University of Tennessee

Microsoft Windows XP Professional: Guide to Creating a More Secure Operating System

Introduction

This document contains specific guidelines for establishing a secure Microsoft Windows XP computing environment. The document is meant to provide The University of Tennessee, administration, faculty, staff, and students with a systematic approach to establish and maintain secure systems, as outlined in the *Secure Desktop and Laptop – Best Practice* found at http://security.tennessee.edu. This guide will be maintained and kept current according to accepted industry standards by LAN and Desktop Support (LaDS) Security.

Compliance with the university's Information Technology Security Strategy, policies, and best practices are mandatory. In some instances, exceptions to policies and best practices must be made due to extenuating circumstances. Such exceptions must be documented and approved prior to implementation. The process for reviewing and approving/disapproving requests for exceptions can be found at http://security.tennessee.edu.

It is highly recommended that systems be reformatted with a clean install of Windows XP Service Pack 3 (SP3) before applying the recommendations found in this guide. The purpose of this is to make sure the system has not already been compromised in any kind of way, so this gives the user a clean system with which to start. Once the rebuild is complete, the system administrator or user should immediately install the latest OS patches, updates, and antivirus program before proceeding with the recommendations in this guide.

It is strongly advised that all user accounts to be used on a daily basis be set up using the principle of least-privileged user accounts. This principle says that each user on a system should be granted the least amount of privileges needed to perform his/her responsibilities. By applying the principle of least-privileged user accounts, the possibility of risks due to error and unnecessary/unauthorized use are significantly reduced. In order to implement this principle, daily users are assigned accounts in the Users group. Members of this group are given limited user rights and are less likely to have problems due to unauthorized access. System administrators are given accounts in the Administrators group and have elevated rights, which allow them to make system changes when necessary. If there is no system administrator, the user can have an account in the Administrators group. The user, while logged into the User account, can right-click on an .exe file, choose "Run As," and enter the administrator-level account name and password.

Please read this document in its entirety before attempting any of the steps listed. It is important that you understand what you are doing before you begin any of these processes or you could cause your computer and/or the applications to cease operating properly. It is also best to complete this guide a section at a time, rebooting between processes and connecting to network applications before proceeding to the next section. This is particularly important when completing Step 3 – Hardening

Local Security Policies. Should you need assistance, please contact your System Administrator, LaDS Security, or the appropriate campus HelpDesk.

Terms of Use

The recommendations in this guide are, in large part, taken from The Center for Internet Security (CIS) *Windows XP Professional Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Baseline Security Settings*. These recommendations are meant to provide system administrators and users with the best settings for providing a more secure computing environment. Please note that the recommendations are fairly generic and in many cases must be tailored to fit the needs of the specific user's system.

UT cannot guarantee that these recommendations are the perfect solution for each and every user's security needs. By following this guide, system administrators and/or users are acknowledging this and the following statements:

1. No system on the network can ever be made completely secure, even when following all the recommendations in this guide.
2. The Office of Information Technology (OIT) and its staff are not responsible for problems or damages that may arise after following the recommendations in this guide. It is important that you understand the changes in the guide before proceeding.
3. System administrators and/or users are responsible for notifying the ISO or the appropriate campus IT security group if specific problems do arise so we may re-evaluate the recommendations.
4. System administrators and/or users are responsible for keeping systems continuously updated with all OS service packs and updates, as well as with all appropriate updates for any applications on said systems, in accordance with the *Acceptable Use of Information Technology Resources (IT0110)*, also known as the AUP.
5. OIT and its staff cannot be responsible for any loss of data, loss of privacy, loss of network connectivity, etc., whether these recommendations are followed or not.

Step 1 - Hardening the Operating Systems and Application Code

All systems analysts, support personnel, and systems users need to be aware that physical security plays an equally important role in the overall protection of each system attached to the university's networks. Restrict access to each machine with a minimum requirement being establishment of a strong screensaver password. Use of screensaver passwords by all Windows XP users on the campus is an excellent protection mechanism from unauthorized physical access.

Setting screen saver passwords:

1. Go to Start → Control Panel → Display.

2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 10 minutes (or less).
4. Check the box beside "On resume, password protect." This will require a password to be entered the next time someone uses the computer.
5. Click on "OK."

