Operating System Security

Table Of Contents

1.1 **Policy Statement**

The Operating Systems must be secured in order to restrict access to critical business data, programs, utilities, system level security tables etc., to only those individuals who require the access to perform functions related to their job.

1.2 Scope

This document addresses Policies and Procedures related to the security of Operating systems This policy and the associated procedures apply to the entire staff and any persons using the Operating System resources of the Company.

1.3 Execution Responsibility

The Administrator-Systems along with Administrator-Network is responsible for implementing and executing the procedures mentioned in this document. The execution of the procedures will be monitored by Head-Infrastructure. CISO and Internal Auditor shall perform periodical reviews to ensure that the Operating Systems are in compliance with the associated policies and procedures

1.4 Detailed Procedures

1.4.1 Operating System Installation

- Review of System Security Controls:

Security features of the OS must be reviewed by Administrator-Systems, along with CISO, prior to system installation.

- Identification, Documentation, and Testing of Security Features:

All security features must be identified, documented and tested by Administrator-Systems prior to use.

- Familiarity with System Security Controls:

Prior to implementation, the Administrator-Systems and CISO must be adequately trained to understand security. Access to systems should not be allowed until security administration functions are in place.

1.4.2 Operating System Access Control

- Restrictions on Access to Advanced Programs and Utilities:

Administrator-Systems should restrict access to programs or utilities that can dynamically alter data (e.g., programs that circumvent the standard access, through an application program, to data files) to those people who demonstrate a business need. The Administrator-Systems should notify the Head-Infrastructure & CTO of such activities

- Restrictions on Access to OS Commands:

The direct access to OS Commands and through sensitive utilities accessing operating system commands should be restricted to those individuals who require this access to perform their job functions.

- Documentation of Essential Programs and Data Files:

Administrator-Systems is responsible for maintaining a record of essential programs and data files. He should also control changes to these files.

- Automatic Time-out of On-line Terminals:

Where technically feasible, and after review with CISO & Head-Infrastructure, the systems should be configured to time-out on-line terminals after three minutes of inactivity.

1.4.3 Privilege Management

- Privileges to be associated with system products:

The privileges associated with each system product (e.g. for each operating system) should be identified, as well as the categories of staff to which they need to be allocated.

- Allocation of privileges based on "Need to Use":

Privileges should be allocated to individuals on a "need-to-use" basis and on an "event-by-event" basis (i.e. the minimum requirement for their functional role only when needed).

- Authorisation process maintenance:

An authorisation process should be followed and a record of all privileges allocated should be made. Privileges should not be granted until the authorisation process is complete. (Refer Annexure 8A of Logical Access Security Chapter).

- Automation of privilege assignment:

Wherever possible, system routines should be developed and used to avoid the need to grant privileges to users. This should be achieved by using menu driven utilities.

- Requirement for special user identification:

Users assigned high privileges for special purposes should use a different user identity for normal business use (e.g. "administrator" or "root" login should not be used to carry out normal activities).

1.5 Windows NT Security

Following are the security procedures related to Windows NT, the operating system deployed in Company network.

1.5.1 Domain Account Policies

1.5.1.1 User Account records

All standard user accounts must only be entered on the authentication domain. Every user must authenticate to the authentication domain, which serves that user's server. User accounts must not exist on any Resource Domain systems or on any user workstations, except the required renamed administrator and disabled guest account.

1.5.1.2 User Account Security

In the Accounts policy ensure enabling of:

- 'Forcibly disconnect remote users' from server when logon hours expire and 'User must log on in order to change password'.
- Use Passfilt.dll from SP2 (Service Pack 2) to enforce strong passwords from Domain User Accounts.

1.5.1.3 User Rights Policy

The basic user rights available on the system must be granted with care while defining user accounts as they override object permissions for accessing network resources.

