2001

System Security in an Open Lab Environment

Erik Quist
Eastern Illinois University

THESIS/FIELD EXPERIENCE PAPER REPRODUCTION CERTIFICATE

TO: Graduate Degree Candidates (who have written formal theses)

SUBJECT: Permission to Reproduce Theses

The University Library is receiving a number of request from other institutions asking permission to reproduce dissertations for inclusion in their library holdings. Although no copyright laws are involved, we feel that professional courtesy demands that permission be obtained from the author before we allow these to be copied.

PLEASE SIGN ONE OF THE FOLLOWING STATEMENTS:

Booth Library of Eastern Illinois University has my permission to lend my thesis to a reputable college or university for the purpose of copying it for inclusion in that institution's library or research holdings.

[redacted] 12/11/01

Author's Signature Date

I respectfully request Booth Library of Eastern Illinois University **NOT** allow my thesis to be reproduced because:

Author's Signature Date

System Security in an Open Lab Environment

(TITLE)

BY

Erik Quist

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

Master of Science in Technology

IN THE GRADUATE SCHOOL, EASTERN ILLINOIS UNIVERSITY
CHARLESTON, ILLINOIS

2001
YEAR

I HEREBY RECOMMEND THIS THESIS BE ACCEPTED AS FULFILLING
THIS PART OF THE GRADUATE DEGREE CITED ABOVE

12|14|01
DATE

[redacted]
ADVISOR

12-14-01
DATE

[redacted]
DEPARTMENT HEAD

THESIS COMMITTEE MEMBERS

[redacted]

Philip Age, Ed.D.
Assistant Professor
Thesis Advisor
School of Technology

12/7/2001
Date

[redacted]

Peter Ping Liu, Ph.D., P.E., C.Q.E., C.S.I.T.
Professor
Graduate Coordinator
School of Technology

12/7/01
Date

[redacted]

Samuel Guccione, Ed.D., C.S.I.T.
Assistant Professor
School of Technology

12/7/01
Date

ACKNOWLEDGMENTS

I would like to give special thanks to Dr. Philip Age for his guidance throughout this research. Without him this research would not have been possible. I would also like to thank Dr. Peter Ping Liu and Dr. Sam Guccione for their influence and support during this research.

I would like to thank Eric Knuth for his work on developing and implementing these new security procedures. I would also like to thank the rest of the staff at the Lumpkin Hall Computer Labs Help Desk for assisting me with setting up and testing all of the workstations. Thank you to Brett Bensley and Gary Robinett for their technical support.

DEDICATION

I would like to thank my wife Deeanne and daughter Karisma for their love and support throughout my graduate career. I would also like to thank my parent's and family for their continual guidance and motivation.

ABSTRACT

This thesis presents a system security process for computer workstations in a university open lab environment, which was developed and implemented for the Lumpkin Hall Computer Labs at Eastern Illinois University (EIU). The system security includes the use of policies and NTFS permissions, registry hacks and script files. These techniques were applied to a mixture of Windows NT 4.0 service pack 6a and Windows 2000 Professional workstations in the Lumpkin Hall Computer Labs. They were then tested for appropriate security setup using a Network Security Checksheet and a survey. The Network Security Checksheet ensured that all of the workstations were configured properly and that the security settings where working properly to protect against known Windows exploits. A survey was used to validate the accessibility to the workstations for students in the School of Business at EIU. This new system security setup has decreased the maintenance workload by approximately 25%.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

Introduction

System Security is a complex issue faced by network administrators. The goal of system security is to protect against attacks, errors and malfunctions, while maintaining accessibility to workstations. The intent of this research is to develop and implement a security procedure in the Lumpkin Hall Computer Labs at Eastern Illinois University (EIU) that will meet the security needs.

There are many means of securing computer systems. A few examples of security techniques include security applications, policies, cloning software, and registry modifications (commonly referred to as registry hacks). In general, securing computer systems requires the use of a combination of techniques. The importance of this is to have a definite plan laid out ahead of time on what end users should and should not have access to on each computer. The plan will also depend on the availability of funds necessary to achieve the desired level of security.

Security applications are among the simplest security techniques. The developers of such applications have already done the research and developed programs to meet the typical security demands of their clientele. Examples of security applications include Full Armor and TheLock. Full Armor Zero Administration (FAZAM) was developed for Windows 95/98/NT. "There are two components to FAZAM: Protection and Undo32" (Full Armor, 1999, p. 6). The protection component protects crucial files on the workstations, while the undo component restores settings to their original settings after a system crash. Full Armor is basically a graphical user interface (GUI) policy editor. Crashcourse Software, Inc. developed TheLock for use on Windows 95/98. TheLock provides security features such as a run list, which allows the administrator to create a list of programs users are permitted to run, and the ability to hide and protect crucial system files. Both of these applications work well, but the licensing costs are high for a large open lab.

Policies are used by Windows NT and Windows 2000 systems. A policy file is created by the administrator and stored either on a server or on each workstation. This file is then read by each workstation during the authentication process when security settings are applied. Another security feature, which is built into the Windows NT and Windows 2000 operating systems, is Permissions. Permissions are set by the administrator on each file and/or folder both on the server and on each workstation. Permissions determine which users are able to access data in a given location, and how much access they have to such data (Microsoft Press, 1999).

Another tool available to network administrators is cloning software. These applications are typically used for recovery rather than security. A commonly used cloning package is Norton Ghost by Symantec Corporation, http://www.symantec.com. Norton Ghost allows the administrator to make an image of a typical hard drive, including all partitioning and system settings. This image can then be used to setup other workstations as well as to restore workstations that have crashed. This is a relatively simple process for Windows 95/98, but requires the use of a Security ID (SID) generator for Windows NT and Windows 2000. It is also crucial to have identical hardware on all workstations setup from a Ghost image since the hardware settings are included in the image. When used properly, ghosting software can save a lot of maintenance time.

Finally, registry hacks are sometimes used to secure a workstation at the local level. The only problem with registry hacks is that incorrect registry edits will render a workstation unusable. Michael Reilly, a contributing editor for *SQL (Structured Query Language) Server Magazine* and cofounder and vice president of Mount Vernon Data Systems, says, "Some administrators worry so much about making changes to the Registry that they neglect numerous opportunities to tune Windows NT and improve their system performance. Don't let the Registry scare you. If you browse in read-only mode and you take the proper backup precautions, you have nothing to fear" (Reilly, 1999, p. 2).

Another important consideration when setting up network security in an open lab environment is keeping the workstations as accessible as possible. Workstations are meant to be used by people of varying computer skill levels, which is important to keep this in mind. If the security applied to a workstation disables too many menus or applications, the purpose of having an open computer lab is defeated. It is best to keep the basic appearance of the computers the same, including drive labeling, menu setup and icon placement. The goal is to keep the workstations up and running, while providing adequate accessibility to users.

According to the Center for Democracy and Technology, "In a landmark 1997 decision, the Supreme Court ruled that the Internet is a unique medium entitled to the highest protection under the free speech protections of the First Amendment to the US Constitution. This gives the Internet same free speech protection as print" (Center, 2000, ¶ 1). In the Lumpkin Hall Computer Labs at Eastern Illinois University, two sets of policies are followed to ensure that students are not denied their First Amendment rights. The first policy is the Lumpkin Hall Computer Lab Policy approved by the School of Business at EIU and posted on the lab website (see Appendix A). The second is the policy for campus wide computer usage, which is under the User Services department (see Appendix B). The goal of system security is not to deny accessibility, but rather to keep workstations running properly.

1.2 Purpose of Research

The purpose of this research is to determine the viability of using Windows NT policies and permissions, registry hacks and script files as the present means of security in the Lumpkin Hall Computer Labs at Eastern Illinois University. This study will provide detailed procedures for the current method of network security used in the Lumpkin Hall Computer Labs at Eastern Illinois University. A Network Security Checksheet will be used to test each workstation for both accessibility and security issues. A student survey will provide valuable feedback, which will be used in the continuous improvement of the system security process in the Lumpkin Hall Computer Labs.

1.3 Definition of Terms

The following is a listing of the definitions of the terms as used in this study.

1. Policy File – The Windows NT .pol files used to setup a group of users security settings on a network.
2. Permissions – Under the NTFS file system, directories and files can be set as Full Control, Modify, Read or Special. These classifications determine the level of access that each user has to the directories and files.
3. Registry – The Registry is the backbone of the Windows operating system. It contains all of the settings for both hardware and software. The Registry is accessed by running either REGEDIT.EXE or REGEDT32.EXE. The Windows NT/2000 policy editor can also modify the registry.
4. Registry hacks – Modifications made to the registry in order to change the operating system settings for security purposes.
5. Script – A program written in either the Batch or Kixstart language that performs a series of tasks at the DOS command line.
6. Windows NT – When discussing Windows NT, this study is referring specifically to Windows NT Version 4.0 with Service Pack 6a.
7. SID – During the installation process a unique Security ID (SID) is created for each workstation. The SID is then used by the authenticating server to identify the workstation during the boot process and during any transactions made with the server. Only Windows NT and Windows 2000 workstations have SID's.

8. Run List – A run list is a list of applications, typically in the form of executable files, that the administrator sets as acceptable to run on a workstation. A run list can be either software based or created in the registry.
9. Local Area Network – "A datacomm system allowing a number of independent devices to communicate directly with each other within a moderately sized geographic area over a physical communications channel of moderate rates" (FIPS 901, 1994, p. 4).
10. Primary Domain Controller (PDC) – A Windows NT server containing the master copy of the account database for a domain. Changes are written to the PDC before being replicated to the Backup Domain Controllers (BDC) in the domain.
11. Backup Domain Controller (BDC) - The server that contains a backup copy of the account database from the Primary Domain Controller (PDC). Used for authentication purposes.

1.4 Limitations

The results of this research were limited by the following:

1. The Lumpkin Hall Computer Labs are open to the public.
2. The Lumpkin Hall Computer Labs are staffed by two full-time employees and eight student workers.
3. The surveys where not distributed in a uniform manner allowing for bias.

1.5 Delimitations

This research was delimited by the following:

1. This study is limited to the open lab facility in Lumpkin Hall at Eastern Illinois University.
2. The operating systems involved in this research are Windows NT Workstation Version 4.0 Service Pack 6a, Windows 2000 Professional and Windows NT Server.
3. Windows NT policies, Windows NT permissions, and registry edits will be used for the security on this network and this research project.
4. The utility programs used in the security process will be those located on the Windows NT Server Resource Kit and the utilities PSLIST.EXE and PSKILL.EXE, found at http://www.sysinternals.com.
5. No firewalls, routers or other networking hardware will be used in this research.
6. The surveys will only be distributed through Faculty in the School of Business at EIU.

CHAPTER 2

Review of Literature

The purpose of this study is to develop a level of security that reduces the required maintenance to a minimum, while keeping the workstations in the open computer labs in Lumpkin Hall as accessible as possible. In order to implement a network security procedure, it is crucial to have a firm grasp on the principles of network security.

First, it is necessary to know what type of environment is being secured. In the case of the Lumpkin Hall Computer Labs, it is a Local Area Network (LAN). According to the Institute of Electrical and Electronic Engineers (IEEE), a LAN is, "a datacomm system allowing a number of independent devices to communicate directly with each other within a moderately sized geographic area over a physical communications channel of moderate rates" (FIPS 901, 1994, p. 4).

Network security consists of two major components. First, the users of the system must have appropriate access to the system. This includes the ability to run approved software, print files and graphics, and access shared data appropriate to their level of access. Secondly, it is the responsibility of network security to protect critical and/or private files/data for the protection of network users and for the upkeep of the network environment. According to Greg Small, a member of the Security Infrastructure Project at Berkeley, "The computer resources to be secured are information, services, and equipment. More to the point, the qualities of these resources that we seek to secure are privacy, integrity, authenticity, and availability. Attacks, errors, and malfunctions threaten these qualities" (Small, 1999, ¶ 3). Small provides a diagram to illustrate this concept.

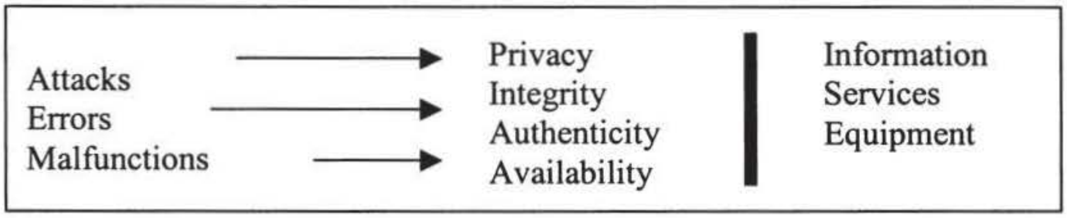


Figure 1. Diagram showing areas that network security deals with. (Small, 1999, p. 1)

Figure 1 illustrates three major issues that must be addressed when securing a network. By limiting the possibility of attacks, errors and malfunctions, an administrator can maintain privacy, integrity, authenticity and availability. This provides administrators with a basic outline for the development of a network security system.

A key factor in securing a network is the operating system driving the network. In the Lumpkin Hall Computer Labs, the two operating systems used are Windows NT and Windows 2000.

According to the Microsoft website, http://www.microsoft.com, a critical issue in securing a network is the operating system(s) used on that network. The operating system provides security at the workstation level. Windows NT and Windows 2000 have been developed specifically for the network environment, which have numerous built-in security features.

> Windows NT Workstation 4.0 provides a virtual gate through which all users, resources, and applications must pass, giving you comprehensive control and security. The security features in Windows NT Workstation include:
>
> - User authentication and access control
> - Industry standard-based certificates to verify the origin of unknown code
> - The Windows NT File System (NTFS) to protect the file system and its contents
> - Auditing to identify potential risks
> - Point-to-Point Tunneling Protocol (PPTP) for secure Internet connections
>
> (Hutton, 1998, ¶ 4)

Older operating systems such as Windows 95/98 did not contain these features, thus leaving them open to attacks.

A commonly used network security tool is security software. Many such packages are available to network administrators. Two such applications are TheLock by Crashcourse Software and Full Armor. TheLock was developed for Windows 95/98 machines by Crashcourse Software. At the time of this research, TheLock did not have a version available for Windows NT or Windows 2000. On Windows 95/98 computers, this application effectively locks users out of system configuration files and limits access to the network. The administrator simply installs this application on each workstation and follows a setup wizard, which allows the administrator to set various levels of security either by workstation or by authenticated user. Some features include the ability to hide items from the desktop and disable access to configuration menus, such as the control panel. Although this application cannot be run on Windows NT or Windows 2000 workstations, it does provide administrators with ideas as to what areas of the Windows operating system to secure.

Full Armor provides a specialized policy editor to create its own policy file, which overrides standard Windows NT policy file. This provides more setting options than the standard Windows NT Policy Editor. For example, there are check boxes for each drive on the workstation. By selecting which boxes are checked, it is possible to hide any combination of drives from users of the system. This is valuable because it keeps users from editing or deleting important program files. Another feature of Full Armor is a run list, which allows the domain administrator to enter a list of files which are either acceptable to run or unavailable for a user to run. This prevents users from installing unwanted software on a workstation. It also makes it more difficult to run hacking software (Full Armor, 1999).

Microsoft provides network administrators with several tools. Documentation on these network administration tools are presented at the Microsoft website, http://www.microsoft.com, in the form of White Books. White Books are technical documents published by the developers and manufacturers, which provide detailed descriptions of their products. Since Windows NT and Windows 2000 were developed specifically for the network environment, they have many security features built into them. The most commonly used network security features are policies and permissions (Microsoft Press, 1999).

Windows NT policies are a set of restrictions entered through the policy editor. The policy editor uses a template to apply the restrictions to the registry during the logon process. Policies can be used to hide drive partitions, hide or disable settings, including many other security related issues. Policy files are stored either on a server or on each workstation. During the logon process, the policy file is read by the workstation and the settings are implemented to the registry. One policy file can contain the policies for several different groups as well as a default policy for anyone not found in any of the established groups. The primary limitation of Windows NT policies is that they can only set values, which are located in the policy editor templates. The template file contains pointers to specific locations in the registry along with values for these variables. The standard templates only contain pointers to some of the many security settings available through registry manipulation (Microsoft Press, 1999).

When using Windows NT policies, it is necessary to set up user groups. There are many different models for setting up user groups. One of the most common ways is to setup a group for each room, job classification, or role. For example, in an open lab environment there could be a group for each lab, a group for special users such as faculty and staff, and a group for administrators. These groups are then assigned a naming convention, which must be the same naming convention used within the policies. Once the groups are created, the administrator places each user into one or more groups using the User Manager. It is important to keep in mind that if a user is in multiple groups, Windows NT will select the highest security level found for each setting (Microsoft Press, 1996).

Permissions are another security feature built into both Windows NT and Windows 2000, which set the access rights for each user. Permissions are located both on the server and workstation levels. They are applied to both shared and unshared files and directories. There are different levels of permissions including read, write, change, full control and special. Full control gives a user the ability to read, write, execute and take ownership of a file or directory. Special control refers to the ability to set permissions differently between a file and its parent directory. For example, a file may be in full control while its parent directory is read only. It is possible to set these levels on every file and directory. When setting permissions, it is important to remember that some files must be set as full control in order for them to function properly. Whenever a new software package is added, it is necessary to experiment with the permission settings to be sure that the program runs no matter which user is logged on to the system. According to Microsoft, each user must have full access to the profiles, as well as to the system and system32 folders. Since these are critical areas to secure, the administrator must find an alternative method of securing these directories (Microsoft Press, 1996).

The Internet is full of valuable information regarding network security. One valuable source of information is called Wayne's NT Resources for Administrators and Users, which can be found at http://is-it-true.org. This site contains many tips on how to modify the registry for security purposes. It also contains links to other useful sites including specific support documents on the Microsoft website. According to this site, it is important to lock down such things as the Windows Explorer and the run command located in the start menu. This site also provides detailed instructions on how to accomplish these tasks (Wayne, 2000).

According to the Wayne's site, security can be set on a workstation through the use of registry hacks, or modifications (Wayne, 2000). The registry is a very large and complicated component of any windows based operating system. Any incorrect changes to the registry can result in an unusable workstation. Wayne provides links to many registry edits, most of which are located on the Microsoft Homepage.

Another source of information on the registry is located on the O'Reilly (2000) website found at http://windows.oreilly.com/registry/ch02.htm. This site is a chapter of a book entitled NT Registry Nuts and Bolts. This site contains a detailed description of the hierarchy of the Windows registry. It also provides detailed procedures for manipulating the registry for security purposes. A firm understanding of the registry is critical before making changes since the registry is the backbone of the Windows operating system.

