



## Introduction

This document specifies the organisation's security standards for computers running Microsoft Windows NT Workstation. It is intended to provide instructions for securing new installations, but could be used as a guide for securing existing systems where required.

Where specific software tools are required to achieve certain of the recommendations (e.g. virus control), this document does not identify or describe those tools, since it is likely that they will change as time passes and the organisation discovers more appropriate methods of achieving the end result. Please refer to the appropriate documentation for the tool currently being used for each task.

**These standards and recommendations should be thoroughly tested before implementation on live systems.**



## Physical & environmental security

- Ensure that temperature and humidity controls are sufficient to comply with the manufacturers' recommendations
- For workstations handling sensitive data, position system keyboards and screens so they are not overlooked by windows or other vantage points

## Disabling unused hardware

- Remove or disable hardware devices (including serial and parallel ports, and unused removable media drives) that may be viewed as a security risk

## Securing the boot sequence

- Configure workstations to boot first from the hard disk, then from the diskette and/or CD-ROM

## NTFS file system

- Ensure that all fixed disk partitions are formatted with NTFS

## Removing unused subsystems

- After verifying that they are not required to run any essential application software, remove the OS/2 and POSIX subsystems by deleting the following strings from the registry:

<b>Hive</b>	HKEY_LOCAL_MACHINE
<b>Key</b>	System\CurrentControlSet\Control\Session Manager\Subsystems
<b>Value Name</b>	Optional
<b>Strings</b>	Os2, Posix

- Delete the following files from the \Winnt\System32 folder:

os2.exe  
os2srv.exe  
os2ss.exe  
pax.exe  
posix.exe  
psxdll.dll  
psxss.exe



## Restricting remote access to the registry

- Locate and select the following registry key using REGEDT32.EXE:

<b>Hive</b>	HKEY_LOCAL_MACHINE
<b>Key</b>	\System\CurrentControlSet\Control\SecurePipeServers
<b>Value Name</b>	\winreg

- Select Permissions from the Security menu
- Ensure that SYSTEM and Administrators are granted Full Control and that no other users or groups are listed

## Restricting anonymous access to Local Security Authority information

- Set the following registry value (if it does not exist, then create it):

<b>Hive</b>	HKEY_LOCAL_MACHINE
<b>Key</b>	System\CurrentControlSet\Control\LSA
<b>Value Name</b>	RestrictAnonymous
<b>Type</b>	REG_DWORD
<b>Value</b>	1

## Disabling LanMan authentication

- Set the following registry value (if it does not exist, then create it):

<b>Hive</b>	HKEY_LOCAL_MACHINE
<b>Key</b>	System\CurrentControlSet\Control\LSA
<b>Value Name</b>	LMCompatibilityLevel
<b>Type</b>	REG_DWORD
<b>Value</b>	2

## Disabling cached logon information

- Set the following registry value (if it does not exist, then create it):

<b>Hive</b>	HKEY_LOCAL_MACHINE
<b>Key</b>	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
<b>Value Name</b>	CachedLogonsCount
<b>Type</b>	REG_SZ



Value	0
-------	---

## Disabling the display of last logged on username

- This is often done through System Policy in which case it is not needed in this document
- Set the following registry value (if it does not exist, then create it):

Hive	HKEY_LOCAL_MACHINE
Key	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name	DontDisplayLastUsername
Type	REG_SZ
Value	1

## Configuring a logon warning banner

- This is often done through System Policy in which case it is not needed in this document
- Set the following registry values (if they do not exist, then create them):

Hive	HKEY_LOCAL_MACHINE
Key	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name	LegalNoticeCaption
Type	REG_SZ
Value	<Standard organisation warning message header>

Hive	HKEY_LOCAL_MACHINE
Key	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name	LegalNoticeText
Type	REG_SZ
Value	<Standard organisation warning message text>

## Securing the registry

- Change the permissions for the *Everyone* group for the following registry entries to **Read**:

Key path	Prevents users from
\SOFTWARE	Installing software
\SOFTWARE\Microsoft\RPC	Gaining access to RPC configuration information



\\SOFTWARE\\Microsoft\\WindowsNT\\CurrentVersion	Gaining Windows NT version information
\\SOFTWARE\\Microsoft\\WindowsNT\\CurrentVersion\\Perflib	Using the Performance Monitor to view the performance of the computer
\\SYSTEM\\CurrentControlSet\\Services\\LanmanServer\\Shares	Changing share information
\\SYSTEM\\CurrentControlSet\\Services\\UPS	Accessing UPS configuration
HKEY_USERS\\.DEFAULT	Changing the default user setting
HKEY_CLASSES_ROOT and all sub keys	Changing file associations and OLE configurations