- Basic user rights should not be assigned to the "Everyone" group. Ensure the "Everyone" group is also removed in the NTFS Permissions Access Control Lists.
- The following default rights are granted to "Administrators", "Backup Operators" and / or "Server Operators" groups. These must be segregated, assigned and monitored to ensure adequate security.
    - Back Up Files and Directories

  - Restore Files and Directories
  - Change the System Time
  - ‘Log On Locally’ right must only be assigned to users who are allowed to login at the Domain Controller server.
  - ‘Shut Down the System’ right must not be granted to Everyone, Guests and Users on the Domain Controllers
- By default these rights are given to the “Administrators” group and must be maintained.
  - Manage Auditing and Security Log
  - Take Ownership of files or other Objects
- ‘Log On as a Service’ right by default is granted to ‘Administrators’ and ‘backup operators’ and must be carefully administered.
- User rights must be assigned to groups only. They must not be assigned to individual user accounts.
- If systems are using Internet Information Server for anonymous web or FTP access, the anonymous account has to be granted “Log On Locally” privileges. If this anonymous access is being granted, Internet Information Server should not be installed on a Domain Controller.
- Service accounts created with additional user rights must not be prefixed with obvious identifier indicating that it is a privileged service account.

1.5.2 Built In Accounts

1.5.2.1 Guest Account

Guest accounts must be disabled. It must never be created. If such accounts need to be created, they must be set to expire immediately following the completion of their use. The Guest account must be renamed and given a password.

1.5.2.2 Administrator Account

- The Administrator account must be renamed to a unique name that is hard to guess.
- The set of administrator IDs must have a backup and be closely controlled for each of the administrator and operator group rights.

1.5.2.3 Privileged Accounts as Emergency account

An additional privileged user account must be created, to be used as an emergency account, in addition to the default privileged administrator account. This new account must be treated as an emergency user ID to be used in an emergency situation. When the Windows NT system has to be accessed as a privileged user and the default privileged administrator account’s password does not give an access to the system, this emergency account ID must be used. The Administrator-Systems must put password of the emergency user in an envelope and hand it over to the Head-Infrastructure, which must be maintained in a fire proof cabinet.

1.5.3 User Accounts Properties

1.5.3.1 User Profile

Mandatory profiles must be used for Guest Accounts, if created, as the user cannot permanently change these profiles.

1.5.3.2 Home Directory

Home directories must be secured with NTFS permissions for access only by the owner of the directory and Administrator-Systems, for administrative purposes only.

1.5.3.3 Login scripts

A login script must be defined for all the users, especially for MS_DOS workstations, as User Profiles cannot be created for them. Login scripts must be stored on an NTFS partition for security. Login Scripts must exist on all servers in the domain using replicator service to maintain identical updated copies of a directory tree on multiple computers. The login script must contain at least a Legal Notice, which will be displayed when the user logs in to the Windows NT server.

1.5.3.4 Logon Process

- On the Windows NT Servers and NT Workstations, the interactive logon process must begin with a Welcome box. The welcome box requests the user to press CTRL+ALT+DEL keys simultaneously, to provide strong defence against any application running background, such as a Trojan horse.
- A LEGAL Caption with a legal notice must be next. The user must acknowledge the notice by selecting the OK button in the message box presented.
- The Windows NT 'standard logon dialog' box must be next in the process. The standard logon dialog requests for user name, password and the server or domain the user wishes to access. In case of wrong user name or password, the system must return 'User authorisation failure' but does not disclose if password or user name has caused the failure.
- On Window 95/98 clients, a legal caption and the standard logon dialog box must be used.

1.5.4 Groups

1.5.4.1 Creating user-groups

- Users must be grouped according to departments or functions to ease administrative burdens and organise security more effectively.
- Global groups and Local groups must use identification that is not obvious.
- The duties must be segregated in a manner that the administrator privileges are not required by the support team members, if any.
- All groups must be reviewed, with the owner of the group to ensure that membership is current and active, at least twice a year. Use the USRSTAT.EXE utility from the NT Server Resource Kit.
- New global groups must have an owner account that is identified in the description field of the group. Owners of the groups must review the group membership on a semi-annual basis. Use the USRSTAT.EXE utility from the NT Server Resource Kit.

1.5.4.2 Everyone Group

The Everyone group includes everyone who accesses a computer, including local and network users. This is a default group having the following permissions, which is a security risk.

- Full Control when you create or share a folder
- Change permissions on the Root directories of all Windows NTFS volumes

- Change permissions in the System32 directory
- Change permissions in the Win32App directory

The Everyone Group must not be granted access to the above-mentioned activities.

1.5.5 Domain Administration

1.5.5.1 Domain Structure

The following must be ensured on domain structures:

- To provide disaster recovery for the Authentication domain, at least one BDC must be at a different site than the PDC
- Bandwidth Considerations, Synchronisation Over Wide area network (WAN) and Remote access (RAS) links, use of the Replication Governor must be considered while planning domains and trust relationships

1.5.5.2 Trust relationships

Each Resource domain must trust at least one Authentication Domain. All resource domain trust relationships must be set, wherever possible, as one-way trusts.