It should also be noted that a system that is allowed unrestricted and unmonitored access to the university population is vulnerable to break-in even if screensaver passwords are set. The *Password Best Practices* can be found at http://security.tennessee.edu under the Policies and Best Practices section and is recommended for all systems at the university.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously click on the Windows button (the key that has the Windows logo) + "L" and the system is automatically locked. A password will be required to resume use of the computer.

Make sure that the operating system and applications are up-to-date with service packs and hotfixes. Microsoft periodically distributes large updates to its operating systems in the form of service packs. Service packs include all the major and minor fixes up to the date of the service pack, and are extensively tested by Microsoft prior to release.

Microsoft also distributes intermediate updates to their operating systems in the form of hotfixes. These updates are usually small and address a single problem. Hotfixes can be released within hours of discovering a particular bug or vulnerability. Since they are normally released so quickly, they should be used with caution. Each hotfix includes a description of the issue it resolves. This should be weighed to determine if the risk of installing the hotfix is worth the risk of not installing it.

It is important to be aware that service packs and hotfixes are not just applicable to operating systems. Individual applications have their own service pack and hotfix requirements. The total security of the system requires attention to both operating system and application levels.

The process of discovering which service packs and hotfixes are needed has been automated since the release of Windows XP.

Configuring the automated process of discovering and installing service packs and hotfixes to a Windows XP SP3 system:

1. Go to Start → All Programs → Accessories → System Tools → Security Center.
2. Under Manage security setting for: click on "Automatic Updates."
3. Choose "Automatic (recommended)" to automatically download recommended updates and install them.

4. Select “Every day” at a time when your computer will most likely be on. Please note that there will not be an update every day and Microsoft does their regular updates on Tuesdays. However, there may be a critical update on another day, so choosing every day is the best option. If you choose a time when your computer is on, the updates will run in the background. Some updates will require a reboot.

Performing the updates manually:

1. Open Internet Explorer.
2. Go to Tools → Windows Update.
3. Choose to begin getting all Microsoft product updates instead of just those for Windows.
4. Click on the link for Express to get the latest high-priority updates.
5. The update process will take a few moments to analyze your system. Click Review and install updates. You will then be prompted with a listing of service packs or hotfixes available for your system from which you can choose to install.

It is recommended that the Windows Time service be enabled for file date/time stamp accuracy and event log precision. Windows XP has a built-in NTP client that can be enabled as follows:

1. Go to Start → Run.
2. Type **cmd** and click “OK.”
3. At the command prompt, type:
   net time /setsntp: ntp.utk.edu
   where ntp.utk.edu is a preferred NTP server.
4. Right-click on “My Computer” and select “Manage.”
5. In the left-hand window, expand “Services and Applications” and select services.
6. In the right-hand window, scroll down and double-click on “Windows Time.” In the drop-down “Startup type” select “Automatic.”
7. Click the button “Start” (unless it is already started) and click on “OK.”

Step 2 - Hardening File System Security

Make sure that your hard drive partitions are formatted with NTFS (NT File System). This file system is more secure than FAT or FAT32 partition schemes. Allowed exceptions to this requirement are centrally managed servers and dual boot systems.

Checking your hard drive partitions:

1. Log in as Administrator or with administrator-level rights.
2. Double-click on “My Computer.”
3. Right-click on each hard drive letter and choose properties.
4. The general tab will identify the File system type.
5. Click cancel to close the properties window.

6. Follow steps 1 – 5 for each drive letter, noting which ones are labeled FAT or FAT32.

Converting FAT or FAT32 partitions to NTFS:

1. Go to Start → Run
2. Type **cmd** and click "OK."
3. At the command prompt, type
   convert drive /FS:NTFS /V
   where drive = one of the drive letters you noted above.
4. Hit return to run the command.
5. Follow steps 1 – 4 for each FAT or FAT32 partition.
6. Reboot the system for the changes to take effect.

Step 3 - Hardening Local Security Policies

Modifying the default local security policy is necessary for further securing your computer. Windows XP allows you easy access to the basic security functionality of your system.

While many system attacks take advantage of software inadequacies, many also make use of user accounts on a Windows computer. In order to prevent this sort of vulnerability, policies define what sort of account/password "behavior" is appropriate, and what auditing behavior is required. The configuration of user account policies is inadequate or disabled in a default installation.