Rob Tidrow (1997) also wrote a book on the Windows NT registry. Similar to the one on the O'Reilly website, http://windows.oreilly.com/registry/ch02.htm, this online book, also available in paperback, contains helpful hints on the inner workings of the Windows NT registry. Tidrow also recommends sections of the registry to edit and how this is best accomplished.

With groups and permissions established and the workstations secured, there is one final issue to address. The Windows NT operating system does not allow for drive mappings or network printers to carry over from the Administrator account to other workstation users. Drive mappings are pointers to shared directories on the network. Each drive mapping includes a drive letter assignment, which appears within the My Computer icon (located on the desktop) for a user to access. These drive mappings are required to permit a user to access shared files or applications. Similarly, network printers are setup by providing a pointer to their location on the network, as well as a pointer to the required driver for the printer. The fact that drive mappings and network printers do not carry over between users on a workstation causes a dilemma on how to allow access to shared network resources and printers. Logon scripts are necessary to enable access to shared resources.

There are many different scripting languages available. One of the most common is the batch file. Batch files allow commands to be executed at the DOS command line. For example, the NET USE command can be used in a batch file to map a network drive by specifying a drive letter and network path. Batch files have one major drawback. Unlike some other scripting languages, batch files do not allow for loops or calculations. Looping is important for scripting because it allows for similar commands to be executed a specified number of times without repeating the command in the program. They can also be used to call other executable programs. Calling other executables is not efficient and can lead to long authentication processes. Many inexperienced computer users will become frustrated if the logon time gets too long and will either walk away or start pounding on the keyboard. This is not what an administrator wants (Microsoft Press, 1995).

One scripting language that gives the administrator more control over the logon scripts is called Kixstart. Kixstart incorporates the usual batch commands with its own set of commands such as looping functions. Using Kixstart, an administrator can create script files, which make changes to the registry on startup. These changes can be for security purposes, or for device mapping purposes. Kixstart is one of many useful utilities included in the Windows NT Resource Kit (Microsoft Press, 1996).

There are many shareware utilities, which can be executed within script files for security purposes. These utilities can perform tasks such as removing unwanted files and/or directories, listing tasks on a remote workstation and/or terminating unwanted applications, editing permissions, and editing the registry. Two such utilities are PSLIST.EXE and PSKILL.EXE, which can be downloaded at http://www.sysinternals.com.

The Windows NT Resource Kit also contains many other useful utilities. Two useful utilities found on the resource kit are XCACLS.EXE and REG.EXE. XCACLS.EXE is a utility to be used to edit the Windows NT permissions at the command line level. It can be executed with a script file during the boot process in order to change the permissions of the current user. More often it is used with a script file during the installation process of each workstation rather than by a logon script (Heyne, 1999).

REG.EXE is a utility for editing the registry at the DOS command line level. It can be used in any script file or simply be run from the command line. Since each user has a profile containing registry settings specific to their logon session, certain settings must be made during the authentication process. This can be accomplished by running a logon script. The logon script then executes the REG.EXE utility to modify the registry for the current user. This allows administrators greater control over the workstations found on the network (Microsoft Press, 1996).

PSLIST and PSKILL are two utilities created by Mark Russinovich, chief software architect and cofounder of Winternals Software. PSLIST allows an administrator to list the tasks currently in use on any remote workstation or server

(Russinovich, 2000a). Similarly, PSKILL allows an administrator the ability to terminate any task that is running on a workstation or server (Russinovich, 2000b). In combination, these two utilities give the administrator a greater amount of control over what is being run on each workstation. The drawback is that these utilities only allow an administrator to terminate an application that is spotted manually. For example, if an administrator suspects that a user is trying to run hacking software, PSLIST can be run to determine what programs are currently being run on the workstation in question, and PSKILL can then be used to terminate any application that is unauthorized.

CHAPTER 3

Methodology

3.1 Procedure

The first step was to determine what needed to be secured in the Lumpkin Hall Computer Labs at Eastern Illinois University. After testing several security techniques including security applications, ghosting and policies and permissions, it was determined that policies and permissions were the best option. The critical areas to secure included the Network Neighborhood, Windows Explorer, system files, and the control panel.

Using known registry hacks, a new policy template was developed (see Appendix C). This template was then used to create policy files. These policy files were placed on the Primary Domain Controller (PDC), which is located in the server closet in Lumpkin Hall. A backup copy was also placed on Backup Domain Controller (BDC).

Next, all of the workstations were setup following the setup procedures for the Lumpkin Hall Computer Labs (see Appendices D and E). This involved an initial format, and then a reinstall of the operating system and all required software. The final process consisted of running several script files on each workstation (see Appendix F).

Once all of the workstations were setup according to specifications, they were checked using a Network Security Checksheet (see Appendix G). This checksheet lists critical functions to enable/disable. A survey (see Appendix H) was then distributed through faculty members to students in the School of Business. These surveys were gathered and analyzed. The surveys were then used to determine how the workstations operated with the new security setup in place.

3.2 Subjects

This research was focused solely on the workstations in the Lumpkin Hall Computer Labs at Eastern Illinois University. It included ninety-three open lab workstations and forty classroom workstations. The operating systems used on these workstations are either Windows NT 4.0 with service pack 6a or Windows 2000 Professional Edition. Authentication and the application of the policy files are handled by the PDC and BDC.

The effectiveness of the security methods was determined by the use of a Network Security Checksheet and a survey. The survey was distributed through faculty in the School of Business to students that use the Lumpkin Hall Computer Labs for their coursework.

3.3 Design

New methods of securing workstations in the Lumpkin Hall Computer labs were researched and tested. Detailed procedures were then developed and used in the setup of the workstations in the labs during the routine summer maintenance (see Appendices D and E).

Once the workstations were setup, they were checked using a Network Security Checksheet (see Appendix G). The checksheet was used to inspect each workstation for complete and proper security setup. Any deficiencies were repaired before moving on to the next workstation.

A survey was distributed through faculty members in the School of Business at Eastern Illinois University (see Appendix H). The surveys were then collected and analyzed to determine how accessible data files, printing, the Internet, and various software packages were in the Lumpkin Hall Computer Labs.

CHAPTER 4

Implementation

4.1 Process

The first step in implementing the new security system in the Lumpkin Hall Computer Labs at Eastern Illinois University was to setup a test workstation in each lab. During this process, each step was documented and placed into a manual for that lab (see Appendices D and E).

During the testing phase, it was found that by setting the permissions too tight, applications including Microsoft Word, Macromedia Dreamweaver and Oracle would not function properly. This was due to the fact that some applications required more access than others to specific directories on the workstation in order to run. An example of this is the Application Data folder found in the C:\WINNT\Profiles\All Users folder on Windows NT workstations and the C:\Documents and Settings\All Users folder on Windows 2000 workstations. Several applications including Microsoft Word, PowerPoint and Access require EVERYONE to have full control permission on this folder. By varying permission levels in a systematic manner, a security level was found that met the needs for the lab (see Appendix F). This also lead to a multiple partition setup including one for the operating system, one for software and one for student access (see Appendices D and E).

For the Lumpkin Hall Computer Labs, the most cost effective method of security was the use of Windows NT Policies and Permissions, registry hacks, and scripts. By creating a unique set of policy file templates, it was possible to lock down workstations in a manner very similar to security applications such as Full Armor.

Windows NT comes with two default policy templates: winnt.adm and common.adm. These default templates did not have enough options to lock workstations down at the desired level. A solution was to merge them together into one template file and add in some registry settings of our own. The final product was a template called lumpkin.adm (see Appendix C).

The creation of template files takes a little practice. The lumpkin.adm template file (see Figures 2 and 3) was created by looking at the default templates and manipulating them using registry hacks found through this research.
For example, changing the location of the personal files from C:\Personal to E:\Personal. The following is a screen shot of how the policy editor looks when using the lumpkin.adm template.

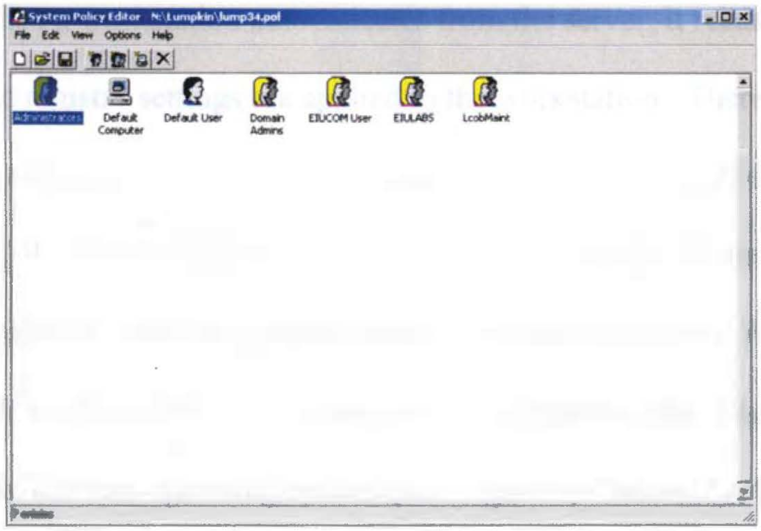
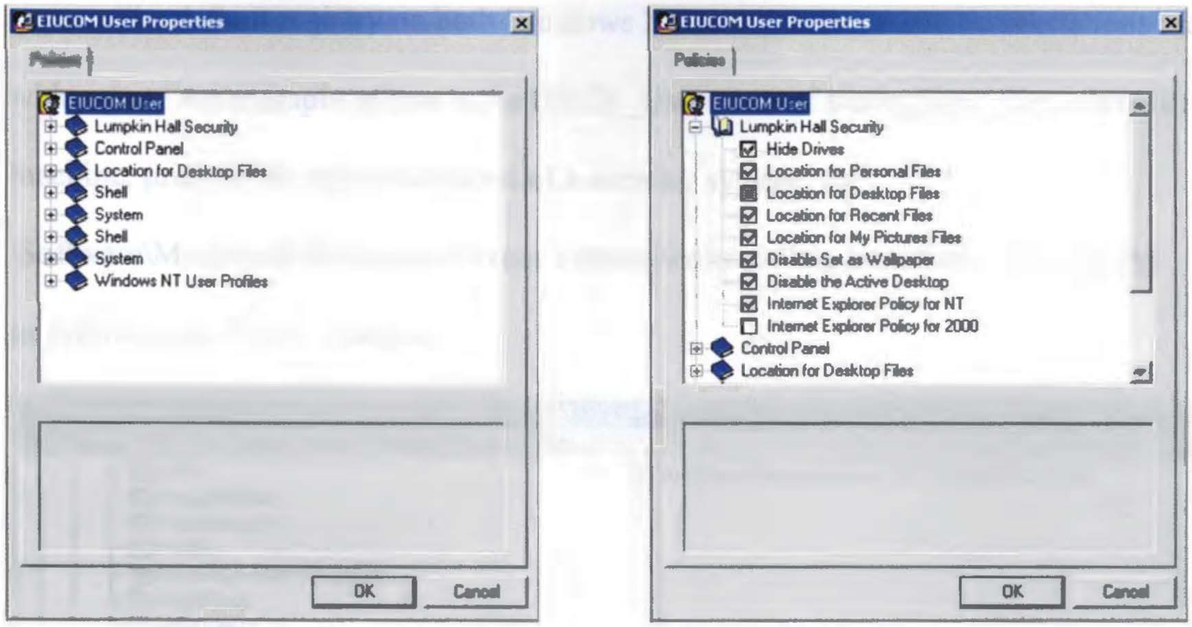


Figure 2. Screenshot of a typical Policy File.

When a group is selected, in this case EIUCOM User, the properties appear as follows in Figure 3.



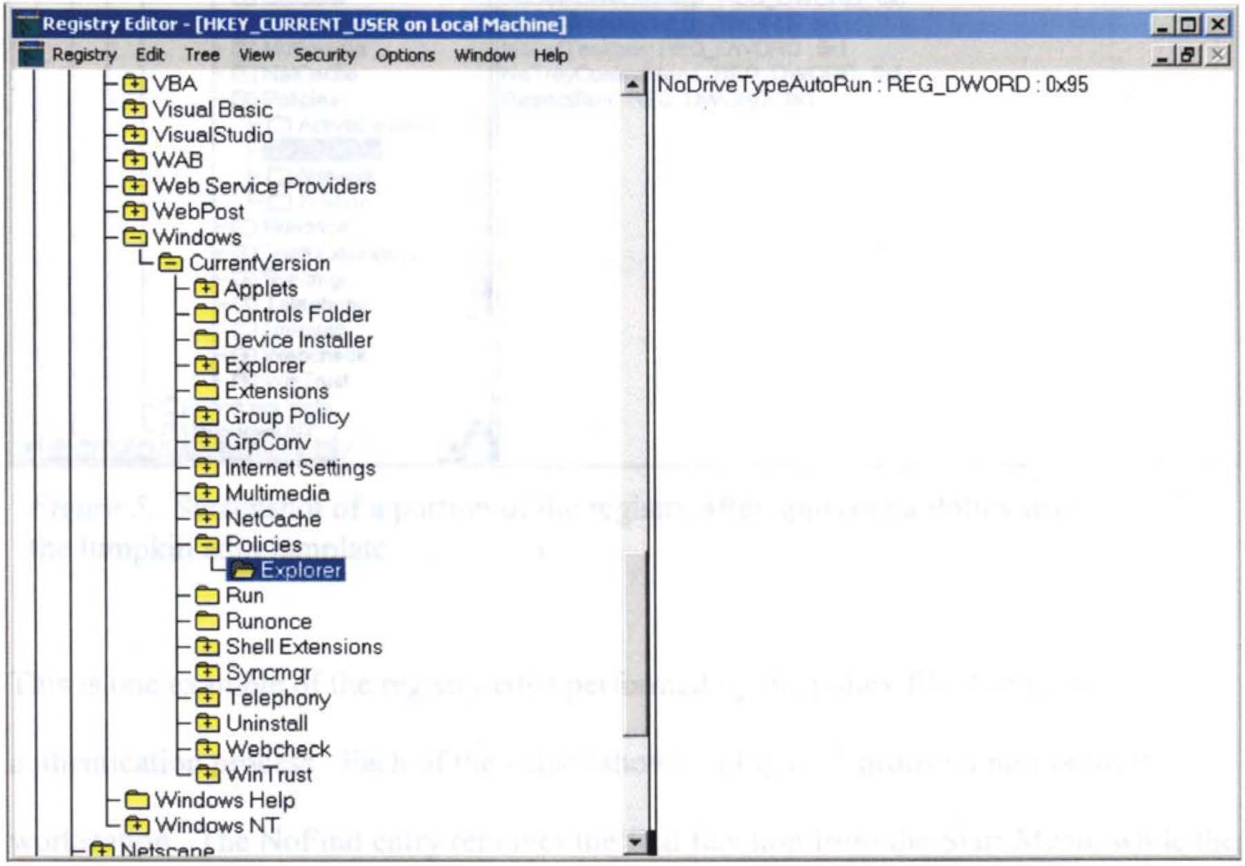
EIUCOM User
- Lumpkin Hall Security
- Control Panel
- Location for Desktop Files
- Shell
- System
- Shell
- System
- Windows NT User Profiles

EIUCOM User
- Lumpkin Hall Security
  - ☑ Hide Drives
  - ☑ Location for Personal Files
  - ■ Location for Desktop Files
  - ☑ Location for Recent Files
  - ☑ Location for My Pictures Files
  - ☑ Disable Set as Wallpaper
  - ☑ Disable the Active Desktop
  - ☑ Internet Explorer Policy for NT
  - □ Internet Explorer Policy for 2000
- Control Panel
- Location for Desktop Files

Figure 3. Screenshot of a Policy using the lumpkin.adm template.

Each checkbox in Figure 3 is associated with a registry setting, which is coded in the template file. When a workstation authenticates from the server, it reads the appropriate policy file and the registry settings are applied to the workstation. There are two major differences that need to be considered when dealing with a mixed environment including Windows NT and Windows 2000 workstations. First, the portion of the registry dealing with Microsoft Internet Explorer is located under a different branch in Windows 2000 than it is in Windows NT. This is accounted for in the lumpkin.adm template by a separate checkbox for each operating system (see Figure 3). Secondly, the Shell in Windows 2000 is slightly different than the Shell in Windows NT. Windows NT stores user profiles in the C:\WINNT\Profiles directory, while Windows 2000 stores profiles in the C:\Documents and Settings folder. For this reason, separate policy files must be created for each operating system. More details on the security settings are available in Appendix E.

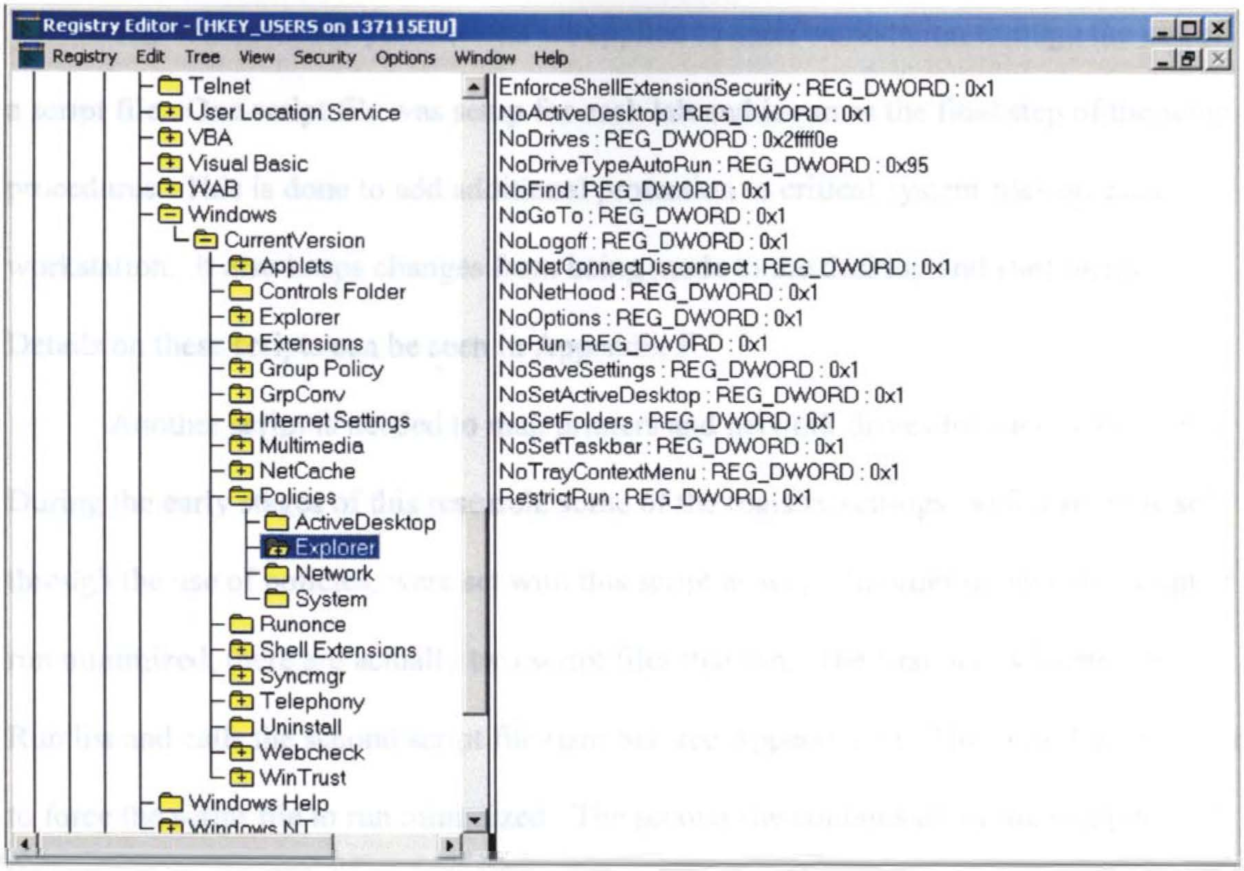
The default registry on both Windows NT and Windows 2000 workstations are wide open. An example of this is the HKEY_Users tree of the registry. On a default machine, prior to the implementation of a security system, the \Software\Microsoft\Windows\Current Version\Policies\Explorer folder will appear as follows (see Figure 4 below).



```
NoDriveTypeAutoRun : REG_DWORD : 0x95
```

Figure 4. Screenshot of a portion of the registry prior to the implementation of a Policy.