1.5.5.3 Synchronising Servers

Security databases between domain controllers must be synchronised to ensure that there are no problems relating to password mismatches and access tokens created without the necessary group memberships.

1.5.6 Directory and File Security

1.5.6.1 Partition Programming

All the Server partitions of Windows NT systems must be created as NTFS (NT File System) instead of the FAT (File Allocation Table) file system.

1.5.6.2 Secure File Sharing

- Proper security must be applied via NTFS and not via the file sharing service as shares on NTFS enforce the security on the underlying directory it maps.
- The administrative shares ($ shares) must be deleted if they are not needed on an installation. Use the “net share” command for the same.
- Each user must be assigned a private share directory on a member server (Non domain controller). The name for the share must be the User ID and appended with ‘$’ to ensure that share is hidden from the browse list.
- Permissions for the share must be set as follows:
    - Everyone group - remove default entry
    - User ID - Full control
    - Shared Local Access (LA)/ Other group (OG) - Full control
- For users that require higher levels of security the ‘shared LA/ OG’ full control permissions must be removed.
- Directory permissions must match the share permissions for user personal shares.
- For files in the application directories, permissions to the Users local group, or Domain Users Global group, must not allow Write, Delete or Full Control access but allow only list access.
- By default executable, batch and DLL files are in separate directories from data files. These files do not allow Write, Delete or Full control access to any created

end-user groups. This helps to prevent the spread of viruses. If this is not possible due to the design of some applications, a quality virus scanner must be employed and updated regularly.

- The developer local and global groups must never have Write, Delete, or Full Control access to any files, directories or shares on a production server.

1.5.6.3 Root directory file permission

- The root directory of the system partition of the Windows NT server includes several files that must be protected from users who might have permissions that allow them to delete or alter the files. These are system files that are loaded when NT server is installed.
- Full control permissions to the C:\boot.ini, C:\ntdetect.com and C:\ntldr files must be assigned to no one other than the administrators and system.

1.5.6.4 Operating System files and directories

The Windows NT operating system directories must have the following permissions to all the groups as mentioned below.

Directory	Groups	Permissions
%systemroot%\	Administrators	Full Control
	Server Operators	Change
	Domain Users	Change
	Creator Owner	Full Control
	System	Full Control
%systemroot%\system32	Administrators	Full Control
	Server Operators	Change
	Domain Users	Change
	Creator Owner	Full Control
	System	Full Control
%systemroot%\system32\config	Administrators	Full Control
	Domain Users	List
	Creator Owner	Full Control
	System	Full Control
%systemroot%\system32\drivers	Administrators	Full Control
	Server Operators	Full Control
	Domain Users	Read
	Creator Owner	Full Control
	System	Full Control
%systemroot%\system32\spool	Administrators	Full Control
	Server Operators	Full Control
	Print Operators	Full Control
	Domain Users	Read
	Creator Owner	Full Control
	System	Full Control
%systemroot%\system32\repl	Administrators	Full Control
	Server Operators	Full Control
	Domain Users	Read
	Creator Owner	Full Control
	System	Full Control

Directory	Groups	Permissions
%systemroot%\repl\repl\ import	Administrators	Full Control
	Server Operators	Change
	Domain Users	Read
	Creator Owner	Full Control
	Replicator	Change
	Network	No Access
	System	Full Control
%systemroot%\system32\repl\export	Administrators	Full Control
	Server Operators	Change
	Creator Owner	Full Control
	Replicator	Read
	System	Full Control

regedit, regedt32 and poledit are programs that allow to make changes to the Windows NT registry. The “Everyone” group and “Domain User” group must have “No Access” permissions to these programs.

1.5.6.5 Application Files and Directories

- Ensure that all the users of the application must be given “Read” permission to the application program directories and files
- “Full control” permissions must be given to “Administrators” group or the application’s privileged user to the application programs.

