups and users. (See Section 2.6.2, Assigning User Rights). The Group Administrators and Domain Administrators should have the user right "Logon Locally" applied If an administrator logs on to a server and system policies appear to have been applied, check that the administrator account does not belong to a group having the right "Access this Computer from the Network" applied. Note: In order to remove Administrator from the Domain User Group, another global group must be set as the Administrator's primary group, such as Domain Admins, in the User Manager for Domains.

2.8.3 Creating System Policies

The following steps will assist the system administrator in the setup of two different system policies that can be the model for creating subsequent policies for specific needs. The first policy is the most restrictive and is the default setting for default computers. The second policy is for default users and domain users and provides the minimum recommended level of restriction.

As shown in the next table, three different settings are used to select System Policies.

- Gray Shade: The registry key will not be modified.
- Checked box: The policy will be implemented and the settings added to the registry.
- Cleared/blank box: The policy will not be implemented - the setting is disabled.

The selected and cleared policy settings are saved to the policy file.

Figure 2.8.3-1 displays the above settings which are used to select system policies.

Key	Description	Default Computer Settings
Network	Affects whether policies are updated automatically or manually.	
SYSTEM POLICIES UPDATE		
Remote Update		Leave Gray
System	Sets Simple Network Mail Protocol (SNMP) settings and allows startup programs to be specified	
SNMP		
Communities		Leave Gray
Permitted Managers		Leave Gray
Traps for Public community		Leave Gray
RUN		
Run	Add programs that are to be launched at startup, such as e-mail.	Leave Gray
Windows NT Network	Enables the creation of hidden shares for each drive letter upon system startup.	
SHARING	Creates hidden system shares C$ and Admin$	
Create hidden drive shares (workstation)		Check
Create hidden drive shares (server)		Check
Windows NT Printer	Disable print spooler browse process.	
Disable browse thread on the computer		Check
Scheduler Priority		Gray
Beep on error enabled		Gray
Windows NT Remote Access	Settings for Remote Access. Apply only if RAS will be installed.	
Max Number of Unsuccessful Authentication Retires		Gray
Max Time Limit of Authentication		Gray
Wait Interval for Callback		Gray
Auto Disconnect		Gray
Windows NT Shell	Specifies location of shared folders. This can be customize if more standardization is required	
All custom shared folders		Gray
Windows NT System	Can modify logon and file system options.	
LOGON	Controls aspects of user's log on appearance	

Key	Description	Default Computer Settings
Log on Banner	Type in caption "Warning: For Official Use Only". The full text must be added to each workstation editing the registry. See Configuring NT Workstation to Display Legal Notice below.	Check
Enable shut down from authorized dialog box.		Check
Do not display logged on user name	The name of the previous user logged onto the workstation or server will not appear.	Check
Run log on script synchronously	User's shell starts after log on script completes. If value is also set in the user section, this value takes precedence.	Check
FILE SYSTEM	Controls File Naming Convention	
Do not create 8.3 file names for long file names	This is required for certain programs at Headquarters.	Gray
Allow extended characters in 8.3 file names	This is required for certain programs at Headquarters.	Gray
Do not update last access time		Gray
Windows NT User Profiles	Defines a slow connection to a logon server.	
Delete cached copies of roaming profiles		Check
Automatically detect slow network connection		Gray
Slow network connection time-out		Gray
Time-out for dialog box		Gray

Figure 2.8.3-1. *Policy Settings for Default Computer Settings*

These settings can be made by following these steps:

1. Create and manage system policies using the System Policy Editor. From the Domain server, log on with Administrator privileges. From START, select Programs, Administrative Tools (Common), System Policy Editor.
2. Open a new policy by choosing File from the Menu bar, then New Policy. Two entries will appear: Default Computer and Default User.
3. Double click on Default Computer to open the Default Computer Properties dialog box. Add the settings listed in column Default Computer settings in Figure 2.8.3-1.
4. Once settings have been made, click OK for settings to be implemented.

Next, the settings for the Default User and Domain Users will be established as listed in the following table. **(Figure 2.8.3-2)**

1. Double click on Default User to open the properties dialog box. Add the settings listed in column Default User.
2. Select the Add Group button from the tool bar, and add the Domain Users groups. Double click on the Domain Users icon to open the properties dialog box. Add the settings listed in column Domain Users.
3. Once settings have been made, click on OK to close.
4. Additional settings can be used to establish shared custom folders, such as program folders and startup folders, in addition to shared custom desktop icons and shared custom start menus. Add those groups that will use these features and point to the custom items within the Windows NT Shell, Custom Folders section.
5. If necessary, add other groups that will need different system policies and modify the system policies as needed.
6. Review the group priorities located under the Options choice on the menu bar. Rank the groups in order of priority using the rule that in the event of a policy conflict, the higher ranked groups take precedence.
7. When finished, save the policy. Select File from the menu bar then Save. Change to the directory <winnt root>system32\repl\import\scripts, and name the file NTCONFIG.POL. System policies will then take effect the first time a user logs on to the system.
8. Use Server Manager to configure Directory Replication. Replicate the Scripts folder, which contains the NTCONFIG.POL file, from the PDC to all BDCs. Refer to the on-line Windows NT Concepts and Planning guide for more information on configuring Directory Replication.

Key	Description	Settings For Default User	Settings for Domain Users
Default User			
CONTROL PANEL	Controls the display settings		
Display			
Restrict Display		Gray	Gray
DESKTOP			
Wallpaper		Gray	Gray
Color Scheme		Gray	Gray
Shell			
RESTRICTIONS	Restrict START items, contents of My Computer, and Network Neighborhood.	Gray	Gray
Remove Run Command from Start Menu		Gray	Gray
Remove Folders from Setting on Start Menu	No access to Control Panel and Printers	Check	Check
Remove Taskbar from Settings on Start Menu	User cannot access properties of the Taskbar	Check	Check
Remove Find command from Start Menu		Check	Check
Hide drives in My Computer		Check	Gray
Hide Network Neighborhood		Check	Check
No Entire Network In Network Neighborhood		Check	Check
No Workgroup Contents in Network Neighborhood		Gray	Gray
Hide all items on desktop		Check	Gray
Disable Shut Down Command		Gray	Gray

Key	Description	Settings For Default User	Settings for Domain Users
Don’t Save Setting at Exit		Check	Check
System			
RESTRICTIONS			
Disable Registry Editing Tools		Check	Check
💣 Run only Allowed Windows Applications	Limits programs Users can run to those listed. **ANY PROGRAM NOT LISTED CANNOT BE RUN BY THE USER. If not used, see instructions below for suggested programs to remove from Workstations.**	Check (Click show and add the full program name. Note, program must have previously been installed)	Check (Add the full program name. Note, program must have previously been installed)
Windows NT Shell			
CUSTOM FOLDERS (all six entries)		Gray	Gray
RESTRICTIONS			
Use only approved shell extensions		Check	Check
Remove File menu from Explorer		Check	Gray
Remove common program groups from Start menu		Check	Gray
Disable Context Menus for the Taskbar	Primarily used to disable the task manager and taskbar properties.	Check	Check
Display Explorer’s default Context menu		Gray	Gray
Remove the “Map Network Drive” and “Disconnect Network Drives” Option	Prevents users changing established network drive mappings **Note: A log on script must be used to provide drive mappings, if this option is used.**	Check	Check

Key	Description	Settings For Default User	Settings for Domain Users
Disable link file tracking		Gray	Gray
Windows NT System			
Parse autoexec.bat		Check	Gray
Run log on scripts synchronously		Check	Check
Disable Task Manager	Primarily used to prevent users from stopping processes	Check	Gray
Show Welcome Tips at Log on		Blank	Blank

Figure 2.8.3-2. *Settings for Default User and Domain Users*

2.8.3.1 System Policy Troubleshooting

System policies applied to existing Windows NT Workstations may not be properly applied. In some cases, registry settings may have been previously set. Therefore, if a System Policy option had been left gray, meaning that no change will occur, the intended effect may not occur. To correct the situation and have the intended policy applied, change the setting using the System Policy Editor to a “check” or “blank”. The next time the user logs on, the correct policy will be applied.

Alternatively, an Administrator can change the registry setting of the individual workstation using the System Policy Editor which includes a feature to remotely edit the registry. To change the Default User and Default Computer settings on a remote workstation do the following:

1. Start the System Policy Editor.
2. From the menu bar select File, then the Connect option. Enter the remote name of the Workstation in the dialog box.
3. A Default Computer icon and Default User icon for the workstation will appear. These represent the current System Policies applied to the remote workstation.
4. Make the appropriate changes to the remote workstation.
5. Save the settings by selecting File from the menu bar, then the Disconnect option. Answer yes to save settings.
6. Have the user log on to verify the correct system policies are being applied.

2.8.4 Configuring NT Server to Display Legal Notice

★ The legal notice in the box below must be displayed on all automated information systems. Users must be presented with this notice prior to receiving access to any system resources.

> U.S. GOVERNMENT COMPUTER
> If not authorized to access this system, disconnect now.
>
> YOU SHOULD HAVE NO EXPECTATION OF PRIVACY
> By continuing, you consent to your keystrokes and data content being monitored.

Perform the following procedure to display this notice during the Windows NT log on process:

1. As the notice will have to be manually installed on each computer, copying it from a text file will be much quicker and more accurate than typing it each time. Prepare the text as it appears in the box above using Notepad.exe and save as a text file.
2. Log on as a member of the Administrators Group.

3. Select the Start button, then Programs, then Accessories, and then Notepad.
4. Open the text file containing the notice.
5. Select the Start button then choose Run from the menu.
6. Type in 💣 **REGEDT32** into the Command Line text box and click on OK. The Registry Editor program will start.
7. Within the Registry Editor, choose the HKEY_LOCAL_MACHINE window and expand the directory structure to HKEY_LOCAL_MACHINE\SOFTWARE\ MICROSOFT\WINDOWS NT\CURRENT VERSION\WINLOGON
8. Double click on the **LegalNoticeCaption**. The String Editor dialog box appears.
9. In the string text box type the following text: **WARNING: For Official Use Only.**
10. Click on OK to close.
11. Switch to NOTEPAD. From the menu bar select Edit and Select All. All text will be highlighted. Next, select Edit and Copy. 💣 Switch back to Registry Editor.
12. Next, double click on **LegalNoticeText**. The String Editor dialog box appears.
13. In the string text box, copy the notice by pressing CTRL-V, then choose OK.
14. Exit Registry Editor, shut down and restart the computer for the changes to take effect.
15. The above message should appear after holding down the CTRL-ALT-DEL keys.
16. Update the Emergency Repair Disk (ERD) and return it to secure storage.

2.9 Windows NT Auditing

2.9.1 Configuring Audit Events

For Windows NT computers, auditable events include those related to System, Application, or Security-generated error or informational messages. By default, Windows NT audits few security-related events. All such events can be examined using the Event Viewer program. The following guidance is provided for establishing audit parameters for NT Servers.