After applying a policy made using the lumpkin.adm template (see Figures 2 and 3), a secured workstation will have the following registry entries.



```
EnforceShellExtensionSecurity : REG_DWORD : 0x1
NoActiveDesktop : REG_DWORD : 0x1
NoDrives : REG_DWORD : 0x2ffff0e
NoDriveTypeAutoRun : REG_DWORD : 0x95
NoFind : REG_DWORD : 0x1
NoGoTo : REG_DWORD : 0x1
NoLogoff : REG_DWORD : 0x1
NoNetConnectDisconnect : REG_DWORD : 0x1
NoNetHood : REG_DWORD : 0x1
NoOptions : REG_DWORD : 0x1
NoRun : REG_DWORD : 0x1
NoSaveSettings : REG_DWORD : 0x1
NoSetActiveDesktop : REG_DWORD : 0x1
NoSetFolders : REG_DWORD : 0x1
NoSetTaskbar : REG_DWORD : 0x1
NoTrayContextMenu : REG_DWORD : 0x1
RestrictRun : REG_DWORD : 0x1
```

Figure 5. Screenshot of a portion of the registry after applying a Policy using the lumpkin.adm template.

This is one example of the registry edits performed by the policy file during the authentication process. Each of the values shown in Figure 5 protect a portion of the workstation. The NoFind entry removes the find function from the Start Menu, while the NoRun entry removes the Run function from the Start Menu. Other changes are made throughout the registry according to the settings chosen by the administrator using the Policy Editor. Additional registry modifications can be seen in Appendix F.

The Windows NT permissions are applied to each workstation through the use of a script file. One script file was setup for each lab and is run as the final step of the setup procedures. This is done to add additional protection to critical system files on each workstation. It also keeps changes from being made to the desktop and start menu. Details on these scripts can be seen in Appendix F.

Another script is needed to map printers and network drives for each workstation. During the early stages of this research, some of the registry settings, which are now set through the use of policies, were set with this script as well. In order to have the script run minimized, there are actually two script files that run. The first one is located in the Run list and calls the second script file (tsm.bat, see Appendix F). This was done in order to force the script file to run minimized. The second file contains all of the mappings for printers and network drives. Examples of these scripts can be seen in Appendix F.

4.2 Results

Once all of the lab workstations were setup, the Network Security Checksheet (see Appendix G) was used to inspect each workstations security settings. This by no means ensures that there is no way of hacking into the workstations in Lumpkin Hall, but each workstation is sufficiently secured to keep the maintenance levels to a minimum. In fact, the time spent maintaining workstations has been reduced significantly since the implementation of the new security procedures.

A few weeks into the semester of Fall 2001, a survey was distributed through classes in the School of Business (see Appendix H). Approximately six hundred surveys were passed out and three hundred and forty three where collected. This survey was used to determine how accessible the workstations are in the Lumpkin Hall Computer Labs. A series of pie charts and bar charts have been used to present the data collected from the surveys (see Figures 6-13).

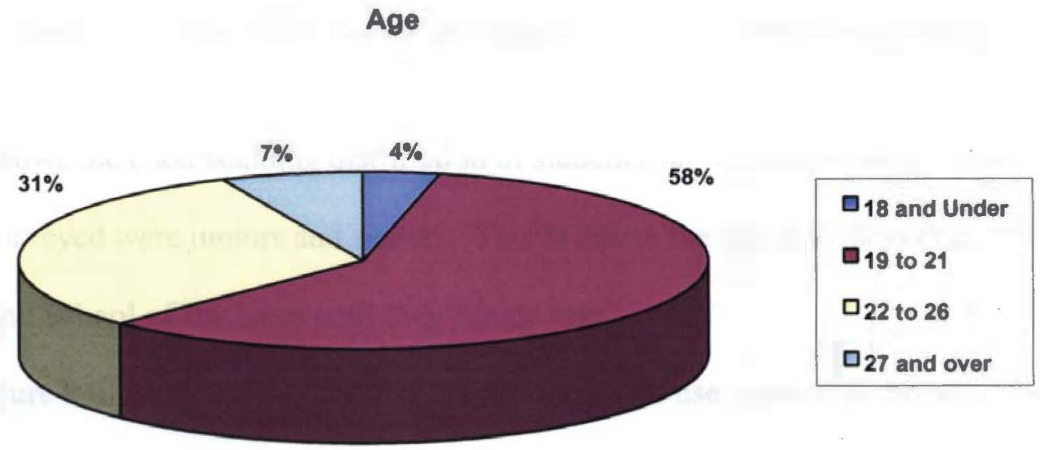


Figure 6. Pie chart of the percentage of users in each age group.

Figure 6 shows that a typical college cross-section was surveyed, with the majority of students falling within the age range from 19 to 21. The fact that 31% of the students surveyed fell within the age range from 22 to 26 reflects the graduate students in the School of Business.

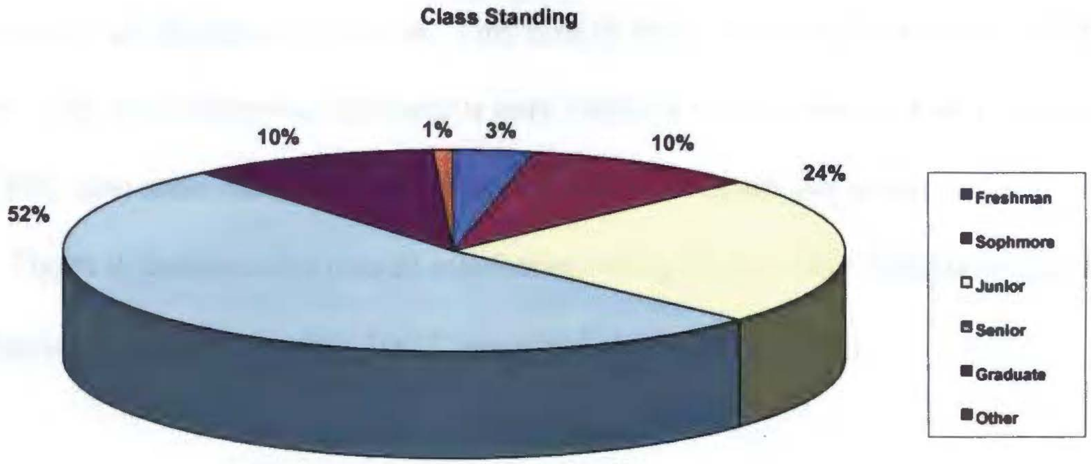


Figure 7. Pie chart showing the percentage of users in each class standing.

Figure 7 shows the class standing distribution of students surveyed. The majority of the students surveyed were juniors and seniors. This is due to the fact that most students do not enter the School of Business until their junior year.

Figure 8 illustrates the average hours per week that users spend in the other labs on campus (see Figure 8a) and in Lumpkin Hall (see Figure 8b).

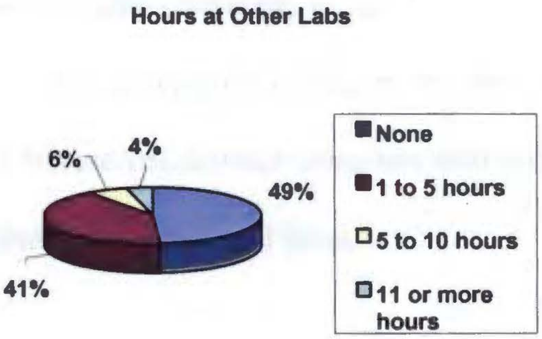


Figure 8a. Pie chart showing the percentage of users that fall under each usage level for other Lab Facilities.

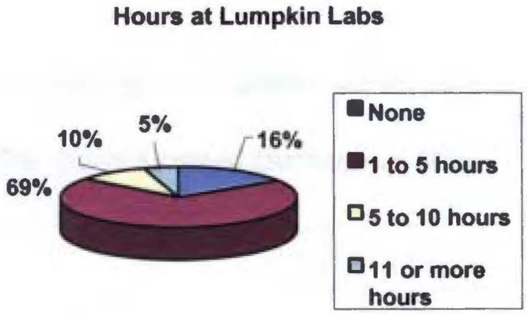


Figure 8b. Pie chart showing the percentage of users that fall under each usage level in Lumpkin.

Figure 8 shows that the students surveyed used the Lumpkin Hall Computer Labs more than the other lab facilities on campus. This is most likely due to the fact that some of the software used in the School of Business is only installed in the Lumpkin Hall Computer Labs. They also show that the typical usage is one to five hours per week.

Figure 9 illustrates the overall satisfaction rating for the other campus facilities (see Figure 9a) and the Lumpkin Hall Computer Labs (see Figure 9b).

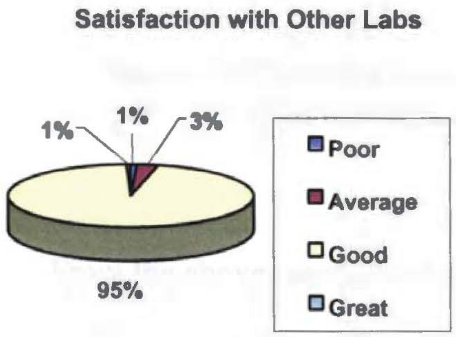


Figure 9a. Pie chart showing the percentage of users that gave ratings for the other Lab Facilities.

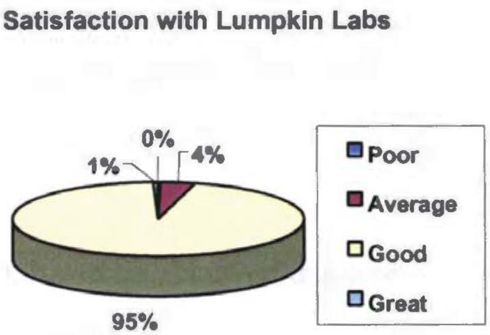


Figure 9b. Pie chart showing the percentage of users that gave ratings for the Lumpkin Hall computer labs.

Figure 9 shows that the majority of students surveyed rate the computer labs at Eastern Illinois University as good.

The next pie chart, Figure 10, shows the percentages of students surveyed that rated themselves on their computer skill level. The majority rated themselves at the moderate computer skill level.

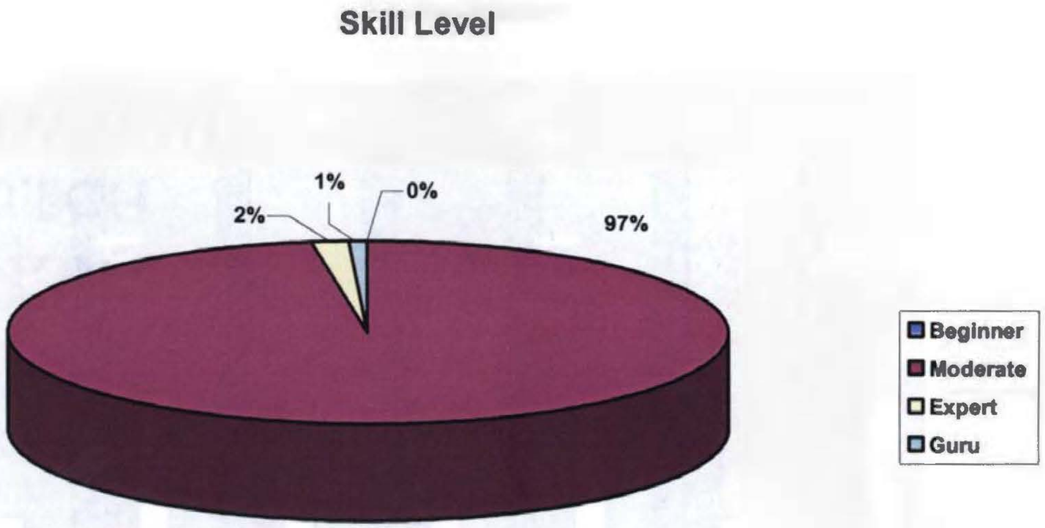
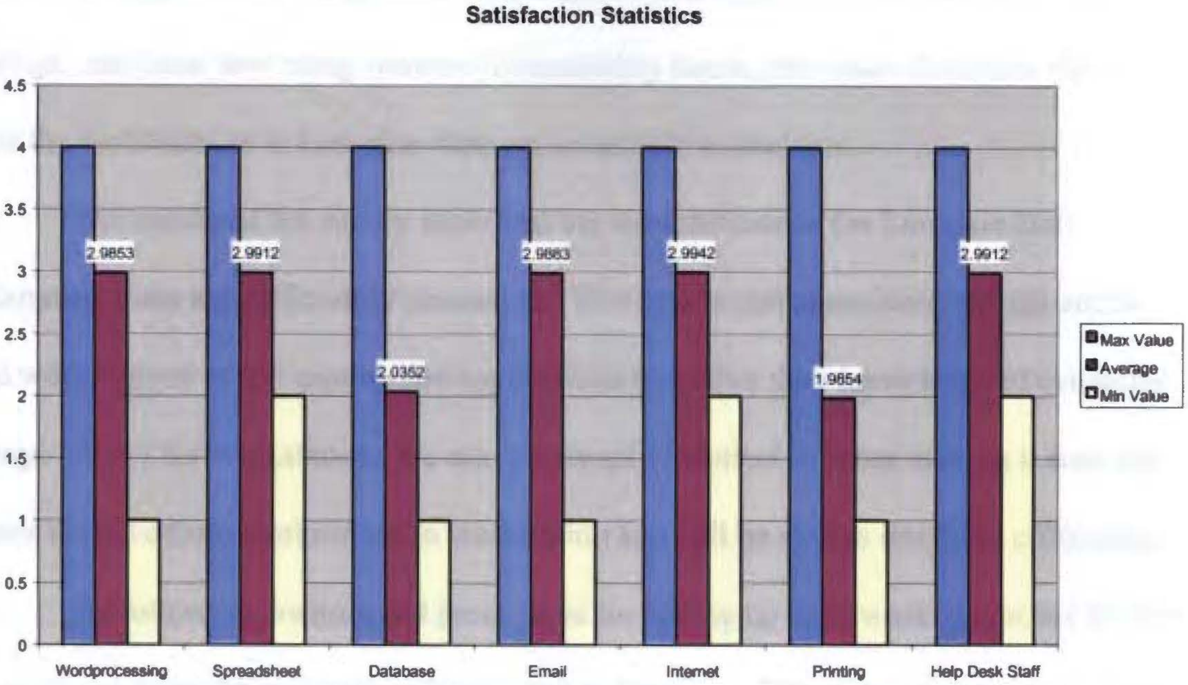


Figure 10. Pie chart showing the percentage of users that fall under each level of computer usage skill.

From the above pie charts (see Figures 6-10), it can be observed that the majority of students fell into the moderate skill level. Moreover, the students surveyed used the Lumpkin Hall Computer Lab Facility more than the other lab facilities available on the EIU campus. This is most likely due to the fact that the surveys were distributed in the School of Business and most of the software used in the School of Business is only located in the Lumpkin Hall Computer Labs.

The final chart (Figure 11) contains the results of the satisfaction levels for various aspects of the labs. These values are on a Likert Scale with one being poor and four being great. This chart (Figure 11) shows that the two weakest areas in the Lumpkin Hall Computer Labs are Database Software and Printing. The low rating for the Database Software can be explained by the recent upgrade to Oracle 8i.



Note: These levels are on a Likert Scale from 1 to 4 with 1 = "Poor", 2 = "Fair", 3 = "Good" and 4 = "Great"

Figure 11. Bar chart showing the average ratings for each of the items.

Many configuration errors occurred during the Oracle 8i upgrade. This added confusion for students using the application. Another component of the lower rating for Database Software is the complexity of mastering Oracle Software. Similarly, the low rating for printing can be explained by the use of dot matrix Epson printers in an attempt to provide a free printing alternative to users. Laser and Color Laser printing are also available in the Lumpkin Hall Computer Labs, but there is a fee for using these printers, and students must come to the Help Desk to request and pick up these higher quality printouts. An alternative method of printing is being discussed at this time. These rating levels are critical since a slight adjustment in the security settings could render an application or one of its components inaccessible. Since there were only two areas that received low ratings, and these low rating were not accessibility issues, this chart illustrates the fact that the workstations in Lumpkin Hall are accessible to students.

The results of the survey show that the workstations in the Lumpkin Hall Computer Labs are sufficiently accessible. This means that users have enough access to the workstations to use appropriate applications to further their knowledge of computer usage. All of the workstations are also practically identical in setup making it easy for users to move from workstation to workstation and still be able to use them efficiently.

By following documented procedures for setting up each workstation, we are able to keep our workstation setups as consistent as possible. The scripts also ensure that the same security settings are applied to every workstation. Using the Network Security Checksheet (see Appendix G), all of the workstations are tested for consistent and complete security settings. Although no network security system can completely rule out the possibility of hackers getting into the system, the security system established through this research has met the needs of the Lumpkin Hall Computer Labs and its users.