1.5.6.6 Event Logging and Review

- The Audit Policy under User Management must be enabled to audit all failed events viz. Audit Successful Logon and Logoff, User and Group Management, Restart, Shutdown and System events, and Security Policy Changes.
- The security messages from the Log menu (Event viewer/administrative tools) must be reviewed and reasoned for any suspect. Specifically Event 534: Unsuccessful Logon and Logoff attempts.
- For very critical non-domain controllers, e.g., file and print server, email server, application server, database server, the Windows NT server system must be set to fail on Audit Failure, this is activated in the Registry under:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SeCEdit\RegValues\MACHINE/System/CurrentControlSet/Control/Lsa/CrashOnAuditFail
  - Set the above value to (1) or change this value using C2 Configuration Manager supplied by the NT Resource Kit.

1.5.6.7 Secure Event Log Viewing

Default configuration allows guests and null logons ability to view event logs (system, and application logs). Security log is protected from guest access by default. It is viewable by users who have “Manage Audit Logs” user right. The Event log services use the following key to restrict guest access to these logs:

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\EventLog\[LogName]
Type REG_DWORD

Set the value for each of the logs to 1. The change takes effect on next reboot. Ensure change of the security on this key to disallow everyone other than Administrators and System any access because otherwise malicious users can reset these values.

1.5.7 Registry Hardening

1.5.7.1 Remote Access to the Registry

No users must have the ability to remotely access the Registry including Administrators. The presence of the winreg subkey in the Registry with the associated ACL determines which users can connect to the Registry remotely. Absence of the winreg subkey allows all users to connect to the Registry remotely. To restrict network access to the registry, use the Registry Editor to create the following registry key:

Hive:	HKEY_LOCAL_MACHINE\system
Key:	\CurrentcontrolSet\Control\SecurePipeServers
Name:	\winreg

1.5.7.2 Restricted Browse list

Sensitive servers and Workstations must be hidden from the browse list by modifying the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Add a value enabling ‘Hidden’.A much easier way to accomplish this setting is at a command prompt with the following command : **net config server /hidden:yes**

1.5.7.3 Strong passwords

On Domain Controllers the PASSFILT.DLL must be installed to enforce the use of strong passwords for all user accounts. This entry will be found in the:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\Notificationpackages registry key.

1.5.7.4 SYSKEY

The SYSKEY features in Windows NT service pack 3 must be utilised to ensure that the password hashes for Windows NT are secured from attempts to dump the hashes. The syskey utility modifies the method that Windows NT uses to store the passwords in the registry. Syskey Permits Strong Encryption of the SAM database.

1.5.7.5 Registry viewing

Default allowed path registry entries are limited to prevent unauthorised viewing of registry data. The default allowed paths registry key allows sensitive sections of the registry to be monitored regardless of registry permissions. The allowed paths registry key must be monitored and can be found under the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg registry key.

1.5.7.6 Automatic logon

Use of the AutoadminLogon Registry value must be prohibited in the environment. This is prohibited, as this key will embed the password in clear text in the registry and bypass default Windows NT authentication process. Set the AutoadminLogon registry value to ‘0’ in the following registry key.

> HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon registry key.

1.5.7.7 Schedule Service

The “at” program allows users to schedule their program to be executed at their desired time and date. This command bypasses the Windows NT’s security and executes the scheduled commands. Restrict user’s ability to submit jobs to the scheduler. Ensure the value of REG_DWORD is ‘0’ to limit job submission to administrator level users only in the following registry key

> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\SubmitControl.

1.5.7.8 Administrative full control

The permissions to the following registry key must be modified to grant full control to only the administrator group. This is accomplished by modifying the permissions for the:

> HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Schedule

1.5.7.9 Hide the Last User Name

The Windows NT Registry must be modified so that the User Name is hidden in each subsequent log on. An unknown user ID and an unknown password make it much more difficult for a would-be intruder to gain access. Use the Registry Editor to create or assign the following registry key value:

> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\Curren t Version\Winlogon of Type:REG_SZ ensure Value:1

1.5.7.10 Shutdown

For Windows NT Workstation it is necessary to Restrict system shutdown to logged on users only, use the Registry Editor to create or assign key value as "Restrict System Shutdown." (Windows NT Server on a dedicated server defaults to restrict system shutdown to only logged-on users.)

1.5.8 Backup and Recovery

- An Emergency Repair Disk (ERD) for recovery must be created during the setup process of Windows NT. Physical protection of the Emergency Repair Disk is crucial.
- File and directory permissions on the \WINNT\REPAIR directory must be modified to remove the default permissions that grant everyone the ability to read the repair information contained in this directory.
- Emergency repair disk procedures must require the use of the ‘/s’ option to update the security information when the repair disk is created.
- Periodic updating of the emergency repair disks for all servers in the enterprise must be ensured.