★ Changes to directory and file object security can only be audited on NTFS partitions. Be sure to use NTFS (not FAT) for all data partitions.

★ System and object level auditing must be activated in User Manager for all domain controllers and servers within a domain. Under no circumstances should *Do Not Audit* be selected in the Audit Policy of a domain controller or server.

To activate auditing, the following steps must be performed:

1. Select the Start button, Programs, Administrative Tools (Common), and User Manager.
2. Under the Policies Menu, choose Audit.
3. On all domain controllers and servers, default audit events must be modified as listed in **Figure 2.9.1-1**.

Event	**Audit Option**
Logon and Logoff	Failure Note: Logon and Logoff Success may be added as needed for system auditing.
File and Object Access	Failure
Use of User Rights	Failure
User and Group Management	Success and failure
Security Policy Changes	Success and failure
Restart, Shutdown, and System	Success and failure
Process Tracking	Failure

Figure 2.9.1-1

★ Access to Manage Auditing and Security Logs must be limited to the system administrator and security officer. All security logs must reside on an NTFS drive.

★ C2 configuration requires that if events cannot be written to the security log, the system should be halted immediately. If the system halts as a result of a full log, an administrator needs to restart the system and clear the log. Save the data to disk before clearing the security log.

2.9.2 File Auditing

★ Within File Auditing, all Windows NT operating system files must be audited for failed attempts. The following steps must be performed to enable auditing of NT operating system files:

1. Open Windows NT Explorer.
2. Highlight the WINNT directory.
3. From the File Menu, choose Properties.
4. From within Properties, choose Security.
5. From within Security, choose Auditing.
6. Click the Add button and choose the Everyone group name.
7. Mark both Replace Auditing on Subdirectories and Replace Auditing on Existing Files check boxes.
8. Mark the Failure check box for all Audit Events.

2.9.3 Registry Key Auditing

★ Within Registry Key Auditing, all registry keys and sub-keys must be audited for failed attempts. The following steps must be performed to enable auditing of registry keys and sub-keys:

1. 💣 Run REGEDT32.EXE. by selecting the Start button, and Run.
2. From the Security Menu, Select Auditing.
3. Click the Add button, and select the group Everyone.
4. Select the Audit Permission on Existing Subkeys check box.
5. Mark the Failure check box for all Audit Events.

Note: Perform above listed steps for HKEY_USERS on local machine and KHEY_LOCAL_MACHINE on local machine. Auditing these two top-level keys will turn on auditing for the remaining keys.

When attempting to audit HKEY_LOCAL_MACHINE an error message will be displayed. This message is normal – click OK and proceed.

2.9.4 Print Auditing

Print auditing, as supported by the Print Manager program, may be useful for certain classes of users.

👍 **Recommendation:** Enable print auditing depending on requirements and security accountability needed for some application specific print tasks. Auditing of printer activity is enabled in the Printer Manager program, and should address print event logging by group.

The following steps must be performed for printer auditing to be enabled:

1. From the Control Panel, select Printers.
2. From the File menu, select Properties.
3. From within Properties, select the Security area.
4. From within Security, select Auditing.
5. Click the Add button and choose the Everyone group name.
6. Select the Failure check box for all Audit Events.

2.9.5 RAS Auditing

Remote Access Service (RAS) can be enabled to generate records in the audit logs that indicate a number of activities, including normal connections, successful disconnection, successful callbacks, disconnects due to idle lines, timed-out authentication, and line errors. Excessive failed connections may indicate that someone is trying to break into an account.

★ If dial-up networking/remote access service (RAS) is installed, all events must be audited. RAS auditing is enabled by default. Do the following to verify that RAS auditing is enabled:

1. 💣 Run REGEDT32.EXE.
2. Look for and highlight the following registry path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\EnableAudit.
3. EnableAudit should be set to 1.

If EnableAudit does not exist:

1. Highlight KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters
2. Choose Add Value from the Edit menu.
3. Add EnableAudit, changing the Data Type to REG_DWORD. Click the OK button.
4. Under the Data Box, type the number 1 to enable auditing. Click the OK button.

★ Within Event Log Settings, all audit logs must be set to ***Do Not Overwrite Events***. Periodically, audit logs should be printed, archived to media, and cleared. To prevent system problems, it is recommended that the system administrator perform this function on a weekly basis. Audit logs must be maintained for a period of six months.

★ The system administrator must perform the following procedures to determine the correct amount of disk space to allocate for the audit file on all domain controllers and servers.

1. In Event Viewer, increase the maximum log size (Log, Log Settings) from 512 kb to 20480 kb or 20 MB.
2. Monitor the actual size of each log for a period of one week. The three audit event logs are: Security (SecEvent.Evt); Application (AppEvent.Evt); and System (SysEvent.Evt). They are located in directory: \WINNT\SYSTEM32\CONFIG\;
3. At the end of one week, write down the size of the log file.
4. Add 50% to this number and enter this as the maximum log file size within Event Log Settings. (Note: While this may be an excessive amount of disk space to allocate to system auditing, if Windows NT is configured to halt when the audit log is full, only system administrators can log on until the security log is cleared. Windows NT is not set to halt by default. If desired, the

system administrator can configure Windows NT to halt by using the 💣 Registry Editor to create or assign the following registry key value:

💣 When the system halts, unsaved data will be lost.

a) Run REGEDT32.EXE.
b) Highlight HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
c) Choose Edit, Add Value.
d) Value Name = CrashOnAuditFail
e) Data Type = REG_DWORD
f) Click OK.
g) Enter 1 for Data.
h) Click OK.

If Windows NT halts as a result of a full security log, the system must be restarted and reconfigured to prevent auditable activities from occurring again while the log is full. After the system is restarted, only administrators can log on until the security log is cleared. For more information on recovering after Windows NT halts, see the "Recovering After Windows NT Halts Because it Cannot Generate an Audit Event Record" in the NT Event Viewer Help.

5. Monitor audit event logs periodically, adjusting the log size as necessary

2.9.6 Understanding the NT Event Log

Generating Windows NT Event Logs is useless unless the system administrator periodically reviews what is recorded in the Audit Logs. The following information will help system administrators understand the contents of the system, security, and application logs.

Figure 2.9.6-1 indicates the five event types that are recorded in the Windows NT Event log.

Symbol	Event Type	Meaning and Example
🛑	Error	Significant problems, such as a loss of data or loss of functions. EXAMPLE: An Error event might be logged if a service was not loaded during Windows NT Workstation startup.
ⓘ	Warning	Events that are not necessarily significant but that indicate possible future problems. EXAMPLE: A Warning event might be logged when disk space is low.
ℹ	Information	Infrequent significant events that describe successful operations of major server services. EXAMPLE: When a database program loads successfully, it might log an Information event.
🔑	Success Audit	Audited security access attempts that were successful. EXAMPLE: A user's successful attempt to log on to the system might be logged as a Success Audit event.
🔒	Failure Audit	Audited security access attempts that failed. EXAMPLE: If a user tried to access a network drive and failed, the attempt might be logged as a Failure Audit event.

Figure 2.9.6-1

The three symbols that are of primary concern are Warning, Error, and Failure Audit. Warning and error messages in the System Log could signal hardware or software problems and alert the system administrator before total failure potentially occurs. Failure audit records failed log on attempts and failed directory and file access.

The Event Log records event ID numbers in all three types of logs. For many events, more information can be viewed than is displayed in Event Viewer by double-clicking the event.

System administrators can sort through the event log by using the NT Event Viewer to:

- Sort events from oldest to newest or from newest to oldest.
- Filter events so that only events with specific characteristics are displayed.
- Search for events based on specific characteristics or event descriptions.
  Filtering has no effect on the actual contents of the log – it changes only the view. All events are logged continuously, whether the filter is active or not.

The following describes the options available in the **Filter** dialog box:

- **Source -** A source for logging events, such as an application, a system component, or a driver.
- **Category** - A classification of events defined by the source. For example, the security event categories are Logon and Logoff, Policy Change, Privilege Use, System Event, Object Access, Detailed Tracking, and Account Management.
- **User** - A specific user that matches an actual user name. This field is not case sensitive.
- **Computer** - A specific computer that matches an actual computer name. This field is not case sensitive.
- **Event ID** - A specific number that corresponds to an actual event.

2.9.6.1 Searching for Events

To search for events that match a specific type, source, or category, click Find on the View menu. Searches can be useful when you are viewing large logs. For example, you can search for all Warning events related to a specific application or search for all Error events from all sources.

Your choices in the Find dialog box are in effect throughout the current session. If Save Settings On Exit on the Event Viewer Options menu is checked when you quit, the current filter settings are available the next time you start Event Viewer.

Auditing of successful and failed attempts can be performed on directories and files as listed in **Figure 2.9.6.1-1**.

Directory Events	**File Events**
Displaying names of files in the directory	Displaying the file’s data
Displaying directory attributes	Displaying file attributes
Changing directory attributes	Displaying the file’s owner and permissions
Creating subdirectories and files	Changing the file
Going to the directory’s subdirectories	Changing file attributes
Displaying the directory’s owner and permissions	Running the file
Deleting the directory	Deleting the file
Changing directory permissions	Changing the file’s permissions
Changing directory ownership	Changing the file’s ownership

Figure 2.9.6.1-1

2.9.7 Archiving Event Logs

When the system administrator archives a log file, the entire log is saved, regardless of any filtering options that may have been specified in the Event Viewer. If the sort order in Event Viewer is changed, event records are saved exactly as displayed if the log is archived in a text or comma-delimited text file. To display an archived log in Event Viewer:

1. On the Log menu, click Open.
2. In the Open dialog box, enter the filename in File Name, and click OK.
3. The Open File Type dialog box appears.
4. Click System, Security, or Application to match the type of log you want to see.

Archived files in the Event Viewer can only be viewed if the log is saved in log file format. Refresh or Clear All Events to update the display or to clear an archived log that does not work.

2.9.8 Audit Log Reporting Utilities

Although Windows NT provides excellent auditing capabilities, the logs generated by Windows NT are cumbersome to review and do not provide meaningful reports. There are third party products available that enable system administrators to easily view and analyze audit logs.

2.9.8.1 Crystal Reports

Crystal Reports 4.5 is shipped with the Microsoft NT 3.51 and 4.0 Resource Kits. Crystal Reports generates reports against current or archived NT event logs.