Account Policies answer the questions like "How often do I need to change my password?" or "How long or how complex does my password need to be?" These policies are often left disabled or weak, leaving many machines vulnerable to attack with little or no effort. Please review the *Password Best Practices*, focusing on the specific details for system administrators. This can be found under the Policies and Best Practices section of the ISO web site (http://security.tennessee.edu).

Auditing Policies determine what sorts of security transactions are recorded in the Security Event Log. By default, nothing is retained in the Security Event Log, so any attempts to compromise a system go completely unrecorded. Logging events is crucial for analysis in the aftermath of an intrusion incident.

It is important to frequently check the Event Viewer to review log files for possible security concerns. It is optimal to log a minimum of seven days of activity in the application, system, and security logs. In order to maintain the information for seven days, users need to increase the size of the log files.

Increasing the size of the event logs:

1. Go to Start → Control Panel → Administrative Tools → Event Viewer.
2. Right-click on each event and choose Properties.

3. Change the maximum log size and choose to "Overwrite events as needed".
   a. Application Log = 16 MB (16384 KB)
   b. Security Log = 80 MB (81920 KB)
   c. System Log = 16 MB (16384 KB)

Accessing the Local Security Policy Editor Tool:

1. Go to Start → Control Panel → Administrative Tools → Local Security Policy.
2. Expand Account Policies by clicking the "+" box.
3. Select the appropriate category.
4. Double-click the individual policy settings to make the following changes.
5. When all settings have been configured, close the policy editor.

Password Policy

POLICY	SECURITY SETTING
Enforce password history	10 passwords remembered
Maximum password age	180 days[1]
Minimum password age	1 day
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

[1]The maximum password age is based on the classification of information on a specific system. For information classified as "Public" the password must be changed every 180 days. For information classified as "Proprietary" the password must be changed every 90 days. For information classified as "Confidential" the password must change every 60 days. For systems with information classified as "Highly Confidential" the user must contact the ISO. Please refer to the *Information Classification Policy (IT0115)* and the *Computer System Classification Policy (IT0116)*, found at http://security.tennessee.edu, for more information.

In order for these settings to properly take effect, you must also make sure that the user accounts do not have "Passwords Never Expire" checked. To confirm user account password status, please do the following:

1. Go to Start → Control Panel → Administrative Tools → Computer Management.
2. Expand Local Users and Groups by clicking the "+" box, then click on the Users folder.
3. Right-click on each user name and choose Properties.
4. If there is a check in the box beside "Password never expires," remove it and click on "Apply," then "OK."

Keep in mind that netid and Exchange passwords also change every 180 days. When you change one password, change them all the same day so you will then be reminded to change them all at the same time. You may want to make these passwords the same or similar so you won't be tempted to write them down and put them in a visible location. Please refer to the *Password Best Practices* for recommendations on making strong passwords. This can be found under the Policies and Best Practices section of the ISO web site (http://security.tennessee.edu).

Account Lockout Policy

POLICY	SECURITY SETTING
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Audit Policy

POLICY	SECURITY SETTING
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No Auditing
Audit logon events	Success, Failure
Audit object access	Failure (minimum)
Audit policy change	Success (minimum)
Audit privilege use	Failure (minimum)
Audit process tracking	No Auditing
Audit system events	Success, Failure

User Rights Assignment

POLICY	SECURITY SETTING
Access this computer from the network	Users, Administrators[2] (Remote Desktop Users[3] - when necessary)
Act as part of the operating system	<None>
Add workstations to domain	<Not Applicable>
Adjust memory quotas for a process	<Default>
Allow logon through Terminal Services	Remote Desktop Users[4]
Back up files and directories	<Default>
Bypass traverse checking	Administrators, Users, Local Service, Network Service, System
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	<None>
Create global objects	<Default>
Create permanent shared objects	<None>
Debug programs	Administrators
Deny access to the computer from the network	Guests, Support_388945a0

Deny logon as a batch job	<Default>
Deny logon as a service	<Default>
Deny logon locally	<Default>
Deny logon through Terminal Services	<Default>
Enable computer and user accounts to be trusted for delegation	<Not Applicable>
Force shutdown from a remote system	Administrators
Generate security audits	Local Service, Network Service
Impersonate a client after authentication	<Default>
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	<None>
Log on as a batch job	<Default>
Log on as a service	<Default>
Log on locally	Users, Administrators[2]
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Users, Administrators[2]
Replace a process level token	Local Service, Network Service
Restore files and directories	Administrators
Shut down the system	Users, Administrators[2]
Synchronize directory service data	<Not Applicable>
Take ownership of files or other objects	Administrators

[2]It is highly discouraged to assign users to the Power Users group. If you MUST add someone to the Power Users group, please add Power Users to this User Rights Assignment.