1.5.8.1 Last Known Good Configuration

- In the event of a system malfunction that results from changes to the configuration, the first recovery attempt must be to invoke the previous start-up configuration, called the Last Known Good Configuration.

- If the Last Known Configuration fails to recover the system, it is necessary to use an Emergency Repair Diskette. The Repair disks must be kept current to ensure that the SAM file data is not lost.

1.5.9 Auditing

Auditing must be enabled through start →Administrative tools → User manager for Domains → Policies →Audit Policy. The following must be audited, at a minimum: Audit failed log on attempts, attempts to access sensitive data, and changes to security settings. The established audit policy must be weighed to the cost (in disk space and CPU cycles) of the various auditing options against the advantages of these options.

1.5.9.1 Domain and Workstation Auditing

- For Domains, auditing in the Security Event Log must be enabled on Resource Domains, as well as Authentication Domains.
- For Workstations, in the USER MANAGER utility under the Audit Policy menu item, auditing in the Data Security Event Log must be set.
- The following settings must be enabled for domain and workstation auditing:

Restart, Shutdown and System	Success and Failure
Logon and Log off	Success and Failure
File/Object Access	Failure
Use of User Rights	Failure
Security Policy Changes	Success and Failure
User/Group Management	Success and Failure
Process Tracking	No events are to be captured (could be enabled if your Windows NT system is not functioning properly)

- Audit logs must be archived regularly to track trends. This is useful for determining resource utilisation for planning purposes, and to track unusual activity on the network.
- Allocate diskette and CD-ROM drives at logon. Use the Registry Editor to ensure that only the user currently logged on locally to the Server or workstation can access diskettes and CDs.
- All servers must have the log size set to a minimum of 20 MB in the Event viewer application. Set the audit log to crash on failure, so that an intruder cannot cover their tracks with spoofed events. The Logevent.exe utility from the resource kit can be used to test this.
- Set security log behaviour. Choose “Do Not Overwrite Events” using the Event Viewer as described in the Windows NT Workstation or Windows NT Server System Guide. Optionally, you can also force Windows NT to stop when it cannot generate an audit event, or enable the system to audit the use of all rights. To do this, use the Registry Editor to create or assign the Registry key
- Audit the Everyone group instead of, or in addition to, the Users group. This will ensure that anyone who can connect to the network is audited, not just the users you create accounts for in the domain.
- Set up a schedule for viewing audit logs and ensure it becomes a regular part of administration tasks.

1.5.9.2 Action against specific threats

In order to combat specific threats ensure auditing of following events

- For threat of Hacker-type break-in using random passwords, enable failure auditing for log on and log off events.
- For threat of break-in using stolen password, enable success auditing for log on and log off events. The log entries will not distinguish between the real users and the phoney ones, but unusual activity on user accounts, such as logons at odd hours or on odd days can be traced.
- For misuse of administrative privileges by authorised users, enable success auditing for use of user rights; for user and group management, for security policy changes; and for restart, shutdown, and system events.
- For improper access to sensitive files, enable success and failure auditing for file and object access events, and then use File Manager to enable success and failures auditing of read and write access by suspect users or groups for sensitive files.
- For improper access to printers, enable success and failure auditing for file and object access events, and then use Print Manager to enable success and failure auditing of print access by suspect users or groups for the printers.

1.5.10 Network Integrity and Security Planning.

1.5.10.1 Use of NetBIOS

This protocol allows the use of the command NBTSTAT, which provides the domain name and computer name of a given IP address and the names of users logged in to it. This command gives an unauthorised user a lot of useful information that could be used to further an attack on a Windows NT system. This is a target for hackers trying to break in to the network. Also, its use causes more broadcast traffic than other protocols. NetBIOS must be disabled.

1.5.10.2 Use of SCOPY

Files copied between directories inherit the permissions of the directories into which they are moved. This introduces the risk that security of sensitive files is compromised when they are copied to another directory. The Windows NT Resource Kit provides the SCOPY command, which must be used to copy files and directories to and from Windows NTFS partitions. Files and directories copied using the SCOPY command retain the permissions and ownership of those objects.