CHAPTER 5

Conclusions

System security is a very complex issue, with many approaches available to administrators. The goal of this research was to show one such method, which was developed, tested and implemented in the Lumpkin Hall Computer Labs at Eastern Illinois University. This method consists of Windows NT Policies and Permissions, registry hacks, and scripting. The criteria that needed to be met included protection of critical system files, protection of School of Business and other personal data stored on the servers, and uniformity throughout the labs. The workstations have to be accessible enough for students to learn how to use them efficiently, while secured enough to keep them up and running year round.

All of the workstations have been tested for appropriate security using the Network Security Checksheet (see Appendix G). This ensures that all of the workstations in the Lumpkin Hall Computer Labs meet the standards developed through this research. Since the implementation of these new security settings, the man-hours spent maintaining workstations have dropped by about 25%. This supports the success of the procedures described throughout this paper.

The accessibility has also been tested through the use of a survey (see Appendix H). The results shown in Figures 6-10 confirm that the workstations are accessible to users. Changes are currently in progress to raise the ratings of database software and printing in the Lumpkin Hall Computer Labs. Hopefully, these two issues will be resolved in the next year.

This security approach has improved the accessibility and security of the workstations within the Lumpkin Hall Computer Lab Facility. Through the use of NTFS Policies and Permissions, registry hacks and scripts, a cost effective and viable security setup has been established. It is hoped that this research will assist other open lab facilities in implementing a successful security procedure of their own.

CHAPTER 6

Further Research

There are several areas in which more research can be done. Three primary areas are the usage of intrusion detection software to further protect a local area network, setting permissions in the registry and the use of ghosting software to cut down on setup and maintenance time.

During this research, funding was not available to purchase intrusion detection software, such as Intact by Pedestal Software, but a demo version was tested. Another intrusion detection application that could be tested is Tripwire. This type of software has a great deal of potential in securing a local area network. For example, this software can be configured to notify the administrator when a secured folder is tampered with.

Windows NT and Windows 2000 also provide the ability to set permissions within the registry. This provides administrators with an increased ability to tweak the level of access allowed to users. One feature of this would be to disallow students access to the Software key in the registry.

At the time of this research, Norton Ghost was being used to a limited degree for setting up and maintaining Windows 95/98 email stations, but it was not being used for Windows NT or Windows 2000 installations. Recently another ghosting package called Drive Image Pro by PowerQuest Corporation has been used on the Eastern Illinois University Campus and is being considered as a possible tool to be used in the Lumpkin Hall Computer Labs.

References

Bixler, David. (1999). MCSE simulation guide: Windows NT server networking guide. Indianapolis: New Riders.

Center for Democracy & Technology. (2000). An overview of the communications decency act (CDA). <http://www.cdt.org/speech/cda> [2000, Dec. 3].

Crashcourse Software. (1999). TheLock. Program Documentation.

Federal Information Processing Standards Publication 191 (FIPS 901). (1994). <http://secinf.net/info/policy/fips191/index.html> [2001, Sept. 23].

Full Armor. (1999). Full armor zero administration and network configuration. Program Documentation.

Hanner, K. and Hormanseder, R. (1999). Managing windows NT file system permissions. <http://www.fim.uni-linz.ac.at/publications/SAT/> [2000, Oct. 10].

Heyne, Frank. (1999). The DACL manager for registry keys. Microsoft Program Documentation.

Heywood, Drew. (1998). Using windows NT server 4. Indianapolis: Que.

Hutton, Susan. (1998). Why Upgrade? Running Windows 95 at work?
Eight solid reasons to move to Windows NT Workstation 4.0.
<http://asia.microsoft.com/windows95/whyupgrade
/runningW95NT.asp> [2001, Sept. 23].

Lumpkin Hall Computer Labs. (2000). Computer Lab Policy. <http://www.eiu.edu/~lcoblab/policy.html> [2000, Dec. 3].

Methvin, David. (1998). Secrets of the NT registry. <http://www.windowsmagazine.com/library/1998/0701/fea0078.html> [2000, Oct. 23].

Microsoft Press. (1999). Guide to windows NT 4.0 profiles and policies. <http://support.microsoft.com/support/kb/articles/Q185/5/89.ASP> [2000, Sept. 13].

Microsoft Press. (1995). Kixtart 95 user's guide. Program Documentation.

Microsoft Press. (1996). Microsoft windows NT server networking guide. Redmond: Microsoft Press.

O'Reilly. (2000). NT registry nuts and bolts. <http://windows.oreilly.com/registry/ch02.htm> [2000, Oct. 12].

Reilly, Michael. (1999). Editing the windows NT registry. <http://www.winntmag.com/Articles/Index.cfm?ArticleID=4719> [2000, Dec. 3].

Russinovich, Mark. (2000a). Pslist. Program Documentation. <http://www.sysinternals.com/pslist.html> [2000, July 12].

Russinovich, Mark. (2000b). Pskill. Program Documentation. <http://www.sysinternals.com/pskill.html> [2000, July 12].

Small, Greg. (1999). The long path to security. <http://wssg-test.berkeley.edu/public/projects/SecurityInfrastructure /articles/The_Long_Path_to_Security/> [2001, Sept. 23].

Symantec Corporation. (2000). Norton Ghost 6.03. Program Documentation.

Tidrow, Rob. (1997). Windows NT registry troubleshooting. <http://www.gasullivan.com/boerg/00000/000d1.htm> [2000, Oct. 24].

User Services. (1997). Appropriate use of information technology services facilities including the world wide web. <http://www.eiu.edu/~infotech/NetFacUse.htm> [2000, Dec. 3].

Wayne's NT Resources for Administrators and Users. <http://is-it-true.org/nt/> [2000, Sept. 15].

APPENDIX A

Lumpkin Hall Computer Labs Policy

Lab Policy

These policies and rules were established so that the computing environment in Lumpkin Hall Labs can be enjoyable and stress free for all students. When these policies/rules are not obeyed, other students have difficulty preparing and completing their assignments. Think about your fellow students before you decide to break the rules.

UNAUTHORIZED DOWNLOADING OF ANY TYPE IS STRICTLY PROHIBITED!!! THIS INCLUDE WALLPAPERS & SCREEN SAVERS!!!!

If unauthorized downloading continues to occur, computers in the lab will be monitored continuously.

NO FOOD OR DRINK ALLOWED IN LABS!

LASER PRINTOUTS ARE NOT FREE! THEY MUST BE PAID FOR WITH A PANTHER CARD! HELP DESK EMPLOYEES ARE NOT AUTHORIZED TO TAKE CASH FOR PRINTOUTS!

HELP DESK EMPLOYEES ARE HERE TO HELP YOU WITH THE EQUIPMENT IN THE LAB AND TO ANSWER QUESTIONS ABOUT THE SOFTWARE PROVIDED IN THE LABS, TO THE BEST OF THEIR ABILITY.
The Help Desk employees WILL NOT do your homework for you or become your personal tutor.

ALTHOUGH THIS IS NOT A LIBRARY, IT IS AN ACADEMIC ENVIRONMENT. PLEASE KEEP NOISE LEVEL LOW SO OTHER STUDENTS CAN CONCENTRATE ON THEIR WORK.

IF THERE IS A CLASS SCHEDULED IN THE LAB, OTHER STUDENTS MUST EXIT THE LAB WHEN THE CLASS BEGINS, UNLESS PERMISSION IS GIVEN BY INSTRUCTOR. <u>NO EXCEPTIONS!!!!!</u>

PLEASE BE PATIENT WITH HELP DESK WORKERS. WE CANNOT HELP MORE THAN ONE STUDENT AT A TIME.

APPENDIX B

User Services Lab Policy

Appropriate Use of Information Technology Services facilities

Including the World Wide Web

Information Technology Services provides computing facilities and services for the legitimate instructional, research, and administrative computing needs of the university. Proper use of those facilities and services supports the legitimate computing activities of EIU students, faculty and staff. Proper use respects intellectual property rights.

Legitimate instructional computing is work done by an officially registered student, faculty, or staff member in direct or indirect support of a recognized course of study. Legitimate research computing is work approved by an authorized official of a university department. Legitimate administrative computing is work performed to carry out official university business.

Intellectual property rights begin with respect for intellectual labor and creativity. They include the right to acknowledgment, the right to privacy, and the right to determine the form, manner and terms of publication and distribution.

Proper computing use follows the same standards of common sense and courtesy that govern use of other public facilities. Improper use violates those standards by preventing others from accessing public facilities or by violating their intellectual property rights. Therefore, the basic policy of the university on proper use is:

- Any use of Information Technology Services facilities or services unrelated to legitimate instructional or research computing is improper if it interferes with another's legitimate instructional or research computing.
- Any use of Information Technology Services facilities or services that violates another person's intellectual property rights is improper.
- Any use of Information Technology Services facilities or services that violates any university policy, any local, state or federal law, or which is obscene or defamatory is improper.
- Any use resulting in commercial gain or private profit (other than allowable under university intellectual property policies) is improper.

The following sections describe some known instances of improper use. They do not constitute a complete list. When new occasions of improper use arise, they will be judged and regulated by the basic policy stated above.

DISRUPTIVE CONDUCT

Avoid behavior at any computing facility that would interfere with another person's legitimate use of the facility. This includes noisy and over-exuberant conduct.

DAMAGE

Avoid actions that would damage Information Technology Services facilities, hardware software, or files.

ACCESS TO FILES

Avoid reading or using others' files without their permission. Proper usage standards require everyone to take prudent and reasonable steps to limit access to their files and accounts.

FRAUD AND FORGERY

Avoid sending any form of electronic communication that bears a fraudulent origin or identification. This includes the forging of another's identity on electronic mail or news postings.

COPYRIGHT

Refer to Eastern Illinois University Regulation 16a.and applicable sections of the Federal Copyright Act, including fair use provisions I Section 107 of H.R. 2223, to avoid violating the copyright law as you contemplate copying software, digital images, and other electronic media. You should also review the report of the Information Infrastructure Task Force (IITF) for concerns about digital images and educational multimedia.

HARASSMENT

Avoid using the university computing facilities to harass anyone. This includes the use of insulting, obscene or suggestive electronic mail or news, tampering with others' files, and invasive access to others' equipment.

NETWORKS

Avoid using local, national and international networks for things that are not legitimate instructional or research activities of the university. This includes, but is not limited to articles for commercial gain posted on electronic news networks and repeated attempts to access restricted resources.

UNAUTHORIZED USE OF ACCOUNTS

Avoid accessing an account not specifically authorized to you, whether it is on an Information Technology Services system or one at another place. Avoid using an account for a purpose not authorized when the account was established, including personal and commercial use.

Don't engage in computing activities that are designed to invade the security of accounts. Attempts to decipher passwords, to discover unprotected files, or to decode encrypted files are examples.

Proper usage standards require that everyone take prudent and reasonable steps to prevent unauthorized access.

UNAUTHORIZED USE OF SOFTWARE

Do not make unauthorized copies of licensed or copyrighted software. Do not make copyrighted or licensed material accessible from a Web page without the specific written permission of the copyright owner.

Avoid actions that are in violation of the terms or restrictions on the use of software defined in official agreements between the university and other parties.

Examples include: the copying of software from personal computers unless it is clearly and specifically identified as public domain software or shareware that may be freely redistributed; and the copying of restricted Unix source code. Read the policy topic "Rules for Access to UNIX Source Code" for more information on Unix license restrictions.

WWW SPECIFIC CLAUSES

General policies for computer use apply to those who develop or are responsible for the development of web pages on our World Wide Web server. However, the ability to publish electronically creates some unique opportunities and concerns. Style issues are covered within the EIU Publications Policy at http://139.67.11.100/PUBSMANUAL/pubman.html. The following four web-specific clauses are necessary.

1. Privacy

   People have a right to privacy. Employees acting within the scope of their employment may not place any item(s) (regardless of whether the person can be identified) such as, but not limited to, pictures, videos, audio-clips, or information about an individual(s) without the express written permission of the individual(s). The exception is those items that are determined to be necessary for university administrative functions.

2. Fair Warning

   Users of the EIU WWW must realize material put on the WWW is available to a wide audience, often beyond that originally intended for the material. There must be a recognition that, in different contexts, material may be construed in a manner different from that of the original intention of the author(s). Therefore, at the request of the appropriate university official(s), an information provider will provide a Awarning page@ at one level before any WWW page(s). This will be a standard page expressing that the content below may not be suitable for all audiences. WWW users, particularly minors, have a right to a "fair warning."

3. Use of University Name, Seal, and Logo

   Use of the university name, seal, and logo is not permitted except as allowed and/or required by university policy and regulations.

4. Personal Home Pages and WWW Servers

   EIU provides Internet/WWW access and resources for conduct of university functions. Personal use, e.g. development and posting of personal home pages and WWW servers, is permitted insofar as such activity does not disrupt, due to time, place, or manner, the conduct of university functions and as long as it is in compliance with the remainder of this and other university policies. The official EIU home page will not link directly to personal pages

ENFORCEMENT

When instances of improper use come to its attention, Information Technology Services will investigate them. During those investigations Information Technology Services reserves the right to access private information, including the contents of files and mailboxes, while making every effort to maintain privacy. Investigations that discover improper use may cause Information Technology Services to:

- Limit the access of those found using facilities or services improperly;
- Refer flagrant abuses to deans, department heads, the responsible vice president, the university

police, or other authorities for appropriate action;

- Disclose private information to other university authorities.

Users who violate this policy may have their computing privileges terminated and may be subject to disciplinary action by the university in accordance with appropriate policies or judicial affairs procedures.

RULES FOR ACCESS TO UNIX SOURCE CODE AND LICENSED SOFTWARE

One of the big factors in the increasing popularity of the UNIX operating system at EIU is how easily UNIX source code applications can be moved among different variations of the UNIX system. This process, commonly called porting, often requires nothing more than copying and compiling an application to move it from one UNIX platform to another. The porting process is so simple that it is easy to lose sight of the ownership of individual programs and the license agreement restrictions on their source code.

1. License Agreements

Source code for computer programs is usually owned by the organization that developed the programs. Since many of these organizations have an economic stake in their developmental investment, they don't just give it away. At a minimum, they usually declare their copyright on the programs. But legally, a more powerful means exists: a license agreement.

Software license agreements are contracts in which the seller agrees to provide the program, and perhaps its source code, provided that the buyer agrees to abide by the rules of the license. Most workstation-based software that is issued with the installation of a UCAN workstation is licensed software. NCSA Telnet and Kermit packages are noted exceptions. Sellers can specify just about any rules they desire so long as the buyer agrees to those rules. And just to make life interesting, every seller of computer software seems to have its own special rules to follow. Licensed software must not be duplicated, distributed, modified, or used without authorization.

Some programs are distributed in source form without a license agreement. They may be totally unrestricted (called ``public domain") or the owner may retain the copyright but allow free distribution. A lot of useful software designed to run on UNIX systems is distributed this way. As a user of one of EIU's systems, you may find source code to such programs in various system directories.

2. Source Code at EIU

Whenever possible, most UNIX system administrators at EIU strive to obtain the source code for programs because it makes it easier to maintain systems and quickly fix problems. In order to obtain source code for commercial software systems, it is necessary to negotiate the ``Terms and Conditions" of the software license agreement with each software vendor. Some of those agreements permit anyone at EIU to have access to the source code while others stipulate restrictions. Therefore, you may find that you have access to source a source code that is restricted by a license agreement. Just because you have access does not mean you have the right to port a program to another system. When it comes to the UNIX operating system and its associated utilities and libraries, EIU adheres to license agreements with IBM, Sun Microsystems, the University of California at Berkeley, and other vendors that redistribute UNIX. These license agreements specify the rules under which we may have access to the source code in the first place.

If you have a UNIX system of any kind and want to obtain source access, please follow these rules:

- Check with the source-code vendor to determine if an additional vendor license is required. Follow the vendor's restrictions on redistributing the vendor's source code.
- Source code access for most Sun UNIX systems is provided under agreements between EIU and the Sun Corporation.
- When in doubt, do not assume you have the right to copy sources from another UNIX system to your own; contact the SUN license administrator at EIU or the administrator of the system from which you wish to copy the sources before doing so.

WASTE

Avoid any wasteful use of Information Technology Services facilities. This includes squandering expendable resources, processor cycles, disk space, or network bandwidth. Use expendable resources such as paper prudently, and recycle them if possible. Use a system whose capacity is appropriate to the size of the computing task.

REQUESTS FOR SERVICES

Information Technology Services is the central coordinating department for computerized instruction, research, and administrative functions of the university. If a change in or addition to programming or networking services is desired, a request must be submitted, in writing, to the Associate Vice President for Information Technology Services. The request shall state in detail the change in service desired and shall be signed by the Fiscal Agent of the requesting unit. User Services support requests should be brought to the attention of the Director of User Services, or if clarification is needed, the request should be discussed with a member of the staff within the User Services Division of Information Technology Services.

Information Technology Services staff shall not be responsible for initiating changes in administrative mainframe applications; however, they do maintain the right to make suggestions. Applications shall be revised when systems software requires it or when hardware that is necessary for processing reaches obsolescence.

ACQUISITION OF COMMODITIES

The Information Technology Services operations manager maintains the inventory of supplies necessary for central data processing system operation. The acquisition of microcomputer supplies is the responsibility of the owning department. Forms that are currently not on inventory must be acquired by the requesting department. However, the acquisition of new forms to be printed by mainframe connected printers must be coordinated through the Associate Vice President of Information Technology Services or the Assistant Director for Operations.

MICROCOMPUTER AND NETWORK SERVICES

Information Technology Services shall provide the following services:

1. Maintenance

Services provided by Information Technology Services staff shall include the repair of microcomputers that are currently approved for maintenance support and consultation on microcomputer and software purchases. Replacement parts are a part of this service fee; however, if, in the judgment of the Information Technology Services staff, the microcomputer is beyond repair, the using department shall be responsible for funding any replacement. A maintenance service fee shall be charged for each IBM PC/XT/AT, Zenith, Swan, Apple, or other covered microcomputer that was purchased from an account other than an appropriated account and that is on inventory.

2. Network Support Services -- Uniform Campus-wide Area Network (UCAN)

Information Technology Services staff shall provide for the installation of network hardware and software components and shall service the communications components that are installed by them. The UCAN circuit boards and the electronic equipment within wiring closets is to be maintained and modified by Information Technology Services staff only. UCAN software components should all be treated as licensed software by end users.

PRINTERS, PLOTTERS AND MODEMS

Information Technology Services staff shall provide advice and minor repairs for printers, plotters and modems; however, the using department is responsible for major repairs and replacements. Examples of minor repairs would include cleaning, simple mechanical adjustment, and the replacement of a print head that is furnished by the using department.