[3]When adding Users/Groups, open the policy's properties and click on "Add User or Group." Click "Object Types" and make sure that the appropriate object type is checked, then click "OK." Next, click "Locations" and make sure that the workstation is selected as the location and click "OK." Enter the object name (i.e., Network Service) in the labeled box, then click "OK."

[4] **It is highly recommended that you disable Terminal Services if it is not needed.** Should you require its use, please keep in mind that Remote Desktop Connection will not work when no users or groups have been designated to allow logon through Terminal Services, so add Remote Desktop Users as a group if necessary. For remote, off-campus access you must use the SSL VPN, https://access.utk.edu (when connecting to Windows XP systems located on the Knoxville campus). VPN access can be requested via the https://remedy.utk.edu/security/sslvpn/ website. In addition, you must configure Remote Desktop within the Windows Firewall to only allow access from the SSL VPNs IP address.

Security Options

POLICY	SECURITY SETTINGS
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limited local account use of blank password to console logon only	Enabled
Accounts: Rename administrator account	<Configure Locally>
Accounts: Rename guest account	<Configure Locally>
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security audits	Enabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not defined
Devices: Allow undock without having to log on	Disabled
Devices: Allowed to format and eject removable media	Administrators, Interactive Users
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Devices: Unsigned driver installation behavior	Warn but allow installation
Domain controller: Allow server operators to schedule tasks	Not defined
Domain controller: LDAP server signing requirements	Not defined
Domain controller: Refuse machine account password changes	Not defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled

Domain member: Disable machine account password changed	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Message text for users attempting to log on	*******WARNING******* This computer system is the property of the University of Tennessee. It is for authorized use only. The university complies with state and federal law regarding certain legally protected confidential information, but makes no representation that any other uses of this system will be private or confidential. By using this system, the user consents to interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized University of Tennessee personnel and law enforcement personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil charges/criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. **LOG OFF IMMEDIATELY** if you do not agree to these conditions. ******* **University of Tennessee*******
Interactive logon: Message title for users attempting to logon	Warning: This is a monitored computer system!
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	1 logons
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require Domain Controller authentication to unlock	Disabled

workstation	
Interactive logon: Require smart card	Not defined
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Enabled[5]
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous access SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	<No Change>
Network access: Remotely accessible registry paths	<No Change>
Network access: Shares that can be accessed anonymously	<No Change>
Network access: Sharing and security model for local accounts	Classic – local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Enabled
Network security: LAN Manager authentication level	Send NTLMv2 response only\refuse LM
Network security: LDAP client signing	Negotiate signing

requirements	
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require message integrity, Require message confidentiality, Require NTLMv2 session security, Require 128-bit Encryption (If you connect to a file server the appropriate settings must be set on the file server, as well.)
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require message integrity, Require message confidentiality, Require NTLMv2 session security, Require 128-bit Encryption (If you connect to a file server the appropriate settings must be set on the file server, as well.)
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory page file	Enabled
System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled
System objects: Default owner for objects created by members of the Administrators group	Object creator
System objects: Require case insensitivity for non-Windows	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

[5] This policy must be enabled on any Microsoft file servers you connect to, as well.

Step 4 - Hardening Default Accounts

Change the default configuration of the Administrator and Guest account. In general, a prospective user must have a username and password to access a Windows XP system. The default installation of Windows XP creates an Administrator and Guest account. By changing these accounts names, system security is greatly enhanced. The following actions should be taken:

Configuring the Administrator Account:

1. Log in as Administrator or with administrator-level rights.
2. Go to Start → Control Panel → Administrative Tools → Computer Management.

3. Expand Local Users and Groups.
4. Click on the Users folder.
5. Right-click the Administrator account and choose to rename it. Make it a non-obvious name.
6. Right-click this renamed Administrator account and select "Set Password".

Configuring the Guest Account:

1. Right-click the Guest account, and choose to rename it. Make it a non-obvious name.
2. Right-click this renamed Guest account, then select "Set Password."