## Securing the file system

- Set file and directory ACLs as shown below:

Folder(s)	User/Group	Permissions
\\Winnt and all subfolders	Administrators: SYSTEM: CREATOR OWNER: Users:	Full Control Full Control Full Control Read
\\Winnt\\Repair	Administrators:	Full Control
\\Winnt\\System32\\config	Administrators: SYSTEM: CREATOR OWNER: Users:	Full Control Full Control Full Control List
\\Winnt\\System32\\spool	Administrators: SYSTEM: CREATOR OWNER: Users:	Full Control Full Control Full Control Read
\\Winnt\\Cookies \\Winnt\\Forms \\Winnt\\History \\Winnt\\Temporary Internet Files \\Winnt\\Profiles \\Winnt\\SendTo \\Winnt\\OcCache	Administrators: SYSTEM: CREATOR OWNER: Users:	Full Control Full Control Full Control Special Directory Access Read, Write & Execute Special File Access - None Specified
\\Temp	Administrators: SYSTEM: CREATOR OWNER: Users:	Full Control Full Control Full Control Special Directory Access Read, Write & Execute



		Special File Access - None Specified
C:\Boot.ini C:\Ntdetect.com C:\Ntldr	Administrators: SYSTEM: CREATOR OWNER:	Full Control Full Control Full Control
Root of all new partitions	Administrators:	Full Control Full Control

## Securing the Administrator account

- Rename the Administrator account to a non-obvious name, in line with your standard account naming conventions
- For each domain, define a 14-character complex (i.e. using a combination made up from any three of lower case, upper case, numeric and symbol characters) password and assign it to the original Administrator account on each workstation in the domain. The symbol characters should be chosen from the following table, since these have been proven uncrackable by L0phtCrack (the most popular password cracking utility for Windows NT/2000). Each character is accessed by pressing ALT plus the relevant three or four digit number on the numeric keypad

**Table of Uncrackable Alt-Characters**

1= Ⓢ	21= §	143= Å	172= ¼	192= ˆ	212= ƒ	232= ϕ	252= ƚ	177= ±	229= ã
2= Ⓣ	22= ¯	144= €	173= ¡	193= ˆ	213= ƒ	233= ϕ	253= *	178= *	230= æ
3= ♥	23= †	145= æ	174= «	194= ˆ	214= ƒ	234= ϕ	254= ■	181= μ	231= ç
4= ♦	24= †	146= €	175= »	195= †	215= †	235= ϕ	255= B	182= ¶	233= é
5= ♣	25= †	148= ö	176= ¶	196= -	216= †	236= ∞	127= □	183= ▪	241= ñ
6= ♠	26= +	153= Ö	177= ¶	197= †	217= †	237= ϕ	131= f	186= °	246= ö
7= ▪	27= †	154= Ü	178= ¶	198= †	218= ƒ	238= €	135= †	187= »	247= ÷
8= ■	28= ˆ	155= €	179=	199= †	219= ■	239= ƚ	149= ▪	188= ¼	
9= ○	29= ++	156= £	180= †	200= ˆ	220= ■	240= ≡	160= B	189= ½	
10= ◻	30= ▲	157= ¥	181= †	201= ƒ	221=	241= ±	161= i	191= ¿	
11= ◊	31= ▼	158= €	182= ¶	202= †	222=	242= ≥	162= €	196= Ä	
12= ♀	32= S	159= f	183= ¶	203= ¶	223= ■	243= ≤	163= £	197= Å	
13= ♪	127= Δ	164= ñ	184= ¶	204= †	224= ∞	244= [	164= x	198= €	
14= ♯	128= Ç	165= Ñ	185= ¶	205= =	225= B	245= J	165= ¥	199= Ç	
15= ♂	129= Ü	166= ¢	186= ¶	206= †	226= ƒ	246= ÷	166= !	201= É	
16= ▶	130= é	167= °	187= ¶	207= ±	227= π	247= ≈	167= §	209= Ñ	
17= ◀	132= ä	168= ¿	188= ¶	208= ˆ	228= Σ	248= °	170= ¢	214= Ö	
18= †	134= å	169= ˆ	189= ¶	209= ¶	229= σ	249= ▪	171= «	220= Ü	
19= !!	135= ç	170= ˆ	190= †	210= ¶	230= μ	250= ▪	172= ˆ	223= B	
20= ¶	142= Ä	171= ½	191= ˆ	211= ˆ	231= ˆ	251= √	176= °	228= ä	

