Introduction

This document specifies the organisation's security standards for computers running Microsoft Windows 2000 Server. It is intended to provide instructions for securing both existing systems and new installations, and is organised in two sections: mandatory standards and recommended good practice.

Mandatory standards are those that must be applied in all cases. Recommended good practice consists of additional guidance from First Base Technologies that is offered for serious consideration in order to strengthen existing security measures.

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.

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

Mandatory standards

Physical & environmental security

- Locate servers in a secure room with access controlled by the administration team
- Change numeric access control codes every 90 days, whenever an authorised individual ceases to require access and whenever code compromise is suspected
- Ensure that uncontrolled access is not possible via suspended ceilings and raised floors
- Review server room access control lists every 6 months
- Place servers in secure racks and establish a procedure to ensure that keys are protected and yet easily available to appropriate authorised personnel. Ensure that backup keys are held off-site in a fireproof safe.
- Position system keyboards and screens so they are not overlooked by windows or other vantage points
- Ensure that servers are not left logged on when unattended, or where this is unavoidable (e.g. where a required application cannot be run as a service) that the console is secured using the ***Lock Computer*** feature
- Ensure that all servers are protected by a UPS and associated software that allows automatic clean shut down
- Ensure that temperature and humidity controls are sufficient to comply with the manufacturers' recommendations
- Ensure that sufficient fire extinguishers of an appropriate type are provided and that smoke alarms are fitted

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

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

- On mission-critical servers, disable the diskette drive and CD-ROM in the BIOS (there is a registry setting to disable them under Windows 2000, however this only disables them as network shares - they are still available to the local user and can still be used to boot the computer)

Installing Windows 2000

- Unless *absolutely unavoidable*, always perform a fresh install of Windows 2000 Server rather than upgrading from Windows NT 4. Upgrades do not modify certain previous security settings, so upgraded systems must have the default Windows 2000 settings applied. Refer to the Microsoft document "Default Access Control Settings in Windows 2000" on TechNet for details on the default Windows 2000 file system ACLs and how to make any necessary modifications.

NTFS file system

- Ensure that all fixed disk partitions are formatted with NTFS
- Existing FAT volumes can be converted to NTFS without loss of data using the CONVERT utility. However, conversions do not modify the previous security settings and must have the default Windows 2000 settings applied. Refer to the Microsoft document "Default Access Control Settings in Windows 2000" on TechNet for details on the default Windows 2000 file system ACLs and how to make any necessary modifications.
- Ensure that user data and application code are placed on separate NTFS partitions from operating system files to help ensure that users do not accidentally gain access to critical system files. In addition, if a user partition is entirely filled, the operating system and its paging file will be unaffected (Windows 2000 may crash if it runs out of available free drive space).

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)

Securing Internet Information Server (if appropriate)

- Ensure that IIS is required to be installed and remove it if not
- Where required, ensure that the latest approved version is installed

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

- Run the ***IIS Lockdown Wizard*** from the Microsoft Security Tool Kit (included as part of the TechNet distribution) to configure IIS for secure operation
- Ensure that the latest approved Service Pack and post-SP hotfixes are applied (see below)

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

Restricting remote access to the registry

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

Hive	HKEY_LOCAL_MACHINE
Key	\System\CurrentControlSet\Control\SecurePipeServers
Value Name	\winreg

- Select Permissions from the Security menu
- Ensure that the Administrators Local Group is granted Full Control and that no other users or groups are listed
- Specify applications that require remote registry access using non-administrative credentials under:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipesServer \Winreg\AllowedPaths.

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

Removing unused subsystems

- After verifying that they are not required to run any essential application software, remove the OS/2 and POSIX subsystems as follows:

- Delete the following strings from the registry:

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

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

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

Disabling unnecessary services

- Disable any services not required for the server to perform its role. In particular, consider whether the server needs any IIS 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 server unless they are strictly required for the server to perform its role

Protecting console access

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

Securing the registry

- Clean-installed Windows 2000 systems are considered to have adequately secure default ACLs on the registry. No changes are recommended.