MAINFRAME, UCAN NETWORK SERVER, AND WORK-STATION FILE SECURITY

Information Technology Services acts as the custodian of all university data bases or data processing files, but it is not the owner of these files. Individual users should take reasonable precautions regarding the physical security of their equipment and should change their passwords frequently. The system administrator for servers other than the mainframe will provide mechanisms for backup and password controls. However, the management, security, and backup of files stored on servers other than the campus mainframe are the responsibility of the individual user. You are best able to assess the level of privacy and security of the data and text files that you create.

APPENDIX C

Lumpkin.adm Policy Template

```
; test code by Erik Quist 4/10/01
****************************************************

CLASS Machine

CATEGORY !!Lumpkin
POLICY !!Logon
      KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Winlogon"
            PART !!AutoLogon CHECKBOX
                  Valuename "AutoAdminLogon"
                  VALUEON "2"
                  VALUEOFF "0"
            END PART
            PART !!DeleteCache CHECKBOX
                  Valuename "DeleteRoamingCache"
                  VALUEON NUMERIC 1
                  VALUEOFF NUMERIC 0
            END PART
END POLICY
POLICY !!RemoteUpdate
            KEYNAME System\CurrentControlSet\Control\Update
            ACTIONLISTOFF
                  VALUENAME "UpdateMode"              VALUE NUMERIC 0
            END ACTIONLISTOFF
                  PART !!UpdateMode                   DROPDOWNLIST
REQUIRED
                  VALUENAME "UpdateMode"
                  ITEMLIST
                        NAME !!UM_Automatic           VALUE NUMERIC 1
                        NAME !!UM_Manual              VALUE NUMERIC 2
                  END ITEMLIST
                  END PART

                  PART !!PolicyPointer COMBOBOX REQUIRED
                  SUGGESTIONS
                        !!Stubdc01_NT !!Stubdc01_2000
                        !!Stubdc06_NT !!Stubdc06_2000
                  END SUGGESTIONS
                  Valuename "NetworkPath"
                  END PART

                  PART !!DisplayErrors                CHECKBOX
                  VALUENAME "Verbose"
                  END PART

                  PART !!LoadBalance                  CHECKBOX
                  VALUENAME "LoadBalance"
                  END PART
            END POLICY
END CATEGORY


;from common.adm
*******************************************************************

CATEGORY !!System
      POLICY !!Run
      KEYNAME Software\Microsoft\Windows\CurrentVersion\Run
            PART !!RunListbox                                LISTBOX
EXPLICITVALUE
            END PART
      END POLICY
END CATEGORY      ; System

;from winnt.adm
**********************************************************************

CATEGORY  !!Network
        CATEGORY !!Sharing
                KEYNAME
System\CurrentControlSet\Services\LanManServer\Parameters

                POLICY !!WorkstationShareAutoCreate
                        VALUENAME "AutoShareWks"
                        VALUEON NUMERIC 1
                  VALUEOFF NUMERIC 0
                        PART !!ShareWks_Tip1            TEXT    END
PART
                        PART !!ShareWks_Tip2            TEXT    END
PART
                END POLICY

                POLICY !!ServerShareAutoCreate
                        VALUENAME "AutoShareServer"
                        VALUEON NUMERIC 1
                  VALUEOFF NUMERIC 0
                        PART !!ShareServer_Tip1         TEXT    END
PART
                        PART !!ShareServer_Tip2         TEXT    END
PART
                END POLICY

        END CATEGORY    ; Sharing

END CATEGORY    ; Network

CATEGORY  !!Printers
KEYNAME System\CurrentControlSet\Control\Print
            POLICY !!PrintManager_Browser_Restrict
            VALUENAME  DisableServerThread
            PART !!Disable_Server_Tip1                          TEXT
            END PART
            PART !!Disable_Server_Tip2                          TEXT
            END PART
            END POLICY

            POLICY !!Scheduler_Thread_Priority
            PART !!Scheduler_Priority
DROPDOWNLIST
            VALUENAME SchedulerThreadPriority
                  ITEMLIST
                        NAME "Above Normal"  VALUE NUMERIC  1
                        NAME "Normal"        VALUE NUMERIC  0
                        NAME "Below Normal"  VALUE NUMERIC  -1
                  END ITEMLIST
            END PART
            END POLICY

            POLICY !!Beep_Enabled
            VALUENAME BeepEnabled
                VALUEON NUMERIC 1
                VALUEOFF NUMERIC 0
            PART !!Beep_Tip1                          TEXT  END PART
            PART !!Beep_Tip2                          TEXT  END PART
            END POLICY
END CATEGORY

CATEGORY  !!RemoteAccess
KEYNAME System\CurrentControlSet\Services\RemoteAccess\Parameters
            POLICY !!MaximumRetries
                  PART !!RAS_Length                         NUMERIC
REQUIRED
                  MIN 1 MAX 10 DEFAULT 2
                  VALUENAME AuthenticateRetries
                  END PART
            END POLICY
            POLICY !!MaximumTime
                  PART !!RAS_Time                           NUMERIC
REQUIRED
                  MIN 20  MAX 600 DEFAULT 120
                  VALUENAME AuthenticateTime
                  END PART
            END POLICY
            POLICY !!CallBackTime
                  PART !!INT_Time                           NUMERIC
REQUIRED
                  MIN 2 MAX 12 DEFAULT 2
                  VALUENAME CallbackTime
                  END PART
            END POLICY
            POLICY !!Auto_Disconnect
                  PART !!Autodisconnect_Time                NUMERIC
REQUIRED
                  MIN 0  DEFAULT 20
                  VALUENAME AutoDisconnect
                  END PART
            END POLICY
END CATEGORY

CATEGORY !!Shell

        CATEGORY !!CustomSharedFolders
                KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"

                POLICY !!CustomFolders_SharedPrograms
                        PART !!CustomFolders_SharedProgramsPath
EDITTEXT REQUIRED  EXPANDABLETEXT
                        DEFAULT !!CustomFolders_SharedProgramsDefault
                        VALUENAME "Common Programs"
                        END PART
                END POLICY

                POLICY !!CustomFolders_SharedDesktop
                        PART !!CustomFolders_SharedDesktopPath
EDITTEXT REQUIRED  EXPANDABLETEXT
                        DEFAULT !!CustomFolders_SharedDesktopDefault
                        VALUENAME "Common Desktop"
                        END PART
                END POLICY

                POLICY !!CustomFolders_SharedStartMenu
                        PART !!CustomFolders_SharedStartMenuPath
EDITTEXT REQUIRED  EXPANDABLETEXT
                        DEFAULT !!CustomFolders_SharedStartMenuDefault
                        VALUENAME "Common Start Menu"
                        END PART
                END POLICY

                POLICY !!CustomFolders_SharedStartup
                        PART !!CustomFolders_SharedStartupPath
EDITTEXT REQUIRED  EXPANDABLETEXT
                        DEFAULT !!CustomFolders_SharedStartupDefault
                        VALUENAME "Common Startup"
                        END PART
                END POLICY

        END CATEGORY
END CATEGORY    ; Shell


CATEGORY  !!System
        CATEGORY !!Login_Policies
                POLICY !!LogonBanner
                KEYNAME "Software\Microsoft\Windows
NT\CurrentVersion\Winlogon"
                        PART !!LogonBanner_Caption
EDITTEXT
                        VALUENAME "LegalNoticeCaption"
                        MAXLEN 255
                        DEFAULT !!LogonBanner_DefCaption
                        END PART

                        PART !!LogonBanner_Text
EDITTEXT
                        VALUENAME "LegalNoticeText"
                        MAXLEN 1024
                        DEFAULT !!LogonBanner_DefText
                        END PART
                END POLICY

                POLICY !!Shutdown_Restrict
                KEYNAME "Software\Microsoft\Windows
NT\CurrentVersion\Winlogon"
                        VALUENAME  ShutdownWithoutLogon
                        VALUEON "1"  VALUEOFF "0"
                        PART !!Shutd_Tip1
TEXT    END PART
```

```
                        PART !!Shutd_Tip2
TEXT    END PART
                        PART !!Shutd_Tip3
TEXT    END PART
                END POLICY

                POLICY !!LastUserName_Restrict
                KEYNAME "Software\Microsoft\Windows
NT\CurrentVersion\Winlogon"
                        VALUENAME DontDisplayLastUserName
                        VALUEON "1"  VALUEOFF "0"
                        PART !!Dont_Display_Tip1
TEXT    END PART
                        PART !!Dont_Display_Tip2
TEXT    END PART
                        PART !!Dont_Display_Tip3
TEXT    END PART
                END POLICY

                POLICY !!Run_Logon_Script_Sync
                KEYNAME "Software\Microsoft\Windows
NT\CurrentVersion\Winlogon"
                        VALUENAME RunLogonScriptSync
                        PART !!Script_Tip1                      TEXT
END PART
                        PART !!Script_Tip2                      TEXT
END PART
                        PART !!Script_Tip4                      TEXT
END PART
                END POLICY

        END CATEGORY    ; Login Policies

        CATEGORY !!FileSystem
                KEYNAME System\CurrentControlSet\Control\FileSystem

                POLICY !!Disable8dot3Names
                VALUENAME "NtfsDisable8dot3NameCreation"
                END POLICY


                POLICY !!AllowExtCharsIn8dot3
                        VALUENAME
"NtfsAllowExtendedCharacterIn8dot3Name"
                        PART !!ExtChars_Tip1
TEXT    END PART
                        PART !!ExtChars_Tip2
TEXT    END PART
                END POLICY

                POLICY !!DisableLastUpdate
                        VALUENAME "NtfsDisableLastAccessUpdate"
                        PART !!LastAccess_Tip1
TEXT    END PART
                        PART !!LastAccess_Tip2
TEXT    END PART
                END POLICY
        END CATEGORY    ;  File system

END CATEGORY    ; System

CATEGORY  !!UserProfiles
KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\winlogon"

                POLICY !!DeleteRoamingCachedProfiles
                VALUENAME "DeleteRoamingCache"
                PART !!DeleteCache_Tip1                                  TEXT
END PART
                PART !!DeleteCache_Tip2                                  TEXT
END PART
                END POLICY

                POLICY !!EnableSlowLinkDetect
                VALUENAME "SlowLinkDetectEnabled"
                END POLICY

                POLICY !!SlowLinkTimeOut
                        PART !!SlowLinkWaitInterval
NUMERIC REQUIRED
                        MIN 1 MAX 20000 DEFAULT 2000
                        VALUENAME SlowLinkTimeOut
                        END PART
                END POLICY

                POLICY !!SlowLinkDefault
                        PART !!DefaultOperation          DROPDOWNLIST
REQUIRED
                        VALUENAME "SlowLinkProfileDefault"
                        ITEMLIST
                                NAME !!PD_DOWNLOAD              VALUE
NUMERIC 1
                                NAME !!PD_USELOCAL              VALUE
NUMERIC 0
                        END ITEMLIST
                        END PART
                END POLICY

                POLICY !!ChooseProfileDefault
                        PART !!DefaultOperation          DROPDOWNLIST
REQUIRED
                        VALUENAME "ChooseProfileDefault"
                        ITEMLIST
                                NAME !!PD_DOWNLOAD              VALUE
NUMERIC 1
                                NAME !!PD_USELOCAL              VALUE
NUMERIC 0
                        END ITEMLIST
                        END PART
                END POLICY

                POLICY !!ProfileDlgTimeOut
                        PART !!ProfileDlgWaitInterval
NUMERIC REQUIRED
```

```
                        MIN 0 MAX 600 DEFAULT 30
                        VALUENAME ProfileDlgTimeOut
                        END PART
                END POLICY

END CATEGORY


;test code by Erik Quist 4/10/01
*****************************************************

CLASS User

CATEGORY !!Lumpkin
POLICY !!HideDrives
             KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
                     PART !!HIDEDRIVES DROPDOWNLIST REQUIRED
                     #if version > 1
                     NOSORT
                     #endif
                     VALUENAME "NoDrives"
                             ITEMLIST
                             NAME !!ACDEFGHY VALUE NUMERIC 50331394
                             NAME !!ADEGHY VALUE NUMERIC 50331430
                             NAME !!AEFGHY VALUE NUMERIC 50331406
                             NAME !!CLEARALL VALUE NUMERIC 0 DEFAULT
                             END ITEMLIST
                     END PART
                     PART !!HIDEDRIVESTEXT1 TEXT END PART
                     PART !!HIDEDRIVESTEXT2 TEXT END PART
END POLICY
POLICY !!PersonalFiles
            KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"
                  VALUENAME "Personal"
                  VALUEON "E:\Personal"
                  PART !!PersonalTip                           TEXT
END PART
END POLICY
POLICY !!Desktop
            KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"
                  VALUENAME "Desktop"
                  VALUEON "E:\Desktop"
                  PART !!DesktopTip                            TEXT
END PART
END POLICY
POLICY !!Recent
            KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"
                  VALUENAME "Recent"
                  VALUEON "E:\Recent"
                  PART !!RecentTip                             TEXT
END PART
END POLICY
POLICY !!MyPictures
```

```
            KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"
                  VALUENAME "My Pictures"
                  VALUEON "E:\My Pictures"
                  PART !!MyPicturesTip                         TEXT
END PART
END POLICY
POLICY !!Wallpaper
            KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop"
                  VALUENAME "NoChangingWallPaper"
                  VALUEON NUMERIC 1
                  VALUEOFF NUMERIC 0
                  PART !!WallpaperTip                      TEXT    END
PART
END POLICY
POLICY !!ActiveDesktop
            KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Policies\Explorer"
                  PART !!NoSet CHECKBOX
                        VALUENAME "NoSetActiveDesktop"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!NoActive CHECKBOX
                        VALUENAME "NoActiveDesktop"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
END POLICY
POLICY !!LumpkinIENT
            KEYNAME "Software\Policies\Microsoft\Internet
Explorer\Restrictions"
                  PART !!NoFileOpen CHECKBOX
                        VALUENAME "NoFileOpen"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!NoFileNew CHECKBOX
                        VALUENAME "NoFileNew"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!NoBrowserSaveAs CHECKBOX
                        VALUENAME "NoBrowserSaveAs"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!NoBrowserOptions CHECKBOX
                        VALUENAME "NoBrowserOptions"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!NoFavorites CHECKBOX
                        VALUENAME "NoFavorites"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
```

```
END PART
PART !!NoSelectDownloadDir CHECKBOX
      VALUENAME "NoSelectDownloadDir"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!NoBrowserContextMenu CHECKBOX
      VALUENAME "NoBrowserContextMenu"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!NoFindFiles CHECKBOX
      VALUENAME "NoFindFiles"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!GeneralTab CHECKBOX
      VALUENAME "GeneralTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!SecurityTab CHECKBOX
      VALUENAME "SecurityTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!ContentTab CHECKBOX
      VALUENAME "ContentTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!ConnectionsTab CHECKBOX
      VALUENAME "ConnectionsTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!ProgramsTab CHECKBOX
      VALUENAME "ProgramTabs"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!AdvancedTab CHECKBOX
      VALUENAME "AdvancedTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!CertifPers CHECKBOX
      VALUENAME "CertifPers"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!SecChangeSettings CHECKBOX
      VALUENAME "SecChangeSettings"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!SecAddSites CHECKBOX
```

```
                        VALUENAME "SecAddSites"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!FormSuggest CHECKBOX
                        VALUENAME "FormSuggest"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!FormSuggestPass CHECKBOX
                        VALUENAME "FormSuggest Pasword"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!ConnwizAdmin CHECKBOX
                        VALUENAME "Connwiz Admin Lock"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!IESettings CHECKBOX
                        VALUENAME "Settings"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!ResetWebSettings CHECKBOX
                        VALUENAME "ResetWebSettings"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!Download CHECKBOX
                        KEYNAME "Software\Microsoft\Internet Explorer"
                        VALUENAME "Download Directory"
                        VALUEON "E:\"
                        VALUEOFF "A:\"
                  END PART

END POLICY
POLICY !!LumpkinIE2K
            KEYNAME "Software\Policies\Microsoft\Internet
Explorer\Control Panel"
                  PART !!NoFileOpen CHECKBOX
                        VALUENAME "NoFileOpen"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!NoFileNew CHECKBOX
                        VALUENAME "NoFileNew"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!NoBrowserSaveAs CHECKBOX
                        VALUENAME "NoBrowserSaveAs"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!NoBrowserOptions CHECKBOX
                        VALUENAME "NoBrowserOptions"
```

```
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!NoFavorites CHECKBOX
      VALUENAME "NoFavorites"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!NoSelectDownloadDir CHECKBOX
      VALUENAME "NoSelectDownloadDir"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!NoBrowserContextMenu CHECKBOX
      VALUENAME "NoBrowserContextMenu"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!NoFindFiles CHECKBOX
      VALUENAME "NoFindFiles"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!GeneralTab CHECKBOX
      VALUENAME "GeneralTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!SecurityTab CHECKBOX
      VALUENAME "SecurityTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!ContentTab CHECKBOX
      VALUENAME "ContentTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!ConnectionsTab CHECKBOX
      VALUENAME "ConnectionsTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!ProgramsTab CHECKBOX
      VALUENAME "ProgramTabs"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!AdvancedTab CHECKBOX
      VALUENAME "AdvancedTab"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
END PART
PART !!CertifPers CHECKBOX
      VALUENAME "CertifPers"
      VALUEON NUMERIC 1
      VALUEOFF NUMERIC 0
```

```
                  END PART
                  PART !!SecChangeSettings CHECKBOX
                        VALUENAME "SecChangeSettings"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!SecAddSites CHECKBOX
                        VALUENAME "SecAddSites"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!FormSuggest CHECKBOX
                        VALUENAME "FormSuggest"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!FormSuggestPass CHECKBOX
                        VALUENAME "FormSuggest Pasword"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!ConnwizAdmin CHECKBOX
                        VALUENAME "Connwiz Admin Lock"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!IESettings CHECKBOX
                        VALUENAME "Settings"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!ResetWebSettings CHECKBOX
                        VALUENAME "ResetWebSettings"
                        VALUEON NUMERIC 1
                        VALUEOFF NUMERIC 0
                  END PART
                  PART !!Download CHECKBOX
                        KEYNAME "Software\Microsoft\Internet Explorer"
                        VALUENAME "Download Directory"
                        VALUEON "E:\"
                        VALUEOFF "A:\"
                  END PART

END POLICY
END CATEGORY

;CATEGORY !!Lumpkin_Printers
;POLICY !!HP_laser
;     KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Devices"
;     ACTIONLISTON
;           Valuename "\\STUBDC01\HP_laser" VALUE "winspool,Ne01:"
;           KEYNAME "Printers\Connections\,,STUBDC01,HP_laser"
;           Valuename "Provider" VALUE "win32spl.dll"
;           Valuename "Server" VALUE "\\STUBDC01"
;     END ACTIONLISTON
;     ACTIONLISTOFF
;           Valuename "\\STUBDC01\HP_laser" VALUE DELETE
;           KEYNAME "Printers\Connections\,,STUBDC01,HP_laser"
;           Valuename "Provider" VALUE DELETE
;           Valuename "Server" VALUE DELETE
;     END ACTIONLISTOFF
;END POLICY
;POLICY !!HP_Color
;     KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Devices"
;     ACTIONLISTON
;           Valuename "\\STUBDC01\HP_Color" VALUE "winspool,Ne00:"
;           KEYNAME "Printers\Connections\,,STUBDC01,HP_Color"
;           Valuename "Provider" VALUE "win32spl.dll"
;           Valuename "Server" VALUE "\\STUBDC01"
;     END ACTIONLISTON
;     ACTIONLISTOFF
;           Valuename "\\STUBDC01\HP_Color" VALUE DELETE
;           KEYNAME "Printers\Connections\,,STUBDC01,HP_Color"
;           Valuename "Provider" VALUE DELETE
;           Valuename "Server" VALUE DELETE
;     END ACTIONLISTOFF
;END POLICY
;POLICY !!HP1
;     KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Devices"
;     ACTIONLISTON
;           Valuename "\\STUBDC01\HP1" VALUE "winspool,Ne02:"
;           KEYNAME "Printers\Connections\,,STUBDC01,HP1"
;           Valuename "Provider" VALUE "win32spl.dll"
;           Valuename "Server" VALUE "\\STUBDC01"
;     END ACTIONLISTON
;     ACTIONLISTOFF
;           Valuename "\\STUBDC01\HP1" VALUE DELETE
;           KEYNAME "Printers\Connections\,,STUBDC01,HP1"
;           Valuename "Provider" VALUE DELETE
;           Valuename "Server" VALUE DELETE
;     END ACTIONLISTOFF
;END POLICY
;END CATEGORY



;from common.adm
*******************************************************************

CATEGORY !!ControlPanel
      CATEGORY !!CPL_Display
            POLICY !!CPL_Display_Restrict
            KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\System

                  PART !!CPL_Display_Disable                CHECKBOX
                  VALUENAME NoDispCPL