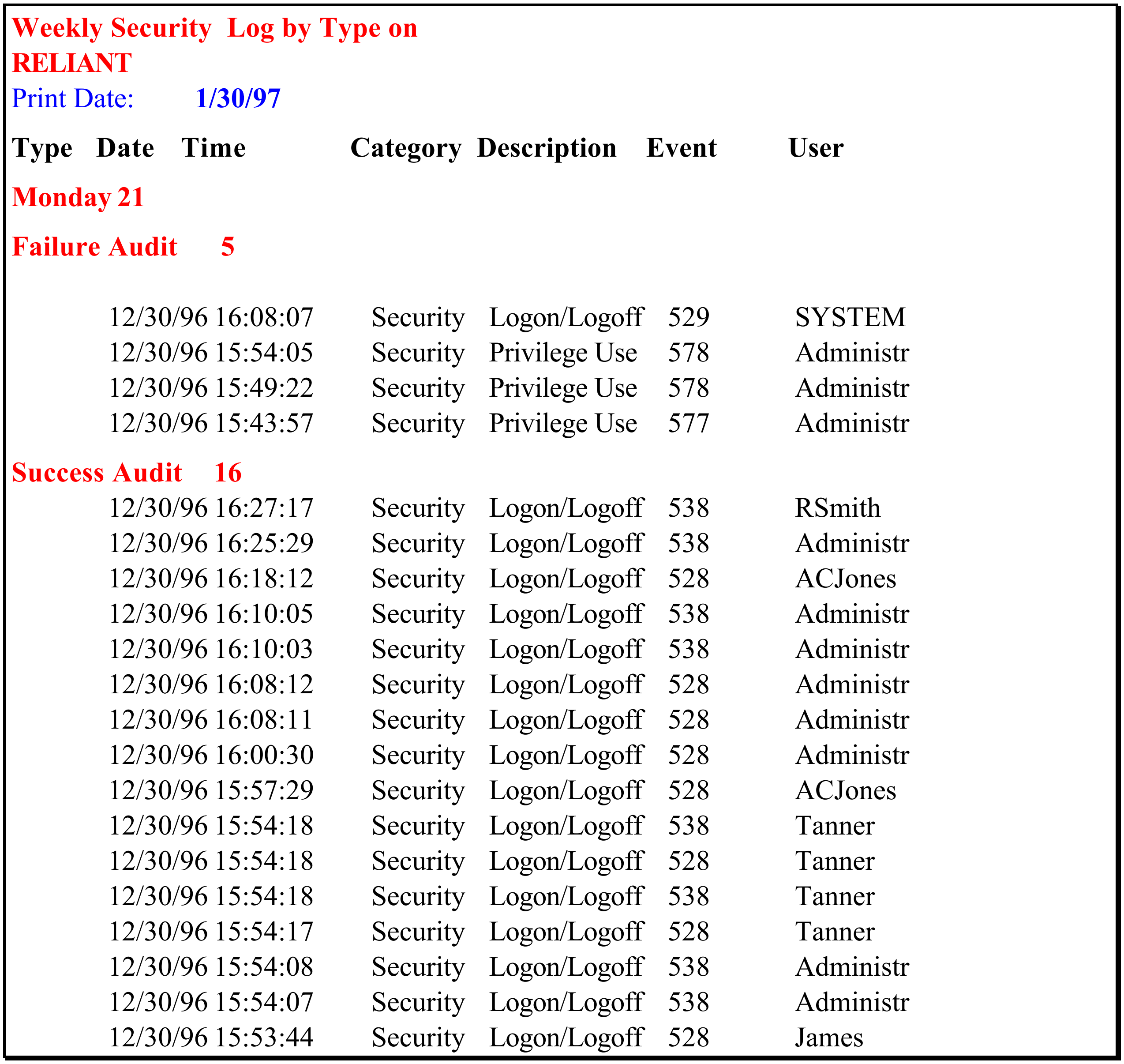
There are ten predefined reports included with Crystal Reports 4.5. These reports are listed in **Figure 2.9.8.1-1**.

Title	File Name	Description
Application Log By Date	APP_DATE.RPT	Lists NT Application Events sorted by date with most recent date first.
Application Log By Source	APP_SRC.RPT	Lists NT Application Events sorted by Source of the event.
Application Log Summary by Type	APP_TYPE.RPT	Summarizes NT Application Events grouped by type.
Security Log by Category	SEC_CAT.RPT	Lists NT Security Events sorted by category.
Security Log by Date	SEC_DATE.RPT	Lists NT Security Events sorted by date with most recent date first.
Security Log Summary by Type	SEC_TYPE.RPT	Summarizes NT Security Events grouped by type.

Title	File Name	Description
System Log by Date	SYS_DATE.RPT	Lists NT System Events sorted by date with most recent date first.
System Log by Source	SYS_SRC.RPT	Lists NT System Events sorted by source
System Log Summary by Type	SYS_TYPE.RPT	Summarize NT System Events grouped by type
Weekly System Log by Type	SYS_WEEK.RPT	Lists NT System Events sorted by day/by type for the last seven days.

Figure 2.9.8.1-1

All of the predefined forms can be modified easily by the system administrator. For example, the *Weekly System Log by Type* can be changed to extract Security or Application events rather than System events. **Figure 2.9.8.1-2** is a sample of the "Weekly Security Log by Type" which shows a list of events recorded in the Security Event log sorted by the type of event which occurred.



Weekly Security Log by Type on RELIANT

Print Date: **1/30/97**

```
Type   Date   Time          Category  Description   Event     User

Monday 21

Failure Audit   5

          12/30/96 16:08:07    Security  Logon/Logoff   529     SYSTEM
          12/30/96 15:54:05    Security  Privilege Use  578     Administr
          12/30/96 15:49:22    Security  Privilege Use  578     Administr
          12/30/96 15:43:57    Security  Privilege Use  577     Administr

Success Audit   16
          12/30/96 16:27:17    Security  Logon/Logoff   538     RSmith
          12/30/96 16:25:29    Security  Logon/Logoff   538     Administr
          12/30/96 16:18:12    Security  Logon/Logoff   528     ACJones
          12/30/96 16:10:05    Security  Logon/Logoff   538     Administr
          12/30/96 16:10:03    Security  Logon/Logoff   538     Administr
          12/30/96 16:08:12    Security  Logon/Logoff   528     Administr
          12/30/96 16:08:11    Security  Logon/Logoff   528     Administr
          12/30/96 16:00:30    Security  Logon/Logoff   528     Administr
          12/30/96 15:57:29    Security  Logon/Logoff   528     ACJones
          12/30/96 15:54:18    Security  Logon/Logoff   538     Tanner
          12/30/96 15:54:18    Security  Logon/Logoff   528     Tanner
          12/30/96 15:54:18    Security  Logon/Logoff   538     Tanner
          12/30/96 15:54:17    Security  Logon/Logoff   528     Tanner
          12/30/96 15:54:08    Security  Logon/Logoff   538     Administr
          12/30/96 15:54:07    Security  Logon/Logoff   538     Administr
          12/30/96 15:53:44    Security  Logon/Logoff   528     James
```

Figure 2.9.8.1-2

2.10 Implementing Server TCP/IP Advanced Security

The Transmission Control Protocol/Internet Protocol (TCP/IP) is the standard protocol for LANs. It is scaleable, routable, and allows systems using different operating systems to communicate. For these reasons and more, it is the protocol of choice for Internet use. However, it does not provide secure data transmissions. The potential threat of using TCP/IP discussed in this configuration guide includes having unauthorized entry into your system via TCP, User Datagram Protocol (UDP), and IP ports.

The established TCP/IP ports are used to facilitate communications between systems. **Disabling the ports prevents accidental or unauthorized entry – access to the system must be through a secure environment that can authenticate the user and then assign proper access rights, or through managed port selection**.

2.10.1 Using Advanced TCP/IP Security at the Server to Mitigate Security Threats

👍 The minimum port requirements for a Windows NT Server, acting as a PDC, BDC, or a Windows Internet Naming Service (WINS) Server, and nothing else, include the following:

- TCP Port 137 – Network Basic Input-Output System (NetBIOS) Name Service
- TCP Port 138 - NetBIOS Datagram Service
- TCP Port 139 - NetBIOS Session Service
- UDP Port 137 - NetBIOS Name Service
- UDP Port 138 - NetBIOS Datagram Service
- UDP Port 139 - NetBIOS Session Service
- IP Protocol Port 1
  - Additional port requirements needed if domain name service (DNS) or dynamic host configuration protocol (DHCP) will be used include:
    - TCP Port 53 - Domain Name Service
    - TCP Port 67 - DHCP/Bootstrap Protocol (BOOTP) Server
    - TCP Port 68- DHCP/BOOTP Server
    - UDP Port 53 - Domain Name Service
    - UDP Port 67 - DHCP/BOOTP Server
    - UDP Port 68- DHCP/BOOTP Server

✿ The minimum port requirements for a Windows NT Server configured to be an Exchange Server, and not a PDC or BDC, include the following:

- UDP Port 137 - NetBIOS Name Service
- UDP Port 138 - NetBIOS Datagram Service
- UDP Port 139 - NetBIOS Session Service
- TCP Port 25 – Simple Mail Transport Protocol (SMTP) [For use with the Exchange Internet Connector]
    - TCP Port 102 - ISO – Transport Service Access Point (TSAP) [For use with the Exchange x.400 Connector]
- IP Protocol 1

2.10.2 Configuring TCP\IP Advanced Security

👍 **Recommendation:** The following steps should be taken to configure TCP/IP advanced security:

1. Log on to the Windows NT workstation or server with an administrator's account.
2. Click the Network Neighborhood icon on the desktop and right click with the mouse. Select Properties.
3. Choose the Protocol Tab.
4. Click on the TCP/IP entry and then select the Properties button.
5. Click on the Advanced button.
6. Check the box to Enable Security, then select the Configure button.
7. For each type of entry (TCP, UDP, or IP Protocol) click on the radio button to Permit Only.
8. Add the appropriate type of ports, depending upon the server's function.
9. Once completed, click on the Close button and the OK button until the window closes. Follow the directions to reboot the computer for the changes to take affect.
10. Test that workstations can continue to log on to the domain and that applications can be properly accessed.

Note: This configuration does not include additional ports that may be required to support other applications using the TCP/IP stack, such as Oracle SQL*Net.

2.11 Recycle Bin

The Recycle Bin is a new feature in Windows NT 4.0. It allows users to recover files deleted from the local hard drive and easily return the files to their original location on the local system. By default, deleted files are saved in the Recycle Bin. However, since each file has an associated ACL, even deleted files stored in the Recycle Bin can be protected from unauthorized access. A user logged-on to the computer will have no access rights to any other user's deleted files on that same computer. This is an important security measure.

The security of the Recycle Bin can be further improved by modifying the properties to automatically delete files without saving them in the Recycle Bin. Having files immediately deleted provides additional protection, especially on systems used to process any level of classified information. Specialized software tools would be needed to recover a deleted file or restore the file from backup.

👍 **Recommendation:** Modify the Recycle Bin properties to immediately delete files. To change the properties of the Recycle Bin to immediately delete files follow these steps.

1. Select the Recycle Bin from the desktop, and click the right mouse button. From the menu, select the Properties option. Choose the Global tab.
2. Check the box next to "Do not move files to the Recycle Bin. Remove files immediately on delete."
3. Click OK to save changes and close.