Step 5 - Hardening Services

Remove programs and services that are unnecessary. The more applications that are installed on your system, the greater the risk of one of them containing a bug or security flaw.

WARNING: Disabling services without understanding what each does can make a system react adversely. Not all services are optional, therefore, be careful which services are changed. The following table outlines several examples of services that can possibly be disabled. Please note that not all services listed are on every computer. If you do not have a service that is in this list, this is not a problem.

It is very important to understand that an improperly configured service can present a vulnerability that can bypass security measures. Thus, it is critical to understand the function of each active service. There are numerous vulnerabilities in the Microsoft BackOffice product and other third party applications. You should contact the appropriate software vendors for additional security information on the services installed on your system.

Accessing Services:

1. Go to Start → Control Panel → Administrative Tools → Services.
2. Double-click service name.
3. Make appropriate changes.

SERVICE	DESCRIPTION	ACTION
Alerter	This service makes it possible for Windows XP computers to "alert" each other of problems. This feature is generally unused.	Disable if unneeded
Automatic Updates	This service enables the download and installation of Windows Updates.	Must be enabled to use the Automatic Updates feature or the Windows Update web site.
Background	This service transfers data between	Must be enabled or certain

Intelligent Transfer Service	clients and servers in the background.	features like Windows Update will not work.
Clipbook	This service is used to transfer clipboard information from one computer to another. This is generally only used in Terminal Services.	Disable if unneeded
Computer Browser	This service maintains an updated list of computers on the network and supplies that list to computers designated as browsers	<Default>
Fax Service	The Fax Service sends and receives faxes. It is generally unused.	Disable if unneeded
FTP Publishing Service	This service provides a reliable method of making files available for download and as a place for users to upload files if required.	Disable
IIS Admin Service	This service manages the IIS metabase.	Disable
Indexing Service	This service indexes contents and properties of files on local and remote computers.	<Default>
Messenger	This service works in conjunction with the Alerter service.	Disable if unneeded
Net Logon	This service supports pass-through authentication of account logon events for computers in a domain.	<Default>
NetMeeting Remote Desktop Sharing	NetMeeting users have the option to share their desktops, and allow other NetMeeting users to control their workstation.	Disable if unneeded (Please be aware that video conferencing capabilities are directly affected by this setting. If you plan to participate in any video conference activities, contact a technical representative for the required settings.)
Remote Desktop Help Session Manager	This service manages and controls Remote Assistance.	Disable until needed
Remote Registry	This service enables remote users to modify registry settings on that specific computer.	<Default>
Routing and Remote Access	This service offers routing services in LAN and WAN environment.	Disabled
Simple Mail	This service sends and receives	Disabled

Transfer Protocol (SMTP)	electronic messages.	
Simple Network Management Protocol (SNMP)	This service is used to configure remote devices, monitor network performance, audit network usage, and detect network faults or inappropriate access.	Disabled
SNMP Trap	This service listens for traps sent to the host and then passes the data along to the Microsoft SNMP management API.	Disabled
SSDP Discovery Service	This service enables discovery of UPnP devices.	Disabled
Task Scheduler	This service enables a user to configure and schedule automated tasks on a computer.	<Default>
Telnet	This service allows a remote user to connect to a machine using a command prompt. Use SSH if this functionality is needed.	Disable
Terminal Services	Allows multiple users to be connected interactively to a machine as well as the display of desktops and applications to remote computers.	<Default>
Universal Plug and Play Device Host	Provides support to host Universal Plug & Play devices.	Disabled
World Wide Web Publishing Services	This service manages and configures the IIS core components that process HTTP requests.	Disabled

Step 6 – Setting File Permissions

There are several system files that need to have the permissions or access rights set for specific users and/or groups. This will control which users/groups can view or make changes to the contents of these system files.

Setting Permissions:

1. Go to the System Root folder. This will be where the operating system has been installed. It will *usually* be C:\Windows, but may vary depending on drive mappings, partitions, etc.
2. Right-click on the appropriate file name (i.e., regedit.exe) and choose "Properties."
3. Choose the "Security" tab, then you will see the groups and/or user names.

4. Remove any group or user name other than “Administrators” and “System.”
5. You will need to add “Interactive” as a group only where indicated.
   a. Click on “Add” under the Group or user names.
   b. Click “Object Types” to make sure Groups is checked.
   c. Click “Locations” to choose the workstation name. Then enter **Interactive** as the object name, and click “OK.”
6. Click on each group name and make sure that “Full Control” is checked under the “Allow” column.