                  END PART

                  PART !!CPL_Display_HideBkgnd              CHECKBOX
                  VALUENAME NoDispBackgroundPage
                  END PART
                  PART !!CPL_Display_HideScrsav             CHECKBOX
                  VALUENAME NoDispScrSavPage
                  END PART

                  PART !!CPL_Display_HideAppearance         CHECKBOX
                  VALUENAME NoDispAppearancePage
                  END PART

                  PART !!CPL_Display_HideSettings           CHECKBOX
                  VALUENAME NoDispSettingsPage
                  END PART
            END POLICY
      END CATEGORY      ; Display

END CATEGORY      ; Control Panel

CATEGORY !!Desktop
      KEYNAME "Control Panel\Desktop"
      POLICY !!Wallpaper
                PART !!WallpaperName
EDITTEXT
                VALUENAME "Wallpaper"
                END PART
                PART !!WALLPAPER_TIP1                               TEXT
END PART
                PART !!WALLPAPER_TIP2                               TEXT
END PART

            PART !!TileWallpaper                           CHECKBOX
DEFCHECKED
            VALUENAME "TileWallpaper"
            VALUEON "1" VALUEOFF "0"
            END PART
      END POLICY

      POLICY !!ColorScheme
            PART !!SchemeName                              DROPDOWNLIST
            KEYNAME "Control Panel\Appearance"
            VALUENAME Current                                    REQUIRED
            ITEMLIST
                  NAME !!Lavender VALUE !!Lavender
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                        VALUENAME ActiveBorder         VALUE "174 168
217"
                        VALUENAME ActiveTitle          VALUE "128 128
128"
                        VALUENAME AppWorkspace         VALUE "90 78 177"
                        VALUENAME Background           VALUE "128 128
192"
                        VALUENAME ButtonDkShadow       VALUE "0 0 0"
                        VALUENAME ButtonFace           VALUE "174 168
217"
                        VALUENAME ButtonHilight        VALUE "216 213
236"
                        VALUENAME ButtonLight          VALUE "174 168
217"
```

```
                        VALUENAME ButtonShadow       VALUE "90 78 177"
                        VALUENAME ButtonText         VALUE "0 0 0"
                        VALUENAME GrayText           VALUE "90 78 177"
                        VALUENAME Hilight            VALUE "128 128
128"
                        VALUENAME HilightText        VALUE "255 255
255"
                        VALUENAME InactiveBorder     VALUE "174 168
217"
                        VALUENAME InactiveTitle      VALUE "90 78 177"
                        VALUENAME InactiveTitleText  VALUE "0 0 0"
                        VALUENAME Menu               VALUE "174 168
217"
                        VALUENAME MenuText           VALUE "0 0 0"
                        VALUENAME InfoText           VALUE "174 168
217"
                        VALUENAME InfoWindow         VALUE "0 0 0"
                        VALUENAME Scrollbar          VALUE "174 168
217"
                        VALUENAME TitleText          VALUE "255 255
255"
                        VALUENAME Window             VALUE "255 255
255"
                        VALUENAME WindowFrame        VALUE "0 0 0"
                        VALUENAME WindowText         VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!Tan256 VALUE !!Tan256
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                        VALUENAME ActiveBorder       VALUE "202 184
149"
                        VALUENAME ActiveTitle        VALUE "0 0 0"
                        VALUENAME AppWorkspace       VALUE "156 129
78"
                        VALUENAME Background         VALUE "128 64 64"
                        VALUENAME ButtonDkShadow     VALUE "0 0 0"
                        VALUENAME ButtonFace         VALUE "202 184
149"
                        VALUENAME ButtonHilight      VALUE "228 220
203"
                        VALUENAME ButtonLight        VALUE "202 184
149"
                        VALUENAME ButtonShadow       VALUE "156 129
78"
                        VALUENAME ButtonText         VALUE "0 0 0"
                        VALUENAME GrayText           VALUE "156 129
78"
                        VALUENAME Hilight            VALUE "0 0 0"
                        VALUENAME HilightText        VALUE "255 255
255"
                        VALUENAME InactiveBorder     VALUE "202 184
149"
                        VALUENAME InactiveTitle      VALUE "156 129
78"
                        VALUENAME InactiveTitleText  VALUE "0 0 0"
                        VALUENAME Menu                VALUE "202 184
149"
                        VALUENAME MenuText            VALUE "0 0 0"
                        VALUENAME InfoText            VALUE "202 184
149"
                        VALUENAME InfoWindow          VALUE "0 0 0"
                        VALUENAME Scrollbar           VALUE "202 184
149"
                        VALUENAME TitleText           VALUE "255 255
255"
                        VALUENAME Window              VALUE "255 255
255"
                        VALUENAME WindowFrame         VALUE "0 0 0"
                        VALUENAME WindowText          VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!Wheat256 VALUE !!Wheat256
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                        VALUENAME ActiveBorder        VALUE "215 213
170"
                        VALUENAME ActiveTitle         VALUE "0 0 0"
                        VALUENAME AppWorkspace        VALUE "173 169
82"
                        VALUENAME Background          VALUE "0 64 64"
                        VALUENAME ButtonDkShadow      VALUE "0 0 0"
                        VALUENAME ButtonFace          VALUE "215 213
170"
                        VALUENAME ButtonHilight       VALUE "235 234
214"
                        VALUENAME ButtonLight         VALUE "215 213
170"
                        VALUENAME ButtonShadow        VALUE "173 169
82"
                        VALUENAME ButtonText          VALUE "0 0 0"
                        VALUENAME GrayText            VALUE "173 169
82"
                        VALUENAME Hilight             VALUE "0 0 0"
                        VALUENAME HilightText         VALUE "255 255
255"
                        VALUENAME InactiveBorder      VALUE "215 213
170"
                        VALUENAME InactiveTitle       VALUE "173 169
82"
                        VALUENAME InactiveTitleText   VALUE "0 0 0"
                        VALUENAME Menu                VALUE "215 213
170"
                        VALUENAME MenuText            VALUE "0 0 0"
                        VALUENAME InfoText            VALUE "215 213
170"
                        VALUENAME InfoWindow          VALUE "0 0 0"
                        VALUENAME Scrollbar           VALUE "215 213
170"
                        VALUENAME TitleText           VALUE "255 255
255"
                        VALUENAME Window              VALUE "255 255
255"
```

```
                        VALUENAME WindowFrame          VALUE "0 0 0"
                        VALUENAME WindowText           VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!Celery VALUE !!Celery
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                        VALUENAME ActiveBorder         VALUE "168 215
170"
                        VALUENAME ActiveTitle          VALUE "0 0 0"
                        VALUENAME AppWorkspace         VALUE "80 175 85"
                        VALUENAME Background           VALUE "32 18 46"
                        VALUENAME ButtonDkShadow       VALUE "0 0 0"
                        VALUENAME ButtonFace           VALUE "168 215
170"
                        VALUENAME ButtonHilight        VALUE "211 235
213"
                        VALUENAME ButtonLight          VALUE "168 215
170"
                        VALUENAME ButtonShadow         VALUE "85 175 85"
                        VALUENAME ButtonText           VALUE "0 0 0"
                        VALUENAME GrayText             VALUE "80 175 85"
                        VALUENAME Hilight              VALUE "0 0 0"
                        VALUENAME HilightText          VALUE "255 255
255"
                        VALUENAME InactiveBorder       VALUE "168 215
170"
                        VALUENAME InactiveTitle        VALUE "80 175 75"
                        VALUENAME InactiveTitleText    VALUE "0 0 0"
                        VALUENAME Menu                 VALUE "168 215
170"
                        VALUENAME MenuText             VALUE "0 0 0"
                        VALUENAME InfoText             VALUE "168 215
170"
                        VALUENAME InfoWindow           VALUE "0 0 0"
                        VALUENAME Scrollbar            VALUE "168 215
170"
                        VALUENAME TitleText            VALUE "255 255
255"
                        VALUENAME Window               VALUE "255 255
255"
                        VALUENAME WindowFrame          VALUE "0 0 0"
                        VALUENAME WindowText           VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!Rose VALUE !!Rose
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                        VALUENAME ActiveBorder         VALUE "207 175
183"
                        VALUENAME ActiveTitle          VALUE "128 128
128"
                        VALUENAME AppWorkspace         VALUE "159 96
112"
                        VALUENAME Background           VALUE "128 64 64"
                        VALUENAME ButtonDkShadow       VALUE "0 0 0"
                        VALUENAME ButtonFace          VALUE "207 175
183"
                        VALUENAME ButtonHilight       VALUE "231 216
220"
                        VALUENAME ButtonLight         VALUE "207 175
183"
                        VALUENAME ButtonShadow        VALUE "159 96
112"
                                    VALUENAME ButtonText            VALUE
"0 0 0"
                        VALUENAME GrayText            VALUE "159 96
112"
                        VALUENAME Hilight             VALUE "128 128
128"
                        VALUENAME HilightText         VALUE "255 255
255"
                        VALUENAME InactiveBorder      VALUE "207 175
183"
                        VALUENAME InactiveTitle       VALUE "159 96
112"
                        VALUENAME InactiveTitleText   VALUE "0 0 0"
                        VALUENAME Menu                VALUE "207 175
183"
                        VALUENAME MenuText            VALUE "0 0 0"
                                VALUENAME InfoText              VALUE
"207 175 183"
                        VALUENAME InfoWindow          VALUE "0 0 0"
                        VALUENAME Scrollbar           VALUE "207 175
183"
                        VALUENAME TitleText           VALUE "255 255
255"
                        VALUENAME Window              VALUE "255 255
255"
                        VALUENAME WindowFrame         VALUE "0 0 0"
                        VALUENAME WindowText          VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!Evergreen VALUE !!Evergreen
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                                VALUENAME ActiveBorder
VALUE "47 151 109"
                                VALUENAME ActiveTitle
VALUE "0 0 0"
                                VALUENAME AppWorkspace
VALUE "31 101 73"
                                VALUENAME Background
VALUE "48 63 48"
                                VALUENAME ButtonDkShadow
VALUE "0 0 0"
                                VALUENAME ButtonFace
VALUE "47 151 109"
                                VALUENAME ButtonHilight
VALUE "137 218 186"
                                VALUENAME ButtonLight
VALUE "47 151 109"
```

```
                                VALUENAME ButtonShadow
VALUE "31 101 73"
                                VALUENAME ButtonText
VALUE "0 0 0"
                                VALUENAME GrayText
VALUE "31 101 73"
                                VALUENAME Hilight
VALUE "0 0 0"
                                VALUENAME HilightText
VALUE "255 255 255"
                                VALUENAME InactiveBorder
VALUE "47 151 109"
                                VALUENAME InactiveTitle
VALUE "31 101 73"
                                VALUENAME InactiveTitleText
VALUE "0 0 0"
                                VALUENAME Menu
VALUE "47 151 109"
                                VALUENAME MenuText
VALUE "0 0 0"
                                VALUENAME InfoText
VALUE "47 151 109"
                                VALUENAME InfoWindow
VALUE "0 0 0"
                                VALUENAME Scrollbar
VALUE "47 151 109"
                                VALUENAME TitleText
VALUE "255 255 255"
                                VALUENAME Window
VALUE "255 255 255"
                                VALUENAME WindowFrame
VALUE "0 0 0"
                                VALUENAME WindowText
VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!Blues VALUE !!Blues
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                                VALUENAME ActiveBorder
VALUE "161 198 221"
                                VALUENAME ActiveTitle
VALUE "0 0 0"
                                VALUENAME AppWorkspace
VALUE "69 139 186"
                                VALUENAME Background
VALUE "0 0 64"
                                VALUENAME ButtonDkShadow
VALUE "0 0 0"
                                VALUENAME ButtonFace
VALUE "164 198 221"
                                VALUENAME ButtonHilight
VALUE "210 227 238"
                                VALUENAME ButtonLight
VALUE "164 198 221"
                                VALUENAME ButtonShadow
VALUE "69 139 186"
```

```
                                VALUENAME ButtonText
VALUE "0 0 0"
                                VALUENAME GrayText
VALUE "69 139 186"
                                VALUENAME Hilight
VALUE "0 0 0"
                                VALUENAME HilightText
VALUE "255 255 255"
                                VALUENAME InactiveBorder
VALUE "164 198 221"
                                VALUENAME InactiveTitle
VALUE "69 139 186"
                                VALUENAME InactiveTitleText
VALUE "0 0 0"
                                VALUENAME Menu
VALUE "164 198 221"
                                VALUENAME MenuText
VALUE "0 0 0"
                                VALUENAME InfoText
VALUE "164 198 221"
                                VALUENAME InfoWindow
VALUE "0 0 0"
                                VALUENAME Scrollbar
VALUE "164 198 221"
                                VALUENAME TitleText
VALUE "255 255 255"
                                VALUENAME Window
VALUE "255 255 255"
                                VALUENAME WindowFrame
VALUE "0 0 0"
                                VALUENAME WindowText
VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!Teal VALUE !!Teal
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                                VALUENAME ActiveBorder
VALUE "192 192 192"
                                VALUENAME ActiveTitle
VALUE "0 128 128"
                                VALUENAME AppWorkspace
VALUE "128 128 128"
                                VALUENAME Background
VALUE "0 64 64"
                                VALUENAME ButtonDkShadow
VALUE "0 0 0"
                                VALUENAME ButtonFace
VALUE "192 192 192"
                                VALUENAME ButtonHilight
VALUE "255 255 255"
                                VALUENAME ButtonLight
VALUE "192 192 192"
                                VALUENAME ButtonShadow
VALUE "128 128 128"
                                VALUENAME ButtonText
VALUE "0 0 0"
```

```
                               VALUENAME GrayText
VALUE "128 128 128"
                               VALUENAME Hilight
VALUE "0 128 128"
                               VALUENAME HilightText
VALUE "255 255 255"
                               VALUENAME InactiveBorder
VALUE "192 192 192"
                               VALUENAME InactiveTitle
VALUE "192 192 192"
                               VALUENAME InactiveTitleText
VALUE "0 0 0"
                               VALUENAME Menu
VALUE "192 192 192"
                               VALUENAME MenuText
VALUE "0 0 0"
                               VALUENAME InfoText
VALUE "192 192 192"
                               VALUENAME InfoWindow
VALUE "0 0 0"
                               VALUENAME Scrollbar
VALUE "192 192 192"
                               VALUENAME TitleText
VALUE "0 0 0"
                               VALUENAME Window
VALUE "255 255 255"
                               VALUENAME WindowFrame
VALUE "0 0 0"
                               VALUENAME WindowText
VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!TheReds VALUE !!TheReds
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                               VALUENAME ActiveBorder
VALUE "192 192 192"
                               VALUENAME ActiveTitle
VALUE "128 0 0"
                               VALUENAME AppWorkspace
VALUE "128 128 128"
                               VALUENAME Background
VALUE "64 0 0"
                               VALUENAME ButtonDkShadow
VALUE "0 0 0"
                               VALUENAME ButtonFace
VALUE "192 192 192"
                               VALUENAME ButtonHilight
VALUE "255 255 255"
                               VALUENAME ButtonLight
VALUE "192 192 192"
                               VALUENAME ButtonShadow
VALUE "128 128 128"
                               VALUENAME ButtonText
VALUE "0 0 0"
                               VALUENAME GrayText
VALUE "128 128 128"
```

```
                                VALUENAME Hilight
VALUE "128 0 0"
                                VALUENAME HilightText
VALUE "255 255 255"
                                VALUENAME InactiveBorder
VALUE "192 192 192"
                                VALUENAME InactiveTitle
VALUE "192 192 192"
                                VALUENAME InactiveTitleText
VALUE "0 0 0"
                                VALUENAME Menu
VALUE "192 192 192"
                                VALUENAME MenuText
VALUE "0 0 0"
                                VALUENAME InfoText
VALUE "192 192 192"
                                VALUENAME InfoWindow
VALUE "0 0 0"
                                VALUENAME Scrollbar
VALUE "192 192 192"
                                VALUENAME TitleText
VALUE "255 255 255"
                                VALUENAME Window
VALUE "255 255 255"
                                VALUENAME WindowFrame
VALUE "0 0 0"
                                VALUENAME WindowText
VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!WindowsDefault VALUE !!WindowsDefault
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                                VALUENAME ActiveBorder
VALUE "192 192 192"
                                VALUENAME ActiveTitle
VALUE "0 0 128"
                                VALUENAME AppWorkspace
VALUE "128 128 128"
                                VALUENAME Background
VALUE "0 128 128"
                                VALUENAME ButtonDkShadow
VALUE "0 0 0"
                                VALUENAME ButtonFace
VALUE "192 192 192"
                                VALUENAME ButtonHilight
VALUE "255 255 255"
                                VALUENAME ButtonLight
VALUE "192 192 192"
                                VALUENAME ButtonShadow
VALUE "128 128 128"
                                VALUENAME ButtonText
VALUE "0 0 0"
                                VALUENAME GrayText
VALUE "128 128 128"
                                VALUENAME Hilight
VALUE "0 0 128"
```

```
                                VALUENAME HilightText
VALUE "255 255 255"
                                VALUENAME InactiveBorder
VALUE "192 192 192"
                              VALUENAME InactiveTitle          VALUE
"192 192 192"
                                VALUENAME InactiveTitleText
VALUE "0 0 0"
                                VALUENAME Menu
VALUE "192 192 192"
                                VALUENAME MenuText
VALUE "0 0 0"
                                VALUENAME InfoText
VALUE "192 192 192"
                                VALUENAME InfoWindow
VALUE "0 0 0"
                                VALUENAME Scrollbar
VALUE "192 192 192"
                                VALUENAME TitleText
VALUE "255 255 255"
                                VALUENAME Window
VALUE "255 255 255"
                                VALUENAME WindowFrame
VALUE "0 0 0"
                                VALUENAME WindowText
VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!BlueAndBlack VALUE !!BlueAndBlack
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                                VALUENAME ActiveBorder
VALUE "192 192 192"
                                VALUENAME ActiveTitle
VALUE "0 0 0"
                                VALUENAME AppWorkspace
VALUE "128 128 128"
                                VALUENAME Background
VALUE "0 0 128"
                                VALUENAME ButtonDkShadow
VALUE "0 0 0"
                                VALUENAME ButtonFace
VALUE "192 192 192"
                                VALUENAME ButtonHilight
VALUE "255 255 255"
                                VALUENAME ButtonLight
VALUE "192 192 192"
                                VALUENAME ButtonShadow
VALUE "128 128 128"
                                VALUENAME ButtonText
VALUE "0 0 0"
                                VALUENAME GrayText
VALUE "128 128 128"
                                VALUENAME Hilight
VALUE "255 255 0"
                                VALUENAME HilightText
VALUE "0 0 0"
```

```
                               VALUENAME InactiveBorder
VALUE "192 192 192"
                             VALUENAME InactiveTitle           VALUE
"192 192 192"
                               VALUENAME InactiveTitleText
VALUE "0 0 0"
                               VALUENAME Menu
VALUE "192 192 192"
                               VALUENAME MenuText
VALUE "0 0 0"
                               VALUENAME InfoText
VALUE "192 192 192"
                               VALUENAME InfoWindow
VALUE "0 0 0"
                               VALUENAME Scrollbar
VALUE "192 192 192"
                               VALUENAME TitleText
VALUE "255 255 255"
                               VALUENAME Window
VALUE "255 255 255"
                               VALUENAME WindowFrame
VALUE "0 0 0"
                               VALUENAME WindowText
VALUE "0 0 0"
                  END ACTIONLIST

                  NAME !!Wheat VALUE !!Wheat
                  ACTIONLIST
                        KEYNAME "Control Panel\Colors"
                               VALUENAME ActiveBorder
VALUE "192 192 192"
                               VALUENAME ActiveTitle
VALUE "128 128 0"
                               VALUENAME AppWorkspace
VALUE "128 128 128"
                               VALUENAME Background
VALUE "128 128 64"
                               VALUENAME ButtonDkShadow
VALUE "0 0 0"
                               VALUENAME ButtonFace
VALUE "192 192 192"
                               VALUENAME ButtonHilight
VALUE "255 255 255"
                               VALUENAME ButtonLight
VALUE "192 192 192"
                               VALUENAME ButtonShadow
VALUE "128 128 128"
                               VALUENAME ButtonText
VALUE "0 0 0"
                               VALUENAME GrayText
VALUE "128 128 128"
                               VALUENAME Hilight