2.12 Assigning File, Directory, and Registry Permissions

2.12.1 NTFS Default Configuration

NTFS provides the C2 compliant discretionary ACLs that can be configured to restrict data access on local hard drives and maintain audit trails of activity as required by Policy. Any *object* known to the Windows NT operating system can have ACLs attached to it. The objects which most users are familiar with are directories and files.

Directories are a class of objects called "container" objects, as they can "contain" files or other directories. Directories are often depicted as file folders in a graphical user interface (GUI) system such as Windows NT. NTFS supports ACL configuration for directories and files, as well as Windows for Workgroups and Windows 95 style share-level security settings. NTFS is a superb tool to use to help meet policy requirements of allowing users to see only what they "need-to-know" and granting users the least amount of access necessary to do their jobs. Windows NT will enforce the more restrictive of share permissions versus NTFS settings on directories and files when there is a configuration overlap.

Floppy disks cannot be formatted for NTFS. (Overhead data required to support security and redundancy for crash protection would be greater than the size available for data.) This means no files stored on floppies can be protected by ACLs. The same is true of files stored on CD-ROM.

2.12.2 Subdirectory Creation

By default, Windows NT computers with NTFS formatted hard drive partitions are wide open. That is, the group Everyone has Full Control (Control, Read, Write, Execute, and Delete) or Change Control (Read, Write, Execute, Delete) access to most of the directory tree. This condition has important security significance.

Windows NT assigns permissions to hierarchical subdirectories created on NTFS drives using rules of inheritance. For example, if a parent directory has the group Everyone with the Full Control permission, all child directories created under that parent will inherit the same permissions. This creates the need for the following actions:

👍 **Recommendation:** Network administrators should remove the Everyone group from the local ACLs of newly created subdirectories.

★ No users outside of systems staff should be assigned the “Full Control” permission, the Special Access “Change” permissions, or “Take Ownership” permissions for any file/directory objects.

2.12.3 The File Protection Model

This section describes how a system administrator may combine the use of hierarchical directories and NTFS permissions to create a file protection schemes. This information is presented for illustrative purposes only. Each system administrator must devise their own bureau specific version of this model. The goal is to create an environment where the principle of least privilege is implemented, and where controlled access protection governs the users' ability to obtain network resources.

👍 **Recommendation:** Before installing Windows NT, the system administrator should document the information protection goals for the entire office in which he/she works. This process would include the identification of the owner of the information, and articulation of the owner's expectations with regard to protection of that information, in concordance with the Policy and other governing regulations. The system administrator should use this information to create a technical plan containing the hierarchical layout of directories on the server or workstation, and determine what permissions will be applied to each directory. Functional groups, rather than individual users should be assigned permissions in ACLs for directories as much as possible. This will help minimize configuration details, and provide for simpler administration.

Recommendation: Groups and folders (directories) should be related to specific functional requirements.

- Create group folders that are general, such as one called \ACCOUNT, and assign the group ACCOUNT “Change” permission to that directory. This directory becomes the common shared file space for the ACCOUNT personnel.
- Create a folder called \ACCOUNT\COST, and assign the specific group ACCOUNTCOST Change permission to that directory.
- There can be private folders for the individuals who are members of the group under each of the group folders. These private folders should be protected in such a way that only the owner and the system administrator have access to the directory.

The private folders have NTFS permissions set to allow full access (read, write, execute, delete) only to the owner of the folder. Another access control entry (ACE) for the private folder permits coworkers from the same group to add documents to the user's private folder.

The Group folders are those designated for a group of users who have the same information access requirements. For example, it is reasonable to setup a group folder called "GENERAL COUNSEL Group" for all Attorneys. The GENERAL COUNSEL Group folder would contain workgroup documents shared by the Attorneys and their administrative staff. Any member of the group GENERAL COUNSEL could add, modify, or delete documents in this folder. The GENERAL COUNSEL Group folder also would contain the private folders for each member of the GENERAL COUNSEL section. Keeping the working data for a specific functional group in one place makes operational security easier, as well as simplifies administrative tasks such as backups. Figure 2.12.3-1 displays settings and folder definitions for use in implementing group folders.

Folder Type	Name	NTFS Perm	Results
Private	User Name e.g.: JJames	Change	Only the Owner (User Name) has full rights to add, modify, or delete anything in the folder.
Private	Section e.g.: Account	Add	Members of the Group can add documents to the User's Private Folder but have no other access.
Group	Section e.g.: Account	Change	Only the members of the Group can add, modify or delete anything in the Group Folder.

Definitions	
Private Folders	This folder is where each user stores his/her own work. Access is limited to the user for anything other than adding a document to the folder. The name of this type of folder is normally a composite of the last name and abbreviations of the user's First and Middle names. **John R. James's** Private Folder would be called JJames.
Group Folders	The Group Folder contains all the Private User Folders for the section, as well as a general repository for workgroup documents. Only the members of the specific group can access it. All of the Accountants (and their clerical/administrative staff) would have their workspace in this folder.

Figure 2.12.3-1

2.12.4 Setting Permissions in Windows NT 4.0

★ In Windows NT 4.0, directory permissions are set using the Explorer. Perform the following steps to set NTFS permissions.

1. Run Explorer and select the directory upon which you would like to set NTFS permissions.
2. Click the right mouse button on the target directory.
3. The last item in the list of options is Properties – click on it and you will see the Properties dialog.
4. Click on the Security Tab and then on Permissions. This box is where the system administrator sets the ACL for each directory.
5. Remove any unnecessary permissions. This determination will come from your information protection goals articulated at the beginning of this process.

👍 **Recommendation:** The ACL for the Group Folders should only include the group that owns the folders. For example, the ACCOUNT Group folder would contain ACEs allowing the group ACCOUNT "Change" access, and the group Administrators "Full Control" access

👍 **Recommendation:** Users and Groups should never be granted "Full Control" access to folders.

2.12.5 Permissions for the Windows NT System Directories

A default Windows NT installation grants the group Everyone "Change" access to critical directories. Unfortunately, many software packages and Windows NT programs write into these directories. Certain files (.INI files, drwtsn32.log, CMOS.RAM, etc.) may need to be set to allow Everyone "Change" access on an individual basis as needed.

💣 **Note:** While changing the directory permissions on the following directories, **DO NOT CHECK "Replace permissions on subdirectories". UNCHECK "Replace permissions on existing files"** where noted**.**

👍 **Recommendation: Figure 2.12.5-1** displays directory permissions which should be set on Windows NT, overriding default Windows NT installation settings.

Directory or File	User Groups	Recommended Permissions
\TEMP	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\IO.SYS	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\MSDOS.SYS	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\BOOT.INI, \NTDETECT.COM, \NTLDR	Administrators	Full Control
	SYSTEM	Full Control
\AUTOEXEC.BAT	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\CONFIG.SYS	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\USERS	Authenticated Users	List
	Administrators	RWXD
	SYSTEM	Full Control
\USERS\DEFAULT	Authenticated Users	RWX
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\WIN32APP	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control

Directory or File	User Groups	Recommended Permissions
	Server Operator	Full Control
\WINNT [System Root]	Authenticated Users	List
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\CONFIG	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\CURSORS	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\FONTS	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\HELP	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\INF	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\PIF	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\SHELLNEW	Authenticated Users	Read
	Administrators	Full Control

Directory or File	User Groups	Recommended Permissions
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\SYSTEM	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\SYSTEM32	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
	Everyone	Remove
\PROFILES	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
.	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\WIN.INI	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\WINFILE.INI	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM.INI	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\ODBCINST.INI	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control

Directory or File	User Groups	Recommended Permissions
\OBDCINST.INI	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
LOCALMON.DLL	Authenticated Users	Read
	Administrators	Full Control
	Power Users	Change
	SYSTEM	Full Control
PRINTMAN.HLP	Authenticated Users	Read
	Administrators	Full Control
	Power Users	Change
	SYSTEM	Full Control
REPAIR	Authenticated Users	Full Control
	Administrators	Full Control
\SYSTEM	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
	Server Operators	Full Control
\SYSTEM32	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\SYSTEM32\RDISK.EXE	Administrators	Full Control
	Server Operators	Read
	SYSTEM	Full Control
\SYSTEM32\REGEDT32.*	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM32\RCP.*	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM32\RSH.*	Administrators	Full Control

Directory or File	User Groups	Recommended Permissions
	SYSTEM	Full Control
\SYSTEM32\AUTOEXEC.NT	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM32\CMOS.RAM	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM32\CONFIG.NT	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM32\MIDIMAP.CFG	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM32\CONFIG	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM32\DHCP	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
	Power Users	Change
\SYSTEM32\DRIVERS	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
	Server Operators	Full Control
\SYSTEM32\OS2	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM32\RAS	Authenticated Users	Read
	Administrators	Full Control

Directory or File	**User Groups**	**Recommended Permissions**
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
	Power User	Change
\SYSTEM32\RAS\*.*	Administrators	Full Control
	SYSTEM	Full Control
\SYSTEM32\REPL	Authenticated Users	List
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\SYSTEM32\REPL\EXPORT	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
	Replicator	Read
	SERVER OPERATORS	Change
\SYSTEM32\REPLL\IMPORT	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
	SERVER OPERATORS	Change
	Replicator	Change
\SYSTEM32\SPOOL	Authenticated Users	Read
	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
	SERVER OPERATORS	Full Control
	PRINT OPERATORS	Full Control
\SYSTEM32\WINS	Authenticated Users	List
	Administrators	Full Control
	SYSTEM	Full Control
\PROGRAM FILES	Authenticated Users	Add and Read
	Administrators	Full Control

Directory or File	User Groups	Recommended Permissions
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\REGEDIT	Administrators	Full Control
	SYSTEM	Full Control
\PROFILES\ADMINISTRATOR	Administrators	Full Control
	CREATOR OWNER	Full Control
	SYSTEM	Full Control
\NTSERVICEPACKUNINSTALL	Administrators	Full Control
	SYSTEM	Full Control
\NTUNINSTALL*	Administrators	Full Control
	SYSTEM	Full Control
\SENDTO	Authenticated Users	Read
	Administrators	Full Control
	SYSTEM	Full Control

Figure 2.12.5-1

2.12.6 Disable POSIX and OS/2 Subsystems

★ The system administrator must disable the POSIX subsystem by deleting the following ps*.* files from \WINNT\SYSTEM32. If not running the Microsoft Multitasking MTA, the system administrator must disable the OS/2 subsystem by deleting the following os2*.exe files from \WINNT\SYSTEM32.

- psxss.exe
- posix.exe
- pscdll.dll
- os2.exe
- os2ss.exe
- os2srv.exe

2.13 NTFS Move/Copy

Some clarification regarding ACL creation that results from using the COPY and MOVE files functions within an NTFS file system environment is necessary. **In a copy operation, NTFS considers the destination file to be a new file whose ACL is based on the default new file ACL of the destination directory, rather than ACLs on the source file. Ownership of the new file is recorded as that of the user who performed the move/copy operation instead of keeping ownership settings of the original file**.