1.5.10.3 Dual-Boot Systems

Dual-boot systems must not be created for Windows NT servers as they pose several security risks. An intruder who gains physical access to the server may boot from the other partition and use it to launch programs against the Windows NT disk partition. Additionally, the non-Windows partition on the disk might become infected with a virus that corrupts the Windows NT partition of the disk.

1.5.10.4 TCP/IP security

- The Windows NT server by default has all the TCP/IP ports enabled. Hence users may attempt to gain unauthorised access to these ports to gain access to the system. The Administrator-Systems must configure TCP/IP security within Windows NT to “Permit Only” those ports that serve a business purpose.

- The following NetBIOS ports must be blocked (135, 137, 139) as these can be used for Denial of Service attacks. If NetBIOS has been unbounded from TCP/IP, then these ports don’t have to be blocked.
- Windows NT, in order to function properly will require other ports for several applications to be listed. Port filtering and blocking must really be handled at the firewall or a software based port filter.

1.5.10.5 Remote Access Service

Remote Access Service must be disabled from all the Windows NT server and enabled only for the servers allowing Remote Access.

1.6 UNIX Security

1.6.1 Access to the Shell Prompt

- End-users must not be allowed access to the shell prompt unless deemed necessary. System Users requiring access to the shell prompt must specify the same on the access request form. This must be approved by the Head-Infrastructure.
- Once verified by the operating system, users must automatically be directed to applications for which they have been authorised. When the application users exit from the application program, they must be logged out of the UNIX system. This may be done by placing an “exit” command at the end of the users’ .profile file.

1.6.2 File and Directory Permissions

1.6.2.1 Access to Powerful Programs and Utilities

File permissions to system commands / utilities e.g., cron, at, finger, rwho, traceroot, netstat, sysstat, etc. must be set to 700 (i.e., no permissions for the group and the world).

1.6.2.2 Ownership and permissions for Application Programs

The ownership of application program files and write permission must only be given to the application’s privileged user or the operating system’s privileged user.

1.6.2.3 Permission to Operating System Files and Directories

Ownership of important files and directories of the operating system (e.g., files in /etc, /bin, /dev directories) should be with the root user and file permission bits to these file and directories should be set to 700 (i.e., deny complete access to the group and the world).

1.6.2.4 Home Directory Permissions

Each UNIX user must be the owner of his / her home directory. Permission bits for these directories must be set to 700. The owner must change file permissions only when necessary to permit group members to view his / her files.

1.6.2.5 Umask value

The umask value should be set to 077 to ensure that all files created will by default have no read-write permissions for the group and the world. Thereafter, the permission bits can be set for respective files / directories as necessary. The umask value can be set in /etc/default/login.

1.6.2.6 SUID, SGID and Sticky Bits

SUID and SGID bits must not be set on executable programs as they can grant access to files that a user with normal access rights may not be able to access. There must be no SUID or SGID shell scripts. The sticky bit must be set where group writeable directories are used or where live data is stored, in order to protect these directories / files from being deleted or accidentally being renamed by another user.

1.6.2.7 Start-up and Configuration Files

System start-up scripts and configuration files (e.g., /etc/inittab, etc.) must be write-protected to prevent write access to the group and the world. All unnecessary inetd services must be commented out of the inetd file to disable high exposure to functions such as finger and ftp. The ownership of user configuration files (e.g., .profile, .login and .cshrc) must be with the root user and the respective users must not be able to change the contents of these files.

1.6.2.8 Access Control Lists

Wherever Access Control Lists are used, access to these lists must be restricted to the Administrator-Systems. Internal Auditors must be given only read access to these lists when necessary.

1.6.3 Prohibition Against Trap Doors / Shell Escapes To circumvent Access Controls

Programmers and other technically oriented staff must refrain from circumventing the authorised access control mechanisms through trap doors found in operating systems and/or access control packages.

1.6.4 Root Privileges

- Root privileges must be given only to the primary Administrator-Systems.
- The Administrator-Systems must never run another user's program as root. He / she must use su and switch over to his/her user-id.
- The Administrator-Systems must use /bin/su rather than just su, to avoid Trojan horses and to minimise path searches for the root account.
- Logs of root password usage must be reviewed within 24 hours.

1.6.5 Root Login Limitations

The root user must not be allowed to do a telnet. The Administrator-Systems must use his regular user account to login through telnet and then use a “su” command to switch to the root account.