VALUE "128 128 0"
                               VALUENAME HilightText
VALUE "0 0 0"
                               VALUENAME InactiveBorder
VALUE "192 192 192"
```

```
                                  VALUENAME InactiveTitle
VALUE "192 192 192"
                                  VALUENAME InactiveTitleText
VALUE "0 0 0"
                                  VALUENAME Menu
VALUE "192 192 192"
                                  VALUENAME MenuText
VALUE "0 0 0"
                                  VALUENAME InfoText
VALUE "192 192 192"
                                  VALUENAME InfoWindow
VALUE "0 0 0"
                                  VALUENAME Scrollbar
VALUE "192 192 192"
                                  VALUENAME TitleText
VALUE "0 0 0"
                                  VALUENAME Window
VALUE "255 255 255"
                                  VALUENAME WindowFrame
VALUE "0 0 0"
                                  VALUENAME WindowText
VALUE "0 0 0"
                   END ACTIONLIST
             END ITEMLIST
             END PART
       END POLICY
 END CATEGORY     ; Desktop

CATEGORY !!Shell
       CATEGORY !!Restrictions
             KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
                   POLICY !!RemoveRun
                   VALUENAME "NoRun"
                   END POLICY

                   POLICY !!RemoveFolders
                   VALUENAME "NoSetFolders"
                   END POLICY

                   POLICY !!RemoveTaskbar
                   VALUENAME "NoSetTaskbar"
                   END POLICY

                   POLICY !!RemoveFind
                   VALUENAME "NoFind"
                   END POLICY

                   POLICY !!HideNetHood
                   VALUENAME "NoNetHood"
                   END POLICY

                   POLICY !!NoEntireNetwork
                   KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\Network
                   VALUENAME "NoEntireNetwork"
                   END POLICY
```

```
                  POLICY !!NoWorkgroupContents
                  KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\Network
                  VALUENAME "NoWorkgroupContents"
                  END POLICY

                  POLICY !!HideDesktop
                  VALUENAME "NoDesktop"
                  END POLICY

                  POLICY !!DisableClose
                  VALUENAME "NoClose"
                  END POLICY

                  POLICY !!NoSaveSettings
                  VALUENAME "NoSaveSettings"
                  END POLICY
      END CATEGORY
END CATEGORY      ; Shell

CATEGORY !!System
KEYNAME Software\Microsoft\Windows\CurrentVersion\Policies\System
      CATEGORY !!Restrictions
            POLICY !!DisableRegedit
            VALUENAME DisableRegistryTools
            END POLICY

            POLICY !!RestrictApps
            KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
            VALUENAME RestrictRun
            PART !!RestrictAppsList LISTBOX
            KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun
            VALUEPREFIX ""
            END PART
            PART !!RestrictApps_Tip1                  TEXT  END PART
            PART !!RestrictApps_Tip2                  TEXT  END PART
            PART !!RestrictApps_Tip3                  TEXT  END PART
            PART !!RestrictApps_Tip4                  TEXT  END PART
            END POLICY
      END CATEGORY
END CATEGORY      ; System


;from winnt.adm
**********************************************************************

CATEGORY !!Shell

        CATEGORY !!CustomShell
                KEYNAME "Software\Microsoft\Windows
NT\CurrentVersion\Winlogon"

                POLICY !!ShellName
                        PART !!ShellNameInst         EDITTEXT REQUIRED
                        VALUENAME "Shell"
                        END PART
                END POLICY


        END CATEGORY


        CATEGORY !!CustomFolders
                KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"

                POLICY !!CustomFolders_Programs
                        PART !!CustomFolders_ProgramsPath
EDITTEXT REQUIRED EXPANDABLETEXT
                        DEFAULT !!CustomFolders_ProgramsDefault
                        VALUENAME "Programs"
                        END PART
                END POLICY

                POLICY !!CustomFolders_Desktop
                        PART !!CustomFolders_DesktopPath
EDITTEXT REQUIRED  EXPANDABLETEXT
                        DEFAULT !!CustomFolders_DesktopDefault
                        VALUENAME "Desktop"
                        END PART
                END POLICY

                POLICY !!HideStartMenuSubfolders
                        KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
                        VALUENAME NoStartMenuSubFolders
                        PART !!HideStartMenuSubfolders_Tip1
TEXT  END PART
                        PART !!HideStartMenuSubfolders_Tip2
TEXT  END PART
                END POLICY

                POLICY !!CustomFolders_Startup
                        PART !!CustomFolders_StartupPath
EDITTEXT REQUIRED  EXPANDABLETEXT
                        DEFAULT !!CustomFolders_StartupDefault
                        VALUENAME "Startup"
                        END PART
                END POLICY

                POLICY !!CustomFolders_NetHood
                        PART !!CustomFolders_NetHoodPath
EDITTEXT REQUIRED  EXPANDABLETEXT
                        DEFAULT !!CustomFolders_NetHoodDefault
                        VALUENAME "NetHood"
                        END PART
                END POLICY

                POLICY !!CustomFolders_StartMenu
                        PART !!CustomFolders_StartMenuPath
EDITTEXT REQUIRED  EXPANDABLETEXT
```

```
                        DEFAULT !!CustomFolders_StartMenuDefault
                        VALUENAME "Start Menu"
                        END PART
                END POLICY

        END CATEGORY

        CATEGORY !!Restrictions
                KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
                        POLICY !!ApprovedShellExt
                        VALUENAME "EnforceShellExtensionSecurity"
                        END POLICY

                        POLICY !!NoOptions
                        VALUENAME "NoOptions"
                        END POLICY

                        POLICY !!NoGoTo
                        VALUENAME "NoGoTo"
                        END POLICY

                        POLICY !!NoFileMenu
                        VALUENAME "NoFileMenu"
                        END POLICY

                        POLICY !!NoCommonGroups
                        VALUENAME "NoCommonGroups"
                        END POLICY

                        POLICY !!NoTrayContextMenu
                        VALUENAME "NoTrayContextMenu"
                        END POLICY

                        POLICY !!NoViewContextMenu
                        VALUENAME "NoViewContextMenu"
                        END POLICY

                        POLICY !!NoNetConnectDisconnect
                        VALUENAME "NoNetConnectDisconnect"
                        END POLICY

                        POLICY !!DisableLinkTracking
                        VALUENAME "LinkResolveIgnoreLinkInfo"
                        END POLICY
        END CATEGORY

END CATEGORY    ; Shell

CATEGORY  !!System
      POLICY !!Parse_Autoexec
      KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Winlogon"
            VALUENAME ParseAutoexec
            VALUEON "1"  VALUEOFF "0"
            PART !!Parse_Tip1                        TEXT  END PART
            PART !!Parse_Tip2                        TEXT  END PART
      END POLICY

        POLICY !!Run_Logon_Script_Sync
        KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Winlogon"
                VALUENAME RunLogonScriptSync
                PART !!Script_Tip1
TEXT    END PART
                PART !!Script_Tip2
TEXT    END PART
                PART !!Script_Tip3
TEXT    END PART
        END POLICY

        POLICY !!DisableLogoff
        KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
        VALUENAME "NoLogoff"
        END POLICY

        POLICY !!DisableTaskMgr
        KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\System
        VALUENAME "DisableTaskMgr"
        END POLICY

        POLICY !!DisableLockWorkstation
        KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\System
        VALUENAME "DisableLockWorkstation"
        END POLICY

        POLICY !!DisableChangePassword
        KEYNAME
Software\Microsoft\Windows\CurrentVersion\Policies\System
        VALUENAME "DisableChangePassword"
        END POLICY

        POLICY !!ShowWelcome
        KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Explorer\Tips"
        VALUENAME "Show"
        VALUEON  NUMERIC 1
        VALUEOFF NUMERIC 0
        END POLICY

END CATEGORY

CATEGORY  !!UserProfiles
        POLICY !!LimitSize
                KEYNAME
"Software\Microsoft\Windows\CurrentVersion\Policies\System"
                VALUENAME EnableProfileQuota

                PART !!SizeMessage                      EDITTEXT
                DEFAULT !!DefaultSizeMessage
                VALUENAME "ProfileQuotaMessage"
                END PART
                PART !!ProfileSize                   NUMERIC REQUIRED
SPIN 100
                DEFAULT 30000
                MAX    30000
                MIN    300
                VALUENAME "MaxProfileSize"
                END PART

                PART !!IncludeRegInProQuota          CHECKBOX
                VALUENAME "IncludeRegInProQuota"
                END PART

                PART !!WarnUser                      CHECKBOX
                VALUENAME "WarnUser"
                END PART

                PART !!WarnUserTimeout               NUMERIC REQUIRED
SPIN 5
                DEFAULT 15
                MIN    0
                VALUENAME "WarnUserTimeout"
                END PART

        END POLICY

        POLICY !!ExcludeDirectories
                KEYNAME "Software\Policies\Microsoft\Windows\System"

                PART !!ExcludeMessage                EDITTEXT
                DEFAULT !!DefaultExcludeMessage
                VALUENAME "ExcludeProfileDirs"
                END PART

                PART !!Exclude_Tip1                  TEXT  END PART
                PART !!Exclude_Tip2                  TEXT  END PART

        END POLICY

END CATEGORY


; String Definitions
*****************************************************************


[STRINGS]

ActiveDesktop="Disable the Active Desktop"
NoSet="No Setting Active Desktop"
NoActive="No Active Desktop"
Wallpaper="Disable Set as Wallpaper"
WallpaperTip="This disables the ability to set a picture as wallpaper"
PersonalTip="This changes the location of Personal Files to
E:\Personal"
PersonalFiles="Location for Personal Files"
```

```
MyPicturesTip="This changes the location of My Pictures Files to E:\My
Pictures"
MyPictures="Location for My Pictures Files"
DesktopTip="This changes the location of Desktop Files to E:\Desktop"
Desktop="Location for Desktop Files"
RecentTip="This changes the location of Recent Files to E:\Recent"
Recent="Location for Recent Files"
LumpkinIENT="Internet Explorer Policy for NT"
LumpkinIE2K="Internet Explorer Policy for 2000"
NoFileOpen="No File Open"
NoFileNew="No New File"
NoBrowserSaveAs="No Browser Save As"
NoBrowserOptions="No Browser Options"
NoFavorites="No Favorites"
NoSelectDownloadDir="No Selection of Download Directory"
NoBrowserContextMenu="No Browser Context Menu"
NoFindFiles="No Find Files"
GeneralTab="Remove General Tab"
SecurityTab="Remove Security Tab"
ContentTab="Remove Content Tab"
ConnectionsTab="Remove Connections Tab"
ProgramsTab="Remove Programs Tab"
AdvancedTab="Remove Advanced Tab"
CertifPers="Remove Personal Tab"
SecChangeSettings="Remove Security Tab"
SecAddSites="Remove ability to add security sites"
FormSuggest="Disable autocomplete forms"
FormSuggestPass="Disable prompt for saving passwords"
ConnwizAdmin="Disable connection wizard"
IESettings="Prevent changes to Temporary Internet File Settings"
ResetWebSettings="Disable ability to reset to default settings"
Download="Set download location to E:"
Lumpkin_Printers="Lumpkin Hall Printers"
HP_laser="HP_laser"
HP_Color="HP_Color"
HP1="HP1"
HP_laser_Device="Add Device HP_laser"
HP_laser="Add HP_laser to the available printers"
HP_Color_Device="Add Device HP_Color"
HP_Color="Add HP_Color to the available printers"
HP1_Device="Add Device HP1"
HP1="Add HP1 to the available printers"
Logon="Roaming Profile/Auto Logon Settings"
AutoLogon="Allow Auto Logon"
DeleteCache="Delete Roaming Cache"
Lumpkin="Lumpkin Hall Security"
hidedrives="Hide Drives"
ACDEFGHY="Show only drives A, C, D, E, F, G, H and Y"
ADEGHY="Show only drives A, D, E, F, H and Y"
AEFGHY="Show only drives A, E, F, G, H and Y"
CLEARALL="Do not hide any drives"
hidedrivestext1="Hide one or more drives from My Computer and Explorer
hidedrivestext2="Note:  Do not use with other Hide Drive policies"
PolicyPointer="Policy Update Location"
PolicyLocation="Policy Update Location"
Stubdc01_NT="\\stubdc01\lumpkin\lumpkin.pol"
Stubdc01_2000="\\stubdc01\lump2000\lump2000.pol"
```

```
Stubdc06_NT="\\stubdc06\lumpkin\lumpkin.pol"
Stubdc06_2000="\\stubdc06\lump2000\lump2000.pol"
Update="Update manually using Policy Update Location"
;common.adm
Network="Network"
Update="System policies update"
RemoteUpdate="Remote update"
UpdateMode="Update mode"
UM_Automatic="Automatic (use default path)"
UM_Manual="Manual (use specific path)"
UM_Manual_Path="Path for manual update"
DisplayErrors="Display error messages"
LoadBalance="Load balancing"
System="System"
DisableFileSharing="Disable file sharing"
DisablePrintSharing="Disable print sharing"
ControlPanel="Control Panel"
CPL_Display="Display"
CPL_Display_Restrict="Restrict display"
CPL_Display_Disable="Deny access to display icon"
CPL_Display_HideBkgnd="Hide Background tab"
CPL_Display_HideScrsav="Hide Screen Saver tab"
CPL_Display_HideAppearance="Hide Appearance tab"
CPL_Display_HideSettings="Hide Settings tab"
Desktop="Desktop"
Wallpaper="Wallpaper"
WallpaperName="Wallpaper Name"
TileWallpaper="Tile Wallpaper"
Wallpaper_Tip1="Specifiy location and name (e.g.
c:\winnt\winnt256.bmp)"
Wallpaper_Tip2="  "
ColorScheme="Color scheme"
SchemeName="Scheme name"
Lavender="Lavender 256"
Celery="Celery 256"
Rose="Rose 256"
Evergreen="Evergreen 256"
Blues="Blues 256"
WindowsDefault="Windows Default"
BlueAndBlack="Blue and Black"
Teal="Teal"
TheReds="The Reds"
Wheat="Wheat"
Wheat256="Wheat 256"
Tan256="Tan 256"
Shell="Shell"
RemoveRun="Remove Run command from Start menu"
RemoveFolders="Remove folders from Settings on Start menu"
RemoveTaskbar="Remove Taskbar from Settings on Start menu"
RemoveFind="Remove Find command from Start menu"
HideDrives="Hide drives in My Computer"
HideNetHood="Hide Network Neighborhood"
NoEntireNetwork="No Entire Network in Network Neighborhood"
HideDesktop="Hide all items on desktop"
DisableClose="Remove Shut Down command from Start menu"
NoSaveSettings="Don't save settings at exit"
Restrictions="Restrictions"
```

```
DisableRegedit="Disable Registry editing tools"
Run="Run"
RunServices="Run services"
RunListbox="Items to run at startup"
RunServicesListbox="Services to run at startup"
NoWorkgroupContents="No workgroup contents in Network Neighborhood"
RestrictApps="Run only allowed Windows applications"
RestrictAppsList="List of allowed applications"
RestrictApps_Tip1="     "
RestrictApps_Tip2="To create a list of allowed applications, click
Show,"
RestrictApps_Tip3="then Add, and enter the application executable name"
RestrictApps_Tip4="(e.g., Winword.exe, Poledit.exe, Powerpnt.exe)."
DomainLogonConfirmation="Display domain logon confirmation"
NoDomainPwdCaching="Disable caching of domain password"
;winnt.adm
Network="Windows NT Network"
Sharing="Sharing"
WorkstationShareAutoCreate="Create hidden drive shares (workstation)"
ServerShareAutoCreate="Create hidden drive shares (server)"
ShareWks_Tip1=Automatically create <drive letter>$ and Admin$ shares
ShareWks_Tip2=when Windows NT Workstation starts.
ShareServer_Tip1=Automatically create <drive letter>$ and Admin$ shares
ShareServer_Tip2=when Windows NT Server starts.
System="Windows NT System"
Login_Policies="Logon"
LogonBanner="Logon banner"
LogonBanner_Caption="Caption"
LogonBanner_Text="Text"
LogonBanner_DefCaption="Important Notice:"
LogonBanner_DefText="Do not attempt to log on unless you are an
authorized user."
Shutdown_Restrict="Enable shutdown from Authentication dialog box"
Shutd_Tip1="When this box is checked, you can click Shut Down"
Shutd_Tip2="in the Authentication dialog box to select options."
Shutd_Tip3="Default: NT Server = Off, NT Workstation = On"
LastUserName_Restrict="Do not display last logged on user name"
Dont_Display_Tip1="When this box is checked, Windows NT does not"
Dont_Display_Tip2="automatically display the user name of the last
person"
Dont_Display_Tip3="to log on in the Authentication dialog box."
Printers="Windows NT Printers"
PrintManager_Browser_Restrict="Disable browse thread on this computer"
Disable_Server_Tip1="When this box is checked, the print spooler does
not"
Disable_Server_Tip2="send shared printer information to other print
servers."
Scheduler_Thread_Priority="Scheduler priority"
Scheduler_Priority="Priority"
Thread_Priority_Above_Normal="Scheduler priority above normal"
Thread_Priority_Below_Normal="Scheduler priority below normal"
Thread_Priority_Normal="Scheduler priority normal"
Beep_Enabled="Beep for error enabled"
Beep_Tip1="A check in this box enables beeping (every 10 seconds) when
a remote"
Beep_Tip2="job error occurs on a print server."
RemoteAccess="Windows NT Remote Access"
```

```
MaximumRetries="Max number of unsuccessful authentication retries"
RAS_Length="Number of retries"
MaximumTime="Max time limit for authentication"
RAS_Time="Length in seconds"
CallBackTime="Wait interval for callback"
INT_Time="Length in seconds"
Auto_Disconnect="Auto Disconnect"
Autodisconnect_Time="Disconnect after (minutes)"
UserProfiles="Windows NT User Profiles"
DeleteRoamingCachedProfiles="Delete cached copies of roaming profiles"
DeleteCache_Tip1="When users with roaming profiles log off,"
DeleteCache_Tip2="delete the locally cached profile (to save disk
space)."
EnableSlowLinkDetect="Automatically detect slow network connections"
SlowLinkTimeOut="Slow network connection timeout"
SlowLinkWaitInterval="Time (milliseconds)"
ProfileDlgTimeOut="Timeout for dialog boxes"
ProfileDlgWaitInterval="Time (seconds)"
Parse_Autoexec="Parse Autoexec.bat"
Parse_Tip1="When this box is checked, environment variables declared"
Parse_Tip2="in autoexec.bat are included in the users environment."
Shell="Windows NT Shell"
CustomFolders="Custom folders"
CustomFolders_Programs="Custom Programs folder"
CustomFolders_ProgramsPath="Path to location of Programs items"
CustomFolders_ProgramsDefault="%USERPROFILE%\Start Menu\Programs"
CustomFolders_Desktop="Custom desktop icons"
CustomFolders_DesktopPath="Path to location of desktop icons"
CustomFolders_DesktopDefault="%USERPROFILE%\Desktop"
HideStartMenuSubfolders="Hide Start menu subfolders"
HideStartMenuSubfolders_Tip1="Check this if you use a custom Programs
folder"
HideStartMenuSubfolders_Tip2="or custom desktop icons."
CustomFolders_Startup="Custom Startup folder"
CustomFolders_StartupPath="Path to location of Startup items"
CustomFolders_StartupDefault="%USERPROFILE%\Start
Menu\Programs\Startup"
CustomFolders_NetHood="Custom Network Neighborhood"
CustomFolders_NetHoodPath="Path to location of Network Neighborhood
items"
CustomFolders_NetHoodDefault="%USERPROFILE%\NetHood"
CustomFolders_StartMenu="Custom Start menu"
CustomFolders_StartMenuPath="Path to location of Start menu items"
CustomFolders_StartMenuDefault="%USERPROFILE%\Start Menu"
CustomSharedFolders="Custom shared folders"
CustomFolders_SharedPrograms="Custom shared Programs folder"
CustomFolders_SharedProgramsPath="Path to location of shared Programs
items"
CustomFolders_SharedProgramsDefault="%SystemRoot%\Profiles\All
Users\Start Menu\Programs"
CustomFolders_SharedDesktop="Custom shared desktop icons"
CustomFolders_SharedDesktopPath="Path to location of shared desktop
icons"
CustomFolders_SharedDesktopDefault="%SystemRoot%\Profiles\All
Users\Desktop"
CustomFolders_SharedStartMenu="Custom shared Start menu"
```

```
CustomFolders_SharedStartMenuPath="Path to location of shared Start
menu items"
CustomFolders_SharedStartMenuDefault="%SystemRoot%\Profiles\All
Users\Start Menu"
CustomFolders_SharedStartup="Custom shared Startup folder"
CustomFolders_SharedStartupPath="Path to location of shared Startup
items"
CustomFolders_SharedStartupDefault="%SystemRoot%\Profiles\All
Users\Start Menu\Programs\Startup"
Restrictions="Restrictions"
ApprovedShellExt="Only use approved shell extensions"
NoOptions="Remove View->Options menu from Explorer"
NoGoTo="Remove Tools->GoTo menu from Explorer"
NoFileMenu="Remove File menu from Explorer"
NoCommonGroups="Remove common program groups from Start menu"
FileSystem="File system"
Disable8dot3Names="Do not create 8.3 file names for long file names"
AllowExtCharsIn8dot3="Allow extended characters in 8.3 file names"
ExtChars_Tip1="Short file names with extended characters may not be
viewable"
ExtChars_Tip2="on computers that do not have same character code page."
DisableLastUpdate="Do not update last access time"
LastAccess_Tip1="For files that are only being read, do not update the
last"
LastAccess_Tip2="access time.  This will increase the file system's
performance."
Run_Logon_Script_Sync="Run logon scripts synchronously."
Script_Tip1="Wait for the logon scripts to complete before starting"
Script_Tip2="the users's shell.  If this value is also set in the"
Script_Tip3="Computer section, that value takes precedence."
Script_Tip4="User section, this value takes precedence."
NoTrayContextMenu="Disable context menus for the taskbar"
NoViewContextMenu="Disable Explorer's default context menu"
NoNetConnectDisconnect="Remove the "Map Network Drive" and "Disconnect
Network Drive" options"
DisableLogoff="Disable Logoff"
DisableTaskMgr="Disable Task Manager"
DisableLockWorkstation="Disable Lock Workstation"
DisableChangePassword="Disable Change Password"
DisableLinkTracking="Disable link file tracking"
ShowWelcome="Show welcome tips at logon"
CustomShell="Custom user interface"
ShellName="Custom shell"
ShellNameInst="Shell name (eg: explorer.exe)"
SlowLinkDefault="Slow network default profile operation"
ChooseProfileDefault="Choose profile default operation"
DefaultOperation="Default option"
PD_DOWNLOAD="Download profile"
PD_USELOCAL="Use local profile"
LimitSize="Limit profile size"
SizeMessage="Custom Message"
DefaultSizeMessage="You have exceeded your profile storage space.
Before you can log off, you need to move some items from your profile
to network or local storage."
ProfileSize="Max Profile size (KB)"
IncludeRegInProQuota="Include registry in file list"
WarnUser="Notify user when profile storage space is exceeded."
```

```
WarnUserTimeout="Remind user every X minutes:"
ExcludeDirectories="Exclude directories in roaming profile"
ExcludeMessage="Prevent the following directories from roaming with the
profile:"
DefaultExcludeMessage="Temporary Internet Files;Temp"
Exclude_Tip1="You can enter multiple directory names, semi-colon
separated,"
Exclude_Tip2="all relative to the root of the user's profile"
```