In contrast, the move operation includes the deletion of the source file, and the newly created file takes upon the ACL attributes of the target directory.

2.14 Protecting Application Files

To prevent users from inadvertently damaging the application software by deleting or overwriting essential files, theoretically, users should not have Write or Delete access to change an application's files and directories. The caveat is that some applications attempt to write user configuration or preference data to the executable directory. The system administrator will need to determine the application's needs with regard to writing to the executable directory.

Additionally, application files should be installed in subdirectories separate from any data directories.

👍 **Recommendations**: The following permissions can be set on applications installed in the manner described:

- When possible, store applications on the server. Server-based storage of executable code will ensure the integrity of the application software, while facilitating upgrades and access control.
- Permissions on applications directories (e.g., "\Program Files\MsOffice") may be set as follows:
- Administrators: Full Control (All) (All)
- Users: Read Access (RX)(RX)
- SYSTEM: Full Control (All) (All)
- When establishing permissions for locally defined groups, system administrators must ensure that groups are assigned only those permissions required to perform their assigned duties.

2.15 Directory Replicator Service

Directory replication allows system administrators to create and maintain identical directory trees and files on multiple servers and workstations. It can be used for load balancing and file maintenance, however, it introduces potential security vulnerabilities if not properly administered. The Directory Replicator Service requires a user account and a service on the server. There is potential for unauthorized disclosure of information through the misconfiguration of import and export directories.

👍 **Recommendation**: The Directory Replicator Service should be activated only by system administrators who fully understand its configuration. A unique user account should be established for this service, and the user account should be audited.

2.16 Configuring Printers

2.16.1 User Restrictions

★ Users must be restricted to printers within their functional areas. Additionally, only authorized system staff are to be granted Full Control over any dedicated or shared printer. **By default, users are permitted to print and delete their print jobs. No further access is required of general users**.

👍 **Recommendation**: In some cases, it may be useful to assign a user to the Print Operators group in NT Server, and modify the ACL of a particular printer object to allow that group Manage Printers permission. This can be implemented at the discretion of the system administrator.

2.16.2 Copying Files to the LPT Port

Access control lists managed by the Print Manager refer to the object representation of the print queuing mechanism, and not the printer or even physical port (parallel or serial). The executable print queue components of Windows NT opens the computers physical port for exclusive access only for the period necessary to pass a given print stream to the printer device. This means that even though Print Manager is used to set NO ACCESS for a given user to a specific ‘printer’, that user can copy files to the LPT port successfully.

2.17 Remote Access/Dial-up Networking

✿ Some sites may need to grant remote access to servers or other network resources for traveling users. Windows NT includes the Dial-up Networking/Remote Access Service (RAS) utility suite to provide for dial-up participation of Domain users. While approved for use with National Security Agency (NSA) approved encryption (e.g., AT&T 1910), this functionality has not been formally reviewed.

2.17.1 Prohibited RAS Use

✿ RAS supports a number of protocols and technologies, including X.25, integrated services digital network (ISDN), and the Internet point-to-point protocol (PPP) and serial line interface protocol (SLIP). Use of the RAS tools for connection of networked Windows NT computers to non- Department LAN/WAN environments is prohibited, as the act links the Department WAN with unknown, untrusted computers.

💣 Connection of a Windows NT computer on a network to the Internet through RAS puts the entire WAN at risk, as there is no Firewall protection.

★ RAS use must be restricted to specific asset use, to connect with strictly configured ‘internal’ servers, and must use currently approved encryption technologies.

2.18 Password-Protected Screen Saver

A password-protected screen saver automatically locks a server after a specified time period without keyboard or mouse activity. To unlock the server, the user must enter the correct password. An additional step towards securing the server would be to not allow a screen saver.

★ **Password-protected screen savers on servers are not allowed. System administrators must log off of the system whenever they leave the area**.

2.19 Service Pack 3

Microsoft recently released Service Pack 3, which includes many fixes from the last release, and also offers several new security features for NT. Service Pack 3 offers five security features, three of which are to be used on the NASA systems. These are the:

- Server message block (SMB) signing, also referred to as the Common Internet File System (CIFS), is a protocol that lets systems transparently access files that reside on remote systems. Packets are inspected to ensure that they came from the system it was supposed to, therefor helping eliminates attacks.
- Anonymous user group is similar to the Everyone group, but it never becomes a member of an authenticated users group. Anonymous accounts are used for system to system communications. Activity of this account shows up in the Event viewer security logs.
- System keys help prevent attempts to crack passwords by using encryption techniques to protect password information stored in the Registry.

👍 **Recommendations**: The security-related changes that NASA to implement for the NT workstation and server are:

- Enable Server Message Block signing via the Registry.
- Disable the Anonymous user group.
- Select the machine-generated random key as the system key.

2.20 Wiping System Page File

Windows NT virtual memory uses a system page file to swap pages from memory of different processes onto disk when they are not being actively used. When the system is running, this can be accessed exclusively by the operating system and is protected. This should, however, be wiped clean when the system shuts down. This ensures that sensitive information will not be available to a malicious user.

If not already active, this feature is accessed by selecting the Start button, Run, and type in REGEDT32.exe at the prompt.

1. **Select the HKEY_LOCAL_MACHINE on the local machine window.**
2. **Select \System\CurrentControlSet\Control\SessionManager**
3. **Select the Memory Management key**
4. **From the Edit menu, choose Add Value...**
5. **At the Value Name: prompt, enter ClearPageFileAtShutdown.**
6. **Select REG_DWORD from the Data Type: drop down list.**
7. **Choose OK in the Add Value window.**
8. **Enter the number 1 (one) for the Data: value in the DWORD Editor, and click on OK.**

3. SERVER ADMINISTRATION

3.1 Log On/Log Off

★ The Secure Attention Sequence (SAS) must be used for initiating both log on *and* log off of Windows NT systems.

The SAS is performed using the same key sequence that would initiate reboot of a DOS/Windows system: CONTROL/ALT/DELETE keys pressed at the same time. This key sequence is special to Windows NT and is not 'caught' by any non-system programs, and is therefore 'Trojan horse proof'. Other options are available to cause log off, such as Program Manager/File/Shutdown menu choice, but they can be 'faked', as can a false logon screen. The SAS gives assurance that no bogus code can be used to gain userid/password combinations or bluff the user into divulging otherwise secure information. Once a user has logged off a server or workstation, services continue to run.

3.2 Emergency Repair Disk

Windows NT installation procedures include the creation of an Emergency Repair Disk (ERD), which is used to recreate Registry databases in the case of a system crash. **Recent revisions of Windows NT include a tool for creating a *fresh* ERD, including all changes made to device drivers, system services, and user logon credentials. It is possible for a rogue ERD to be loaded that would nullify current security settings, restoring a previous environment.**

★ **It is imperative that only authorized system staff create ERDs. Additionally, all ERDs must be handled as system backup material and stored in a secure location.**

Note: The ERD is not a complete solution for recovering the system. A Backup utility must be used in conjunction with the ERD to fully recover from a disaster. The ERD cannot fully restore the system partition information, cannot repair unmountable partitions except for the system partition, and does not replace a damaged NTFS boot sector.

To create an Emergency Repair Disk, a 1.44MB diskette is required:
1. Select Start, and then Run.
2. Type **rdisk /s** in the dialog box, and then OK.
3. Select Yes in the Setup window to create the emergency repair disk.

3.3 Last Known Good Configuration

A fail-safe feature of Windows NT, known as ‘Last Known Good Configuration’, allows for rollback to the most recent successful boot configuration, should errors keep a system from starting or operating properly. Settings that would be rolled back, such as administrator passwords, may provide opportunity for malicious activities.

Recommendation: System administrators may consider cycling through a second system boot after making key changes to security settings on users or groups. **File system access control list (ACL) changes are not cached with ‘Last Known Good Configuration’ and would not be affected**.

3.4 Log On Credentials from Domain Server

A Windows NT Domain has one Primary Domain Controller (PDC) that keeps a master copy of all user log on credentials. Other Windows NT Server computers may serve as Backup Domain Controllers (BDC) and keep copies of the master user security database. In this way, if the PDC is down or unreachable, users will still be authenticated.

If a Windows NT Server that is a member of a domain is booted and cannot contact a PDC or BDC, a user can log on locally with ‘cached’ credentials from the last time the user signed on to that server. This condition presents a potential picture of latency of domain security settings at the workstation. For example, suppose an NT Workstation is setup to only allow log on using a domain account. The system administrator disables the account of the user of that workstation on the PDC. With knowledge of this scenario, a disgruntled, disabled user could disconnect his workstation from the local-area network (LAN) and log on to the computer using the cached credentials, thereby accessing any information on that system (but not systems on the network). The system administrator can delete cached profiles by logging on to the local workstation, choosing System from the Control Panel, selecting the User Profiles tab and deleting the user's profile from the list.

★ The system administrator must delete any cached profiles of disabled accounts on local workstations (and servers, if the cached profile belonged to an administrator) to prevent unauthorized entry.

3.5 Performing System Security Audits

There are several third party utilities available that make it easy for a system administrator to perform periodic security audits of the Windows NT system. Audit areas may include C2 compliance, file and registry ACLs, user account status, and other areas of security concern. Three utilities include: Intrusion Detection's Kane Security Analyst (KSA); Somarsoft's DumpAcl; and the C2 Configuration Utility included in the Windows NT Resource Kit. A brief description of the utilities is included in Section 6, Third Party System Auditing and Analysis Utilities.

3.6 Add-ins for Windows NT Components

Some utility programs included with Windows NT are extensible through custom coding or scripting. Freeware and commercial products are available that provide some useful functionality when 'grafted' in to the familiar Windows style utilities. Examples might include a stopwatch start/stop tool to time phone conversations, tickler files to beep as reminder of appointments, encoder/decoder tools, or file compressors. Extreme caution must be exercised to prevent individuals from installing their own personal system enhancements, as this type of enhancement is a prime 'Trojan horse' vehicle. It must be recognized that while a user is signed on, any program that is run *is* that user and can exercise the full permission set available to that user.

👍 **Recommendation**: End users should be educated regarding good computer security practices. This training should include information regarding users' responsibilities in preventing the spread of viruses and other wildlife, and the prohibition regarding installation of personal computer software.

-

3.7 Backups

Regular backups of data on servers and local hard disks prevents data loss and damage caused by disk failures, power outages, virus infection, and network problems. It is critical on an operational system to perform backups regularly.

★ The system administrator must implement and document a full backup and recovery procedure for system programs and information to ensure continuity of operations.

★ Backup tapes must be stored securely and audit logs must be reviewed regularly.