- Record the password and store it in a physically secure location to which only the IT Security team have access



## Securing the Guest account

- Ensure the account is disabled
- Rename the account to a non-obvious name, in line with your standard account naming conventions
- Set a complex (i.e. using the same criteria as described above for the Administrator password) 14-character password on the account
- Restrict its Logon Hours to disallow logon at all times

## Securing user accounts

- Do not create user accounts on workstations (i.e. only in domains)

## Disabling unnecessary services

- Disable any services not required for the workstation to perform its role. In particular, consider whether the computer needs any Peer Web Services components and whether it should be running the Server service for file and print sharing.
- Do not install any applications or utility software on the workstation unless they are strictly required for the workstation to perform its role

## Configuring the Account Policy

- Set the following standard Account Policy:

Parameter	Setting
Maximum password Age	<b>60 days</b>
Minimum password Age	<b>14 days</b>
Minimum password length	<b>6 characters</b>
Password uniqueness	<b>8</b>
Account lockout after	<b>3 bad logon attempts</b>
Reset account after	<b>30 Minutes</b>
Lockout duration	<b>Forever</b> (until unlocked by Security Admin)
Forcibly disconnect remote users from server when logon hours expire	<b>No</b>
Users must logon in order to change password	<b>No</b>



## Configuring the User Rights Policy

- Make the following changes:

User Right	Groups assigned this right by default on workstation	Change for workstation
<b>Access this computer from the network</b> Allows a user to connect over the network to the computer	Administrators, Everyone and Power Users	Administrators, Backup Operators, Power Users
<b>Bypass traverse checking</b> Allows a user to change directories and travel through a directory tree, even if the user has no permissions for those directories	Everyone	<none>
<b>Log on locally</b> Allows a user to log on at the computer, from the computer's keyboard	Administrators, Backup Operators, Everyone, Guests, Power Users, and Users	Administrators, Backup Operators, Power Users, Users
<b>Shut down the system</b> Allows a user to shut down Windows NT	Administrators, Everyone, Guests, Power Users, and Backup Operators	Administrators, Backup Operators, Power Users

## Configuring the audit policy

- Day-to-day auditing is not recommended for workstations

## Configuring Event Log settings

- Configure the following log settings:

Log	Maximum Log Size	Event Log Wrapping
Application	512 KB	Overwrite Events as Needed
Security	512 KB	Overwrite Events as Needed
System	512 KB	Overwrite Events as Needed



## Protecting console access

- Configure the Logon Screen Saver to activate after 10 minutes of inactivity and to be password protected

## Creating & securing Emergency Boot Disks

- Create an Emergency Boot Disk for each class of machine where the disk configuration is identical and test that it can be used to boot the workstation
- Store the disks in an appropriate secure location, with access restricted to designated personnel
- Ensure that copies are held off-site in a fireproof safe

## Creating & securing Emergency Repair Disks

- Since it is usually more efficient to reinstall a “standard build” workstation from an image than it is to troubleshoot it (including using the Repair process), it is not recommended to create ERDs for workstations

## Securing Internet Explorer

- Ensure that the latest approved version of Internet Explorer is installed
- Ensure that the latest approved Service Pack and post-SP hotfixes are applied (see below)

## Installing anti-virus software and updates

- Ensure that the latest approved anti-virus product is installed and configured in line with organisation standards

## Installing the latest (approved) service pack

- Ensure that the latest approved Service Pack is installed
- “approved” means that a formal test process has been carried out to ensure compatibility with all relevant system software and applications, meaning that given configurations could require different service packs



### Installing the appropriate post-service pack security hotfixes

- Ensure that the latest approved post-SP hotfixes are applied as appropriate
- “approved” means that a formal test process has been carried out to ensure compatibility with all relevant system software and applications, meaning that given configurations could require different post-SP hotfixes



## References

The following sources were used as reference material in the production of this document:

- *Microsoft Security Tool Kit* (Microsoft Corporation)
- *Windows NT Security Checklist* (ISF)
- *Windows NT Security Guidelines* (NSA Research)
- *Windows NT Security Step by Step* (The SANS Institute)