APPENDIX D

Windows 2000 Setup Procedures

Windows 2000 Install Instructions

Turn on Power
Press F1 to enter BIOS
Password (see Administrator)

Settings should be as follows:

Main:
Leave all defaults

Advanced:
Plug+Play = No
Reset config data = No
Num Lock = On

Security:
User password = clear
Supervisor password = Set (see Administrator)

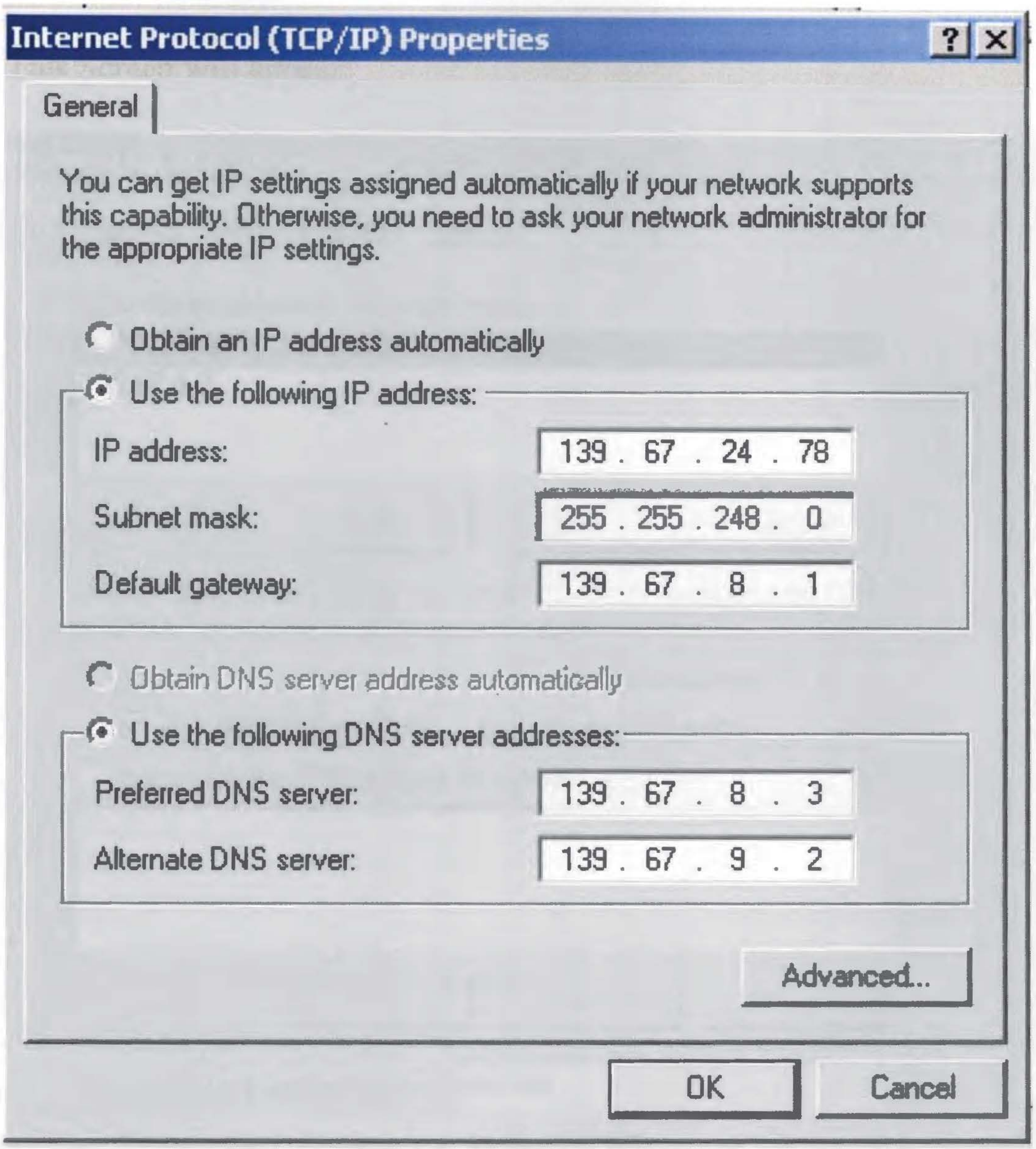
Power:
Power Management = Enabled
Hard drive = Disabled
VESA = Standby
Fan Always On = Yes
Power Button = On/Off

Boot:
Silent Boot = Enabled
Quick Boot = Enabled
Scan user flash area = Disabled
After power failure = Last state
On Modem Ring = Stay off
On LAN = stay on
On PME = stay off
First Boot = Hard Drive (CD-ROM for installation)
Second Boot = CD-Rom (Hard Drive for installation)
Third Boot = Removable devices

Put in Operating System Backup CD and press F10 (yes to accept)
Press any key to start from CD

At welcome screen press Enter to setup Windows 2000
Press F8 to agree to license
Press ESC to not repair
Delete all partitions by highlighting and pressing D
    -Then press Enter followed by L
Press C to create a new partition
    -10001MB partition
Highlight C partition and press Enter to setup Windows 2000
Format NTFS
At regional settings click Next
Put the Tag#eiu as Name and Eastern Illinois University as the organization
Enter the product key from spreadsheet
Computer Name : Tag#eiu
Admin Password : (See Administrator)
Central Time Zone
Choose custom Network Settings
Add protocol NetBEUI
Highlight TCP/IP and click properties

This screen will appear:



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 139 . 67 . 24 . 78

Subnet mask: 255 . 255 . 248 . 0

Default gateway: 139 . 67 . 8 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 139 . 67 . 8 . 3

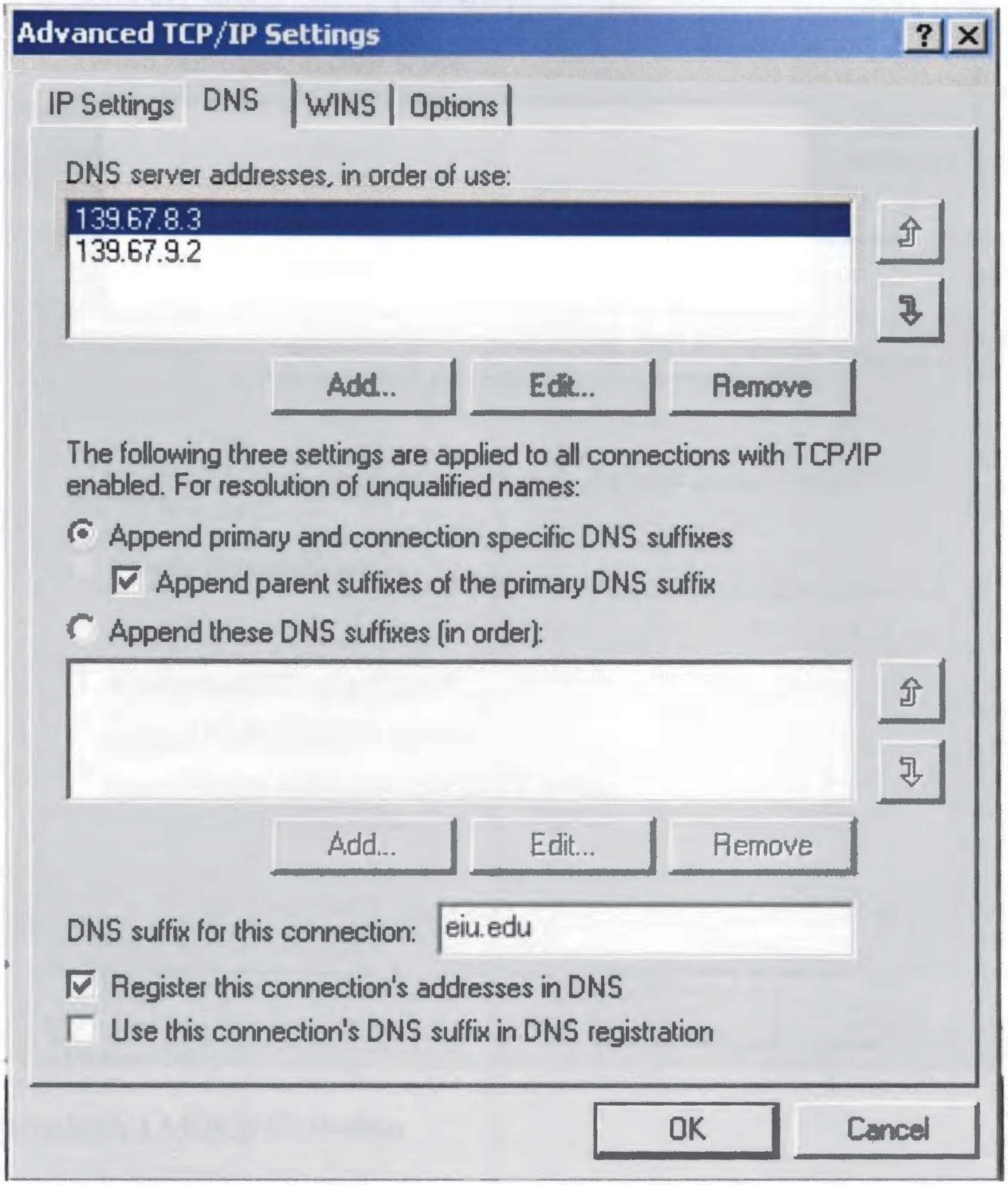
Alternate DNS server: 139 . 67 . 9 . 2

IP Address will be unique for each computer. IP's are located on the spreadsheet at the front of this manual.

Subnet Mask, Default Gateway, Preferred DNS server, and Alternate DNS server will always be the same.

Click the Advanced Button
Click the DNS Tab

This Screen will appear:



Advanced TCP/IP Settings

DNS server addresses, in order of use:

139.67.8.3
139.67.9.2

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

DNS suffix for this connection: eiu.edu