👍 **Recommendation:** A backup plan should include the following:

- A schedule of when the backups take place.
- A schedule of tape rotation.
- A tape storage plan. If physical security is implemented to protect servers, but unauthorized people can get access to your backup tapes, data is not protected. Any on-site location should be as far away from the information processing facility as possible. The system administrator must ensure that alternate storage locations are protected from environmental conditions, such as extreme heat, humidity, air pollution, and fire.
- A list of spare hardware in case of a failure in the backup device.
- A plan to test backed up data regularly to verify that backup procedures and equipment are reliable. It is a good idea to check to make sure that backup is working properly by performing a restore occasionally.
- A list of data to back up. Different types of data that should be backed up include:
- **User Data:** The greatest amount of change on any server is in the users' folders. Users constantly add, modify, or delete files from the computer. The system administrator should perform daily backups of changes to users' folders.
- **Registry:** The Registry is the most critical set of system files on the computer as far as day-to-day operations are concerned. A user would know quickly if a system file is missing or corrupt — the computer would crash, or fail to execute the command. The Registry is different. he computer might start, then hang at the logon screen because all the security settings are missing or some required service did not start. The system administrator must ensure there is a current backup of the Registry, particularly on a PDC. Otherwise, if the PDC crashes and a BDC is not available, the system administrator would have to rebuild information about all users, groups, and permissions.
- **Application Programs:** Application programs, such as Microsoft Word for Windows, are typically what network users are involved with on a daily basis. The system administrator can always reinstall the executable files from the original distribution media, but the down time and lost productivity make this approach less than ideal. Additionally, the system administrator might have customized the application programs to suit the organization needs. The difficulty of reproducing those settings can be greater than reloading the programs themselves.

In case of disaster (data loss, hardware failure, power outages, etc.), a recovery plan needs to be in place. Backup operations based on careful planning and reliable equipment make file recovery easier and less time consuming.

3.7.1 Backup Products

Many Windows NT backup utilities are available today. NASA is currently using the following two products.

3.7.1.1 Legato NetWorker for NT

Legato NetWorker for NT, v4.4, is an Enterprise solution that is being used in the NASA environment on HQDATA1 and HQDATA2. This product will be used for all servers once it proves to be a solid performer. Compared to other backup products, Legato is very granular in that a Backup Administrator creates and schedules the jobs, and a Backup Operator can start, stop, pause, or cancel jobs only, and not reconfigure anything. The separation of duties helps the backup operation be less prone to human error.

An add-on product developed by St. Bernard Software, Open File Manager, in also being used. This product copies of the file as it existed in its binary form at the time it was first opened by the client. The product does not require that the server has ‘exclusive lock’ on the files.

3.7.1.2 ARCserve

ARCserve 6.0, from Cheyenne Software, Inc., is also an Enterprise Backup solution for Windows NT 3.5x and NT 4.0 and is the first such program to earn Microsoft’s “Designed for BackOffice” seal of approval.

ARCserve 6.0 backs up mission critical data including in-use files, the NT Registry, messaging systems such as MS Exchange and Lotus Notes, and databases such as MS SQL Server and Oracle Server without interrupting operations.

4. THIRD PARTY SYSTEM AUDITING AND ANALYSIS UTILITIES

There are several third party system auditing and analysis utilities available that make it easy for a System Administrator to perform periodic security audits of the Windows NT system. Three utilities that tend to complement one another are described below.

4.1 Kane Security Analyst 4.0

The Kane Security Analyst (KSA) by Intrusion Detection Systems is a useful tool for assessing Windows NT networks, servers, or workstations. An evaluation of KSA software and found it to be a valuable tool for system administrators. The various reporting of KSA covers all aspects of NT security, and the software is easy to install, configure, and run. Configuring the software does not require extensive knowledge of Windows NT and the application is easy to use.

KSA checks Windows NT 3.51 or 4.0 domain, server(s), or workstation(s) for security vulnerabilities based on predefined security policies. The default security policies are based upon Intrusion Detection's own "Best Practices" in addition to C2 level security specifications. KSA modifiable security standards cover all areas of the C2 level requirements for Windows NT and many of the *Windows NT 4.0 Security Configurations*. The software does not make permanent changes to the NT operating environment, instead it reports the vulnerabilities.

Current KSA voice/fax numbers, hard copy mail address, and up-to-date ordering instructions including current prices are available at http://www.intrusion.com. The Intrusion Detection's "Best Practices" for NT security span six critical areas. These are:

- **Account Restrictions:** Verifies authorized users of the system prior to their use.
- **Password Strength:** Confirms that the Administrative controls over passwords conform with best practices.
- **Access Control:** Reviews access controls to system and data resources.
- **System Monitoring:** Audits unauthorized and authorized system and user activities.
- **Data Integrity:** Ensures that overall system integrity is in place.
- **Data Confidentiality:** Ensures that data is secure when stored on and transmitted across the network.

Reports generated by the software compare the predefined security criteria against the actual Windows NT configuration being assessed. The list of NT security features KSA analyzes includes:

- Domain Security
- Excessive User Rights
- Registry Security Settings
- Group and User Access

- Audit Policies
- Event Logs
- Shares
- Access Control List (ACL) Directory Permissions
- Uninterruptible Power Service (UPS) Status
- Vulnerable User Ids

4.1.1 Software Features

The four major functions available as icon selections for KSA software are:

- **Set Security Standard:** Where assessment criteria is customized. The NT 4.0 configurations should be applied here.
- **Run Security Audit:** Three choices of run mode can be selected:
    - ▪ Update Last Assessment Based On Current Security Standard
    - ▪ Develop a Previously Stored Snapshot
    - ▪ Take and Develop a New Snapshot On Current File Server
- **Survey Risk Analysis:** Displays overall risk survey in graph form of the six security areas and their assessment score. Individual machines can be displayed for more detail.
- **Review Compliance History:** Displays assessment dates and scores.
- Additional Icon Functions include:
    - **Account Policy Analysis** displays default account information for setting up new users of all machines assessed.
    - **Report Manager** lets you select which assessment reports you want to print.
    - **Expert Mode Analysis** allows you to view how every User ID scored on the assessment. The three security areas that are analyzed are Account Restriction, Password Strength, and Access Control.
    - **Report Card** shows how the assessment scored based on the six security areas.
    - **Event Log Analysis** shows Security Events and Login violations for each machine assessed.
    - **C2 Security Summary** details nine requirements of C2 level security and reports pass/fail status for each machine that was assessed.
    - **File Rights** show which groups have what access levels to files on all machines that were assessed.
    - **Registry Rights** show which groups have what access levels to the registry of all machines that were assessed.
    - **Archive Management** allows you to save assessments to a specified file location or open existing assessments that have been archived.
    - **View Scheduled Assessments** lets you see the schedules, if any, that were set up.

4.1.2 KSA Reports

The reports that KSA generates after the assessment is performed are:

- **Security Report Card:** Based on the six security areas listed earlier. Included in this report are ten areas where improvements are most needed.
- **Audit Policy Report:** Failed and successful security events. Lists all assessed machines and reports the security audit log results (Security Event Log Auditing must be enabled).
- **Account Policy Analysis:** Compares the security standard settings to the actual account policies defined on the machine or domain.
- **Trusted Domains:** Lists all one-way and two-way trusts.
- **Domains That Cannot Be Administered.** Trusted domains that KSA could not return information about.
- **Password Cracking Summary:** Lists all User IDs for passwords found in the Cracker's Dictionary.
- **Current User Compliance Summary:** A compliance score is recorded for the assessed domain, along with the importance of each test performed in the categories of Account Restrictions, Password Strength, and Access Control.
- **Login Violations:** Summarizes failed login attempts and account lockouts from the event log.
- **Security Events Summary:** Lists all failed and successful security events that are in the security audit log of all machines assessed at the time of assessment.
- **Password Scripting On Machines**: Checks that no passwords are being stored in the registry as clear text.
- **C2 Security Compliance Summary:** Displays a machine's adherence to the C2 security standard.
- **Sensitive Services Summary:** Checks all machines for Remote Access Service (RAS), File Transfer Protocol (FTP), Structured Query Language (SQL), Dynamic Host Configuration Protocol (DHCP), and Internet Information Servers (IIS) services running**.**
- **User IDs Never Logged Into:** Checks for User IDs never used.
- **Guest User ID Security Summary:** Tests eight requirements for tight control of the GUEST account and whether they are being followed.
- **Inactive User IDs:** Checks against predetermined length of time.
- **UPS Device Summary:** Checks whether UPS service is turned on and configured.
- **Machine Compliance Summary:** Based on criteria for three security categories – System Monitoring, Data Integrity, and Data Confidentiality.
- **Machine Security Log Configuration:** Auditing configuration information.
- **Started Services Summary:** Services started on every machine assessed.
- **Application and System Log Summary:** Displays the settings defined for application and system logs.
- **Account Restrictions Summary:** Lists all users in domain and account restrictions.
- **Password Strength Summary:** Lists password weaknesses.

- **Group Membership Report:** Lists all groups and members of each group.
- **Group Membership (By User):** Lists all users and groups which they are members.
- **Access Control Report:** Lists all users and groups and whether they have excessive User Rights or Administrator equivalent.
- **Disabled Users Report:** All accounts either disabled by administrator or locked out.
- **Network Authentication From Non-NT Clients:** Lists any machines running client software other than Windows NT.
- **Current Security Standards For Windows NT:** Summary of the security standards that were used to perform current assessment.
- **User Account Summary:** Lists all users by full name and description.

4.2 Somarsoft DumpAcl

DumpAcl is a program for Microsoft Windows NT that will dump the permissions (discretionary access control lists - DACLs) and audit settings (SACLs) for the file system, registry, printers, and shares. This report can be sent to the screen, file, or printer in a listbox format that is easy to read and makes apparent any holes in system security. DumpAcl also dumps user, group, and replication information.

Current Somarsoft voice/fax numbers, hard copy mail address, and up-to-date ordering instructions including current prices are available at http://www.somarsoft.com. Some of the various reports that DumpAcl generates are: permissions reports for file systems, registry, printers, shares and shared directories; and, reports for users, groups, policies, rights, and services.

4.3 C2 Security Manager

The C2 Configuration Manager software is included in the Windows NT Resource Kit. C2 Configuration Manager reports the security posture of NT Servers or Workstations in accordance with predefined C2 Security Standards, as defined in the National Computer Security Center (NCSC) Orange Book, and may be used to make changes to security attributes within Windows NT Server or Workstation.

The utility will check only the NT Server or NT Workstation on which it is installed. C2 Configuration Manager reports upon and has the ability to make changes to the following areas on an NT server or workstation:

- **File Systems** – Checks if all volumes use NT file system (NTFS). If they do not, gives the option to format the volumes.
- 💣 **OS Configuration** – Checks if DOS is installed on the system. If it is, gives the option to delete the MS-DOS system files, and sets the system selection time to 0.