SYSTEM FILE NAME	PERMISSIONS SETTINGS
%SystemRoot%\regedit.exe	Administrators: Full; System: Full
%SystemRoot%\system32\at.exe	Administrators: Full; System: Full
%SystemRoot%\system32\attrib.exe	Administrators: Full; System: Full
%SystemRoot%\system32\cacls.exe	Administrators: Full; System: Full
%SystemRoot%\system32\debug.exe	Administrators: Full; System: Full
%SystemRoot%\system32\drwatson,exe	Administrators: Full; System: Full
%SystemRoot%\system32\drwtsn32.exe	Administrators: Full; System: Full
%SystemRoot%\system32\edlin.exe	Administrators: Full; System: Full; Interactive: Full
%SystemRoot%\system32\eventcreat.exe	Administrators: Full; System: Full
%SystemRoot%\system32\\eventtriggers.exe	Administrators: Full; System: Full
%SystemRoot%\system32\ftp.exe	Administrators: Full; System: Full; Interactive: Full
%SystemRoot%\system32\net.exe	Administrators: Full; System: Full; Interactive: Full
%SystemRoot%\system32\net1.exe	Administrators: Full; System: Full; Interactive: Full
%SystemRoot%\system32\netsh.exe	Administrators: Full; System: Full
%SystemRoot%\system32\rcp.exe	Administrators: Full; System: Full
%SystemRoot%\system32\reg.exe	Administrators: Full; System: Full
%SystemRoot%\system32\regedt32.exe	Administrators: Full; System: Full
%SystemRoot%\system32\regsvr32.exe	Administrators: Full; System: Full
%SystemRoot%\system32\rexec.exe	Administrators: Full; System: Full
%SystemRoot%\system32\rsh.exe	Administrators: Full; System: Full
%SystemRoot%\system32\runas.exe	Administrators: Full; System: Full; Interactive: Full
%SystemRoot%\system32\sc.exe	Administrators: Full; System: Full
%SystemRoot%\system32\subst.exe	Administrators: Full; System: Full
%SystemRoot%\system32\telnet.exe	Administrators: Full; System: Full; Interactive: Full
%SystemRoot%\system32\tftp.exe	Administrators: Full; System: Full; Interactive: Full
%SystemRoot%\system32\tlntsvr.exe	Administrators: Full; System: Full

Step 7 – Set Registry Keys

Certain registry keys can be configured to further secure the OS. It is important to first save the registry as it is before making the changes.

Accessing and saving the registry:

1. Go to Start → Run, then type **regedit** and click "OK".
2. Go to File → Export and chose a name and location to save the current registry settings.
3. Next proceed with the following settings. (Please keep in mind that not all systems will have all of the following keys and subkeys as this is based on what is installed on a given system.)
4. When assigning a value, please make sure you are using a decimal base.

REGISTRY KEY	VALUE	PURPOSE
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	(REG_DWORD) 255	Disables autoplay from any disk type, regardless of application
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	(REG_DWORD) 255	Disables autoplay for current user
HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun	(REG_DWORD) 255	Disables autoplay for the default profile
HKLM\System\CurrentControlSet\Services\CDrom\Autorun	(REG_DWORD) 0	Disables CD autorun
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting	(REG_DWORD) 2	Protects against source-routing spoofing
HKLM\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt	(REG_DWORD) 1	Enables IPSec to protect Kerberos RSVP traffic
HKLM\System\CurrentControlSet\Control\Session Manager\Safe-DllSearchMode	(REG_DWORD)1	Enables Safe DLL Search Mode
HKLM\System\CurrentControlSet\Services\WebClient\Parameters\ useBasicAuth	(REG_DWORD)1	Disables WebDAV basic authentication (SP2 & SP3)

Step 8 – Configure Windows Firewall

The Windows Firewall is a valuable tool for protecting a computer from unauthorized access through the Internet or network. It is important to make sure the firewall is turned on and configured properly. The firewall is available with SP2 and SP3. It is required that all Windows XP systems are updated with the latest service packs and updates.

Accessing the Windows Firewall:

Go to Start → All Programs → Accessories → System Tools → Security Center.