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

- Note that upgrades from Windows NT 4 do not modify the previous security settings and should have the default Windows 2000 settings applied. Refer to the Microsoft document "Default Access Control Settings in Windows 2000" on TechNet for details on the default Windows 2000 registry ACLs and how to make any necessary modifications.

Securing the file system

- Clean-installed Windows 2000 systems are considered to have adequately secure default ACLs on the file system. No changes are recommended.

- Note that upgrades from Windows NT 4 do not modify the previous security settings and should have the default Windows 2000 settings applied. Refer to the Microsoft document "Default Access Control Settings in Windows 2000" on TechNet for details on the default Windows 2000 file system ACLs and how to make any necessary modifications.

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 a combination made up from any three of lower case, upper case, numeric and symbol characters) 14-character password on the account

- Restrict its Logon Hours to disallow logon at all times

- Restrict its Logon Workstations to one non-existent workstation name

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 server 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

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

Table of Uncrackable Alt-Characters

1= ☺	21= §	143= Å	172= ¼	192= └	212= ╘	232= Φ	252= ⁿ	177= ±	229= å
2= ☻	22= ▬	144= É	173= ¡	193= ┴	213= ╒	233= Θ	253= ²	178= ²	230= æ
3= ♥	23= ↨	145= æ	174= «	194= ┬	214= ╓	234= Ω	254= ■	181= µ	231= ç
4= ♦	24= ↑	146= Æ	175= »	195= ├	215= ╫	235= δ	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= ƒ	186= °	246= ö
7= •	27= ←	154= Ü	178= ▓	198= ╞	218= ┌	238= ∈	135= ‡	187= »	247= ÷
8= ◘	28= ∟	155= ¢	179= │	199= ╟	219= █	239= ∩	149= •	188= ¼	
9= ○	29= ↔	156= £	180= ┤	200= ╚	220= ▄	240= ≡	160= B	189= ½	
10= ◙	30= ▲	157= ¥	181= ╡	201= ╔	221= ▌	241= ±	161= ¡	191= ¿	
11= ♂	31= ▼	158= ₧	182= ╢	202= ╩	222= ▐	242= ≥	162= ¢	196= Ä	
12= ♀	32= S	159= ƒ	183= ╖	203= ╦	223= ▀	243= ≤	163= £	197= Å	
13= ♪	127= ⌂	164= ñ	184= ╕	204= ╠	224= α	244= ⌠	164= ¤	198= Æ	
14= ♫	128= Ç	165= Ñ	185= ╣	205= ═	225= ß	245= ⌡	165= ¥	199= Ç	
15= ☼	129= ü	166= ª	186= ║	206= ╬	226= Γ	246= ÷	166= ¦	201= É	
16= ►	130= é	167= º	187= ╗	207= ╧	227= π	247= ≈	167= §	209= Ñ	
17= ◄	132= ä	168= ¿	188= ╝	208= ╨	228= Σ	248= °	170= ª	214= Ö	
18= ↕	134= å	169= ⌐	189= ╜	209= ╤	229= σ	249= ·	171= «	220= Ü	
19= ‼	135= ç	170= ¬	190= ╛	210= ╥	230= µ	250= ·	172= ¬	223= ß	
20= ¶	142= Ä	171= ½	191= ┐	211= ╙	231= τ	251= √	176= °	228= ä	

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

- Change the password(s) if an administrator who knows them leaves the Organisation or is reassigned to a non-administrative role, or if you suspect the password(s) have been compromised.

- Create a "sacrificial goat" account named Administrator with no privileges and ensure that the event log is inspected regularly for evidence of attempts to use this account

- Enable account lockout across the network on the original Administrator account by using the PASSPROP.EXE utility from the Windows NT 4.0 Server Resource Kit (this utility is not included in the Windows 2000 Server Resource Kit, but use of the Windows NT 4.0 version on Windows 2000 systems is recommended by Microsoft)

Establishing separate accounts for Administrators

- Create separate administrator-equivalent accounts for each individual who genuinely requires administrative privilege to perform elements of their job function (as few as is strictly necessary)

Applying the appropriate security template

- Apply the security template appropriate to the server role, to configure the following policies:

- Password Policy (Account Policies\Password Policy)
- Account Lockout Policy (Account Policies\Account Lockout Policy)
- Audit Policy (Local Policies\Audit Policy)
- User Rights Assignment (Local Policies\User Rights Assignment)
- Security Options (Local Policies\Security Options)
- Event Log settings (Event Log\Settings for Event Logs)

Creating & securing Emergency Boot Disks

- Create an Emergency Boot Disk for each machine (or class of machine where the disk configuration is identical) and test that it can be used to boot each system
- 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
- Ensure that disks are updated if changes are made to a system's disk configuration

Creating & securing Emergency Repair Disks

- Create an Emergency Repair Disk for each machine
- Store the disks in an appropriate secure location, with access restricted to designated personnel
- Ensure that disks are updated each time changes are made to a system's configuration
- Ensure that up-to-date copies are held off-site in a fireproof safe

Limiting trust relationships

- Ensure that only authorised trust relationships are configured between different Active Directory Forests, or between Active Directory Forests and legacy Windows NT domains (in particular ensure that no inappropriate trust relationships are left in place after test scenarios have been completed and the trusts are no longer required).

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

Installing anti-virus software and updates

- Ensure that the latest approved anti-virus product, appropriate to the machine's role, is installed and configured in line with organisation standards

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

Recommended good practice

Securing user accounts

- Create users only in domains (i.e. not on workstations or Member Servers)
- Allocate a unique username to each user, in line with standard Organisation account naming conventions
- Enable the option ***User must change password at next logon*** when creating a new account
- Ensure that regular user accounts do not have their password set to ***User cannot change password*** (this does not apply to service accounts)
- Ensure that regular user accounts do not have their password set to ***Password never expires*** (this does not apply to service accounts)
- Ensure that user accounts do not have their password set to ***Store password using reversible encryption***
- Restrict each user's allowed ***Logon Hours*** as appropriate
- Restrict each user's allowed ***Log On To…*** (workstations) where possible and appropriate

Configuring Domain Operators membership

- Improve management of the system by adding relevant users to the Account Operators, Server Operators, Backup Operators, Print Operators and Power Users Local Groups, rather than granting them full administrative powers
- Use the forms provided in the document "NT / W2K Rights and Abilities" to determine privileged access requirements

Delegating administrative control

- Delegate administrative control as appropriate to avoid the need for multiple administrators to have authority over the entire domain or site. This privilege can be delegated at three levels:
  - Delegate permissions to change properties on a particular container
  - Delegate permissions to create and delete objects of a specific type in an OU, e.g. users

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

- Delegate permissions to manage specific properties on objects of a specific type in an OU, e.g. set a password on a user object

Promoting the use of RunAs

- Encourage the use of the ***RunAs*** feature to allow privileged users to run processes from a non-privileged context

Configuring group memberships

- Create appropriate (Domain) Local and Global Groups to match corporate requirements
- Use a naming convention that identifies the group type
- Assign users to Global Groups only, appropriate for the access required to perform their job function
- Grant privileges to (Domain) Local Groups only
- Allocate appropriate Global Groups to (Domain) Local Groups
- (Native Mode domains only) Use Universal groups to assign privileges to related resources in multiple domains, assigning global groups as members

Configuring shares and setting appropriate ACLs

- Assign folder permissions to appropriate user groups in line with corporate policy. The following general points should be considered:
  - Executable files should be set to ***Read***
  - Access to data files should be limited to defined groups rather than ***Everyone***
  - The maximum permission assignment should be ***Modify*** rather than ***Full Control***, unless the ability to alter security or take ownership is explicitly required
  - Access to particularly sensitive files should be denied to all but a particular group, i.e. excluding any of the Administrator or domain Operators groups

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk

References

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

- *Microsoft Security Tool Kit* (Microsoft Corporation)
- *Security Operations Guide for Windows 2000 Server* (Microsoft Corporation)
- *Securing Windows 2000 Step by Step* (The SANS Institute)
- *Hardening Windows 2000* (SystemExperts Corporation)

First•Base Technologies Town Hall Chambers High Street Shoreham-by-Sea West Sussex BN43 5DD UK
Tel: +44 (01273 454 525 Fax: +44 (0)1273 454 526 info@firstbase.co.uk