- **OS/2 Subsystem** – Checks if the OS/2 subsystem is installed, and if it is gives the option to disable it.
- **Posix Subsystem** – Checks if the Posix subsystem is installed, if it is, gives the option to disable it.
- **Security Log** – Checks whether the Security Log is set to overwrite events, and gives the option to change setting to Do Not Overwrite, or Overwrite as needed.
- 💣 **Halt on Audit Failure** – Checks whether the System is set for halt when security log is full, and gives the Option to set to halt.
- **Display Logon Message** – Checks whether a logon message is displayed. Gives a text box for typing in a message to be displayed.
- **Last Username Display** – Checks whether the previous name is displayed at log on, and gives the option to hide it.
- **Shutdown Button** – Checks if the shutdown button is displayed, or whether a User has to log on in order to shutdown the computer. Gives an option to select Hide Shutdown button.
- **Password Length** – Checks whether a minimum password length has been set – C2 password length is 6. Gives the option to change required password length.
- **Guest Account** – Checks whether the Guest Account has been disabled, and if not, gives the option to disable it.
- 💣 **Networking** – Checks whether there are any networking services installed. To be C2 compliant, ideally would be to have a stand-alone computer. Gives the option to delete any networking services.
- **Drive Letters & Printers** – Checks whether only administrators may assign drive letters and printers, or whether all users can. Gives option to change to only administrators.
- **Removable Media Drives** – Checks whether floppy drives and CD-ROM drives are allocated at log on. Allocating them prevents programs other users are running from accessing them. Gives option to allocate drives.
- 💣 **Registry Security** – Checks whether Access Control Lists have been set to restrict access to the system registry keys. Gives option to apply permissions, and stores information in the file C2REGACL.INF.
- 💣 **File System Security** – Checks whether Access Control Lists have been set for the files in the system directories. Gives option to apply permissions, and stores information in the file C2NTFACL.INF.
- **Other Security Items** – C2Config program is unable to detect these items, but states that they should be configured:
  - Power-On Password – The power-on password feature, to be C2 complaint, must be configured as documented in the *Setup and Installation Guide*.
  - Secure System Partition (reduced instruction set computing (RISC) systems only) – Use disk administrator to secure RISC system partition.
  - Change User Manager Program Icon – Setting up NT Server, the User Manager for Domains icon must be replaced with the User Manager icon.

- Restrict Use of User Rights – Configure user rights of the accounts on the system as described in *Windows NT C2 Security System Administrators Guide*.

💣**Use caution** when using the C2 Configuration Manager to make changes to your NT installation. **Improper use may cause undesirable results.**

Appendix A

Acronyms

Acronyms

Acronym	Defined As
ACE	Access Control Entry
ACL	Access Control List
BDC	Backup Domain Controller
BIOS	Basic Input-Output System
BOOTP	Bootstrap Protocol
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
DACL	Discretionary Access Control List
DCOM	Distributed Component Object Model
DDE	Dynamic Data Exchange
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DOS	Disk Operating System
ERD	Emergency Repair Disk
FAT	File Allocation Table
FTP	File Transfer Protocol
GUI	Graphical User Interface
HPFS	High-Performance File System
ID	Identification
IIS	Internet Information Server
IP	Internet Protocol
ISDN	Integrated Services Digital Network
KSA	Kane Security Analyst
LAN	Local-Area Network
LSA	Local Security Authority
NCSC	National Computer Security Center
NetBIOS	Network Basic Input-Output System
NSA	National Security Agency
NTFS	NT File System
OS/2	Operating System/2
PC	Personal Computer
PDC	Primary Domain Controller
PPP	Point-to-Point Protocol
RAID	Redundant Array of Inexpensive Disks
RAMP	Rating Maintenance Phase
RAS	Remote Access Service

Acronym	**Defined As**
RISC	Reduced Instruction Set Computing
SAM	Security Account Manager
SAS	Secure Attention Sequence
SID	Security Identification
SLIP	Serial Line Interface Protocol
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Mail Protocol
SQL	Structured Query Language
SRM	Security Reference Monitor
TCP	Transmission Control Protocol
TSAP	Transport Service Access Point
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
WAN	Wide-Area Network
WINS	Windows Internet Naming Service

Appendix B

Windows NT 4.0
Server Security Configuration Checklist

Windows NT 4.0
SERVER
Security Configuration Checklist

	YES	NO
OPERATING SYSTEM (Section 2.0)		
Windows NT 4.0 is the only operating system.		
Windows NT 4.0 using only NTFS partitions.		
SERVER INSTALLATION AND CONFIGURATION		
Hardware Considerations		
Only hardware listed in Microsoft's Hardware Compatibility List is used.		
Physically Securing Server and Software (Section 2.2)		
BIOS Year 2000 compliant.		
Safeguard hardware and Windows NT operating system as listed below:		
Physically restrict and limit access to hardware, particularly any configured as Windows NT Servers. Servers should be housed in the computer room.		
Physically secure the hard drives by locking them in place, or locking the case to prevent unauthorized removal of the media.		
Force Domain Administrators to log on to any Windows NT Server locally.		
Disable the floppy drives through the BIOS to prevent it from being used as a boot device, and to prevent unauthorized installation of software.		
Password protect the BIOS to prevent the floppy drives being activated without authorization.		
Physically secure software, particularly the Windows NT installation disks and CDs.		
Virus scanning software installed and regularly used to detect and remove viruses.		
Disk Redundancy: Stripe Sets and Mirror Sets (Section 2.3)		
Use RAID 1 or RAID 5 disk redundancy method.		
Disk redundancy hardware conforms to Microsoft's Hardware Compatibility List.		
Access to User Manager utility in both stand-alone and domain environments restricted to unauthorized system staff.		
Guidelines followed as listed below for creating and managing user accounts.		
The system administrator must establish an account for every individual requiring access to NT workstations or server resources.		

	YES	NO
Users must not share accounts. Accounts used for services or proxies must be unique to the service.		
Each user account must be included in only those groups assigned permissions and/or rights to those resources required operationally by the user.		
Do not assign a user account to a new user by changing the username and other properties of an existing user account.		
System and domain administrators are required to maintain at least two user accounts. User accounts that are members of the Administrative group must be used only for performing administrative functions. Normal processing must be done with a non-privileged account.		
User Account Policy (Section 2.6)		
Settings listed below established within the Account policy		
Maximum Password Age - Set to Expire in 90 days.		
Minimum Password Age - Set to none, as a user can bypass this feature.		
Minimum Password Length - Must be 6-8 characters in length. Under no circumstances are blank passwords permitted.		
Password Uniqueness - The default value of five provides a sufficient rotation period.		
Account Lockout - Must be selected. The following are the minimum required settings. System administrators may implement a more restrictive lockout policy if required by their operational environment. Lockout after 3 bad log on attempts Reset count after 30 minutes Lockout duration 'forever'		
Forcibly Disconnect Remote Users When Logon Hours Expire - NT Server only. Use this box judiciously. While it may be desirable, forcibly logging off a user may cause a loss of data.		
Users Must Log On to Change Password - Leave unchecked. When unchecked, allows users to change their expired passwords without notifying an administrator. (Note: This is optional. Password changing may be handled manually by the system administrator.)		
PASSFILT.DLL installed.		
Recommended changes listed below are made in reference to user rights.		
Access this computer from the network. Revoke this right from Everyone and Power Users. Add only groups that need to access this computer from the network. Revoke this right from Administrators to force Administrators to log on locally (optional).		

	YES	NO
Debug programs. Revoke this right from Administrator on domain controller and non-domain controller servers.		
Log on locally. On domain controllers and non-domain controller servers, revoke this right from everyone *except* administrators.		
Shut down the system. On domain controllers and non-domain controller servers, revoke this right from everyone *except* Administrators.		
Configurations listed below followed when establishing user account settings.		
User Name. Must be configured in accordance with policy naming conventions. The required format is [FIRST INITIAL][LAST NAME]. Example: JJames.		
Full Name. Follow naming conventions.		
Description. Should include the individual's job title, e.g., Clerk or Secretary.		
User Must Change Password at Next Logon. Should be selected unless the system administrator chooses to handle password changes manually.		
Users Cannot Change Password. Should not be selected.		
Password Never Expire. Policy requires that users' passwords change every 90 days. This feature can force a user's password to expire at the end of this time automatically. This may be done manually, as well.		
Account Disabled. Do not select for normal users. Could be used to temporarily turn off an account, or for TDY accounts.		
Groups. The system administrator of security officer must create an NT group plan, logically dividing all users into functional areas. Users must be assigned only to those groups that they need for access to resources required to perform their job duties.		
Profile. See Section 2.8.2, Implementing System Policies. Login Scripts: In the \winnt\system32\repl\import\scripts directory. Should be stored on an NTFS partition. NT permissions to login scripts must be restricted to execute for users (this is the default). Login scripts may be configured to connect users to those resources required to perform their assigned duties. Additionally, the login script may be used to synchronize the workstation's clock with the primary domain controller. This is achieved by adding a 'net time' statement to the beginning of login scripts as follows: net time "\\name of the primary server"/set/yes Home Directory: The default home directory \USERS\DEFAULT is located on the local drive of an NT workstation. To ensure that all data files are being backed up, system administrators may change the default home directory to a sub-directory of a shared		

	YES	NO
network directory on a server. All home directories must reside on an NTFS drive.		
Hours. By default, users are permitted to access NT at any time. The system administrator must establish reasonable hours of operation for the system and ensure that access to the network outside of normal business hours is monitored. This option can be modified for individuals requiring access after normal business hours on an as-needed basis.		
Logon To. The system administrator may use this option to specify the workstations from which a user can log on to using this domain account.		
Account. Account Expires: the system administrator may choose to create an account with an expiration date (for example, a TDY user account). Normal accounts should never expire (this is the default). Account type: All accounts should be global, which is the default.		
Guest account disabled.		
All user accounts specifically identify an authorized user.		
Administrator Account renamed.		
Administrator account only used by the system administrator or delegated alternates.		
Second (personal) account for non-administrative functions created for system administrator.		
Password for administrator account stored in writing and secured in accordance with policy.		
Groups (Section 2.7)		
Rule of thumb listed below followed to manage security using groups.		
Devise a Windows NT group architecture based on functional/operational needs.		
Create the user accounts and add them to these functional/operation groups.		
Apply NTFS permissions against functional/operational groups by adding only groups to the ACLs for objects (e.g., files and printers).		
Principle of least privilege followed when assigned users to groups.		
Membership on a group determined by the user's need to access the collective resource permissions and system rights of the group.		
All groups created by system administrator and possess only those privileges required by the group to perform assigned duties.		
Configurations listed below followed with respect to built-in local groups.		
Administrators - Membership in this group results in the user account gaining superuser attributes. This group must include only the		

	YES	NO
designated security officer, system administrator, and authorized system staff. General users must never be assigned to the Administrators group. The username “Administrator” must not be listed as a member of this group (this vulnerability is removed by implementing the recommendations contained in the section on built in user accounts.		
Backup Operators - This group must include only those system staff assigned backup duties, if they are not already members of the Administrators group. No excess user access rights have been assigned to this group. However, it is important to note that any user assigned access to this group will be able to backup all files on the system regardless of the permissions established on the files.		
Everyone - This group encompasses all local workstation and domain users, and all users from other domains. Note: By default, many NTFS permissions on objects allow the Everyone group Change access (9, Write, Execute, and Delete) or Full Control access (Change access with Take Ownership and Change Permissions access added), This is completely opposite to the principle of least privilege. Changing this default must be addressed aggressively by the system administrator. (See assigning User Rights and Assigning File, Directory, and Registry Permissions sections.)		
Guests - Username “Guest” must be disabled. Anyone authorized to sign-on to a computer resource must be fully identifiable through user account credentials.		
Users - This group should provide a template for locally devised common functional/operational user groups.		
Add users to global groups on the domain.		
Add the global groups to local groups.		
Membership in Domain Admins group limited to administrators.		
Domain Users considered a template for creating global groups comparable to the Users local group.		
System Policy (Section 2.8)		
Recommendations followed as listed in Section 2.8.1 in reference to implementing system policies.		
All users without administrative privileges included in the group Domain Users.		
Domain Users group has the user right “Access this Computer from the Network” applied using the User Manager for Domains.		
“Access this Computer from the Network” applied only to non-administrator groups and users.		
Legal notice displayed on all automated information systems.		