RULE	SETTING
General Tab	
Protect all network connections	Enabled (On)
Don't allow exceptions	Uncheck (disable) if you use applications requiring you to set exceptions.[6] Check (enable) in less secure locations, i.e., airports.
Exceptions Tab	
Allow remote administration (Group Policy)	Unchecked (disabled)
Allow File and Printer Sharing exception	Unchecked (disabled)
Allow Remote Desktop exception	Unchecked (disabled)
Allow UPnP Framework exception	Unchecked (disabled)
Display a notification when Windows Firewall blocks a program	Checked (enabled)
Advanced Tab	
Security Logging Settings – Log Dropped Packets	Checked (enabled)
Security Logging Settings – Log Successful Connections	Checked (enabled)
Security Logging Settings – Log file path and name	%SystemRoot%\firewall_standard.log (rename file to anything other than default name, which is pfirewall.log)
Security Logging Settings – Log file size limit	4096 KB (minimum)
ICMP Settings – Allow incoming echo request	Unchecked (disabled)
ICMP Settings – Allow outgoing source quench	Unchecked (disabled)
ICMP Settings – Allow outgoing packet too big	Unchecked (disabled)

[6]You must allow exceptions to use such applications as Novell, SAP, and antivirus clients.

Step 9– Incident Notification and Response

While the actions outlined in this guide will dramatically increase system security, system vulnerabilities may exist. New security holes are discovered regularly, thus, preparing for the worst is critical. It is important for the general user to be aware of potential threats, to monitor the performance and functionality of your system, and to

notify the ISO or position of authority (POA) on your campus if you see any unusual activities**.** The POA list can be found at http://security.tennessee.edu.

It is imperative that a suspected compromise of any system that stores, processes, or transmits information considered confidential or highly confidential, as categorized in the *Information Classification Policy (IT0115)*, must be reported immediately to the ISO. This includes social security numbers, credit card numbers, personally identifiable information, or information covered by FERPA, GLBA, or HIPAA.

Should you feel an incident has occurred, do NOT reboot, unplug, or otherwise alter the system when a confirmed incident has been discovered, unless directed by a member of the ISO or the incident is unlikely to be prosecuted and additional forensic information gathering is unnecessary. Otherwise, collection of valid evidence can be negatively impacted by losing critical information stored in system memory.

Additional information, including specific instructions, can be found in the *Incident Response Process Best Practice* at http://security.tennessee.edu under Policies and Best Practices, along with the *Information Classification Policy (IT0115)*

Additional Resources

No one document can provide a complete guide to securing a Windows XP system. The following resources are available for additional information regarding the theory and concepts behind this document.

The Center for Internet Security – http://www.cisecurity.org
The SANS Institute – http://www.sans.org
National Institute of Standards and Technology – http://csrc.nist.gov/itsec/guidance_WinXP_Home.html
National Security Agency Security Recommendation Guides – http://nsa2.www.conxion.com/winxp/
Microsoft Windows Security – http://www.microsoft.com/security
Service Pack Information – http://www.microsoft.com/windowsxp/pro/downloads/default.asp
Current Critical Hotfixes – http://www.microsoft.com/windowsxp/pro/downloads/servicepacks/sp1/hfdeploy.asp
Security Bulletins – http://www.microsoft.com/technet/security/
Microsoft Product Security Notification Service – https://profile.microsoft.com/RegSysProfileCenter/default.aspx?lcid=1033

Contact Information

Information Security Office (system)
(865) 974-6555

security@tennessee.edu

IT Support Help Desk – Chattanooga
(423) 425-4000
helpdesk@utc.edu

Tech Support – College of Veterinary Medicine
(865) 755-7917
vetpcsupport@mail.ag.utk.edu

Technology Services – Institute of Agriculture
(865) 974-7308
(865) 974-7159

OIT HelpDesk - Knoxville
(865) 974-9900 – students, faculty, and staff
tcshd@utk.edu

LaDS Security – Knoxville
(865) 974-9900

Operations Center (after hours service) - Knoxville
(865) 974-6027

ITS Helpdesk – Martin
(731) 881-7900
helpdesk@utm.edu

UTHSC Helpdesk – Memphis
(901) 448-2222
helpdesk@utmem.edu

IT Security Group – Memphis
(901) 448-5848

Computer Services – Space Institute
(931) 393-7363
cs@utsi.edu