1.6.6 Use of Shadow Password File

The shadow password feature must be enabled. The ownership of the shadow password file must be with the root user and file permissions must be set to 700 to ensure that the group and the world does not have read or write access.

1.6.7 User Groups

General users must not have a Group ID of 0. User groups must be reviewed on a regular basis to ensure users are in correct groups with rights which are commensurate with their job responsibilities.

1.6.8 UNIX Networking

1.6.8.1 Network Information Services (NIS)

The following guidelines must be implemented to reduce the risk on account of NIS :

- When running NIS always use “+:*:0:0:::” instead of “+::0: 0:::” in the password file for NIS clients
- The servers must not have a + in the ID field (+:*: 0: 0:::)

1.6.8.2 Network File Systems

The Network File System (NFS) must not be enabled on any of the UNIX workstations. There must not be any entry in /etc/exports file. The entry for “nfsd” must also be commented out of the /etc/inetd.conf and /etc/services files.

Where the use of Network File System (NFS) cannot be avoided, the following guidelines must be followed:

- Files or directories must be exported in the read-only mode
- Executable programs on the server must be exported as read-only
- Only those machines which will be mounting NFS must be allowed to have access. This can be specified through the access = [machinelist] option in the /etc/exports file.
- Anonymous users must not be allowed to mount the NFS by setting anon= -1 in the /etc/exports file.
- The root = [machine-list] option must not be used, unless necessary, to prevent root access from the specified machines
- A separate file system must be created for NFS. The root directory or a user’s personal directory must not be defined as the NFS.
- When using NFS, unique Ids must be used across the network servers to prevent users from gaining access to files belonging to other users with the same user-id.

1.6.8.3 Use of Trusted Hosts

- There should not be any entry in the /etc/hosts.equiv file.
- The .rhosts and .netrc files must not be present in any user’s home directory. The Administrator-Systems must periodically scan user home directories to ensure that there are no unauthorised users of these files.

1.6.9 File Transfer Protocol

1.6.9.1 Use of Anonymous FTP

Anonymous FTP must be prohibited and disabled (by deleting the “ftp” user account).

1.6.9.2 Prohibiting certain users from using FTP

The /etc/ftpusers file must have entries for all system accounts such as root, adm, auth, bin, cron, daemon, lp, nobody, uucp, etc., and any other user accounts, who should not have permission to do ftp.

1.6.9.3 Using Trivial FTP

Trivial FTP (tftp) must not be used for doing file transfers to a UNIX machine, as it does not require user authentication. This must be disabled by putting # at the beginning of the line containing the ftpd entry in the /etc/inetd.conf and /etc/services file.

1.6.10 UNIX to UNIX Copy Program (UUCP)

The use of UUCP must be discouraged. Where the use of UUCP cannot be avoided, the following security provisions must be applied:

- Each user listed in the /usr/lib/uucp/L.sys file must have a separate login and password
- All UUCP control files must be owned by uucp and must be assigned access permissions that allow no access to general users.
- The commands listed in the /usr/lib/uucp/L.cmds file must be those that an outside UUCP user normally needs to execute to perform his / her tasks. The use of these commands must be approved by the Head-Infrastructure.
- UUCP access must be restricted to as small a number of files/directories as possible
- Directory exportation must not be permitted
- UUCP scripts must be owned by root/uucp to prevent modification by users using UUCP programs
- The following conditions must be met when setting up the /usr/lib/uucp/Permissions file :
  - LOGNAME, must specify a list of all hosts which are permitted to login
  - Remote hosts must only be permitted to read and write files from the default uucp public directory
  - The CALLBACK parameter must be set to “Yes”

1.6.11 UNIX System Monitoring

To detect unauthorized access or activity on a client or host server, logs must be maintained and a monitoring program must be implemented. Logs must be retained for a period of as decided by the CISO. Following are some of the tests to be included in this program:

- Check for dormant accounts and remove them
- Check for correct grouping of user IDs
- Review accounts added since the previous audit and check against authorisation sheets to ensure that no unauthorised accounts were added
- Check individual “last login” times in the last log for activity at suspicious times of the day
- Check the su log for switches to the root id from any user-ids not authorised to know the root password
- Review the acct log to find out who executed certain restricted commands from which terminal at what time and date.
- Review unusual login times
- An audit trail for all activities performed using the root ID should be generated. This should be logged to a printer or to a remote secure computer.
- Guidelines should be laid down for periodic monitoring of the activities within 24 hours.