	YES	NO
Windows NT Auditing (Section 2.9)		
System and object auditing activated as listed below in User Manager for all domain controllers and servers within a domain.		
Logon and Logoff - Failure. Note: Logon and Logoff Success may be added as needed for system auditing.		
File and Object Access - Failure		
Use of User Rights - Failure`		
User and Group Management - Success and failure		
Security Policy changes - Success and failure		
Restart, Shutdown, and System - Success and failure		
Process Tracking - Failure		
Access to Manage Auditing and Security Logs limited to the system administrator and security officer.		
All security logs reside on NTFS drive.		
Within File auditing, all Windows NT operating system files audited for failed attempts.		
Within Registry Key Auditing, all registry keys and sub-keys audited for failed attempts.		
Depending on requirements and security accountability for some application specific print tasks, print auditing enabled.		
All events audited if dial-up networking/remote access service (RAS) is installed.		
Within Event Logs Settings, all audit logs set to *Do Not Overwrite Events*.		
Procedures followed as listed in Section 2.9.5, RAS Auditing, to determine the correct amount of disk space allocated for the audit file on all domain controllers and servers.		
Implementing Server TCP/IP Advanced Security (Section 2.10)		
Set minimum port requirements for a Windows NT Server, acting as a PDC, BDC, or a WINS Server, and nothing else, as listed below. Note: This configuration does not include additional ports that may be required to support other applications using the TCP/IP stack, such as Oracle SQL*Net.		
TCP PORT 137 - Network Basic Input-Output System (NetBIOS) Name Service		
TCP PORT 138 - NetBIOS Datagram Service		
TCP PORT 139 - NetBIOS Session Service		
UDP Port 137 - NetBIOS Name Service		
UDP Port 138 - NetBIOS Datagram Service		
UDP Port 139 - NetBIOS Session Service		
IP Protocol Port 1		

	YES	NO
Additional port requirements needed if domain name service (DNS) or dynamic host configuration protocol (DHCP) will be used include:		
TCP Port 53 - Domain Name Service		
TCP Port 67 - DHCP/Bootstrap Protocol (BOOTP) Server		
TCP Port 68 - DHCP/BOOTP Server		
UDP Port 53 - Domain Name Service		
UDP Port 67 - DHCP/BOOTP Server		
UDP Port 68 - DHCP/BOOTP Server		
Set minimum port requirements for a Windows NT Server configured to be an Exchange Server, and not a PDC or BDC, as listed below.		
UDP Port 138 - NetBIOS Datagram Service		
UDP Port 139 - NetBIOS Session Service		
TCP Port 25 - Simple Mail Transport Protocol (SMTP) [For use with the Exchange Internet Connector]		
TCP Port 102 - ISO - Transport Service Access Point (TSAP) [For use with the Exchange x.400 connector]		
IP Protocol 1		
Recycle Bin (Section 2.11)		
Recycle Bin properties modified to immediately delete files.		
Assigning File, Directory, and Registry Permissions (Section 2.12)		
Everyone group removed from the local ACLs of newly created subdirectories.		
No users outside systems staff assigned to “Full Control” permission, the “Special Access” permissions “Change” permissions, or “Take Ownership” permissions for any file/directory objects.		
Before installing Windows NT, document information protection goals for the entire post of office.		
Groups and folders (directories) are related to specific functional requirements.		
The ACL for Group Folders only includes the group that owns the folders.		
Users and Groups are not granted “Full Control” access to folders.		
Set directory permissions as displayed in Figure 2.12.5-1 of this document.		
Disabled POSIX subsystem by deleting the following files from \WINNT\SYSTEM32: psxss.exe; posix.exe; and psxdll.dll.		
If not running the Microsoft Multitasking MTA, disabled the OS/2 subsystem by deleting the files os2ss.exe, os2.exe, and os2srv.exe from \WINNT\SYSTEM32.		
Protecting Application Files (Section 2.14)		
Permissions set on applications installed in the manner described below.		
When possible, store applications on the server. Server-based storage		

	YES	NO
of executable code will ensure the integrity of the application software, while facilitating upgrades and access control.		
Permissions on applications directories (e.g., “\Program Files\MsOffice”) may be set as follows: Administrators: Full Control (All)(All) Users: Read Access (RX)(RX) SYSTEM: Full Control (All)(All)		
When establishing permissions for locally defined groups, system administrators must ensure that groups are assigned only those permissions required to perform their assigned duties.		
Directory Replicator Service (Section 2.15)		
Directory Replicator Service activated only by system administrators who fully understand its configuration.		
Established unique user account for Directory Replicator Service and audited.		
Configuring Printers (Section 2.16)		
Users restricted to printers within their functional areas.		
Only authorized system staff granted Full control over any dedicated or shared printers.		
Assigned user to Print Operators group in NT Server and modified ACL of particular printer object to allow that group Manage Printers permission (at systems administrators discretion).		
✿ **Remote Access/Dial-up Networking (Section 2.17)**		
RAS use restricted to specific Department asset use, to connect with strictly configured internal servers, and use currently approved encryption technologies.		
Password-Protected Screen Saver (Section 2.18)		
Password-protected screen savers on servers are to be removed. System administrators are to log off the system whenever they leave the work area.		
Service Pack 3 (Section 2.19)		
Enable Server Message Block signing via the Registry.		
Disable the Anonymous user group.		
Select the machine-generated random key as the system key.		
SERVER ADMINISTRATION (Section 3.0)		
Log on/Log Off (Section 3.1)		
The Secure Attention Sequence (SAS) used to initiating both log and log off of Windows NT systems.		
Emergency Repair Disk (Section 3.2)		
Only authorized system staff created ERDs.		
All ERDs handled as system backup material and stored in a secure		

	YES	NO
location.		
Last Known Good Configuration (Section 3.3)		
Cycled through a second system book after making key changes to security settings on users or groups.		
Log On Credentials from Domain Server (Section 3.4)		
Deleted any cached profiles of disabled accounts on local workstations (and servers, if the cached profile belonged to an administrator) to prevent unauthorized entry.		
Add-ins for Windows NT Components (Section 3.6)		
Educate end users regarding good computer security practices.		
Backups (Server 3.7)		
Implemented and documented full backup and recovery procedure for system programs and information to ensure continuity of operations.		
Backup tapes stored securely.		
Audit logs reviewed regularly.		
Backup plan created using recommendations listed in Section 3.7		
Windows NT Schedule Service and AT Command used to automate backups.		
Backups of critical data run on daily basis.		

INDEX

A

Access Control Entry .... *See ACE*
Access Control List .... *See ACL*
ACE 3, *48*, *50*, *1*
ACL *3*, *20*, *46*, *49*, *50*, *57*, *59*, 63, *64*, *70*, 73, *1*
ARCserve 66

B

Backup Domain Controller .... *See BDC*
Basic Input-Output System .... *See BIOS*
BDC 9, 10, 44, 45, 63, 65, 1
BIOS *6*, *7*, 44, *1*

C

C2 .... 1, 3, 46, 64, 69, 70, 71, 72, 73
  Configuration Utility 64
  Level 69, 70
  Rating 1
CMOS.RAM 50
Crystal Reports 41

D

Default Computer 24, 27, 28, 29
Default User 19, 23, 25
DOS 5, 24, 62, 72, 1
drwtsn32.log 50
Dual-Boot 5

E

Emergency Repair Disk .... *See ERD*
ERD 19, 34, 62, 1
Explorer 3, 31, 35, 49

F

FAT 5, 34, 1
File Allocation Table .... *See FAT*

G

Guest 19, 21, 71, 73

H

Hardware Compatibility 5

Hardware Compatibility List........8
High-Performance File System........*See HPFS*
HPFS........5, 1

I

INI files........50

K

Kane Security Analyst........*See KSA*
KSA........*64*, *69*, *70*, *71*, *1*

L

Local Security Authority........*See LSA*
LSA........*2*, *1*

N

National Computer Security Center........*See NCSC*
National Security Agency........*See NSA*
NCSC........1, 3, 72, 1
NetBIOS........44, 45, 1
Network Basic Input-Output System........*See NetBIOS*
NSA........59, 1
NT Backup........66
NT File System........*See NTFS*
NTCONFIG.POL........29
NTFS........5, 18, 20, 21, 34, 35, 46, 47, 48, 49, 57, 72, 1
NTFSDOS.EXE........5, 6

O

Oracle........45, 66
OS/2........5, 72, 1

P

PDC........*9*, *10*, *25*, *29*, *44*, *45*, *63*, *65*, *1*

R

RAS........27, 37, 59, 71, 1
Recycle Bin........46
REGEDT32.EXE........36, 37
Registry........24, 26, 28, 31, 37, 38, 46, 62, 64, 65, 66, 69, 71, 72
  Key Auditing........36
  Rights........70
  Security........73
Registry Editor........4, 34, 38

Remote Access Service..*See RAS*

S

SAM...*2*
Security Account Manager...*See SAM*
Security Identification...*See SID*
Security Reference Monitor..*See SRM*
Server Manager...3, 29
Service Pack..3
SID..9, 2
Somarsoft DumpAcl...64, 72
SRM...*2*, *3*, *2*
System Policy Editor..3, 23, 29

T

TCP/IP..44, 45
Third Party...41, 64, 69

U

UDP...44, 45, 2

W

Windows 95...24, 46

Y

Year 2000..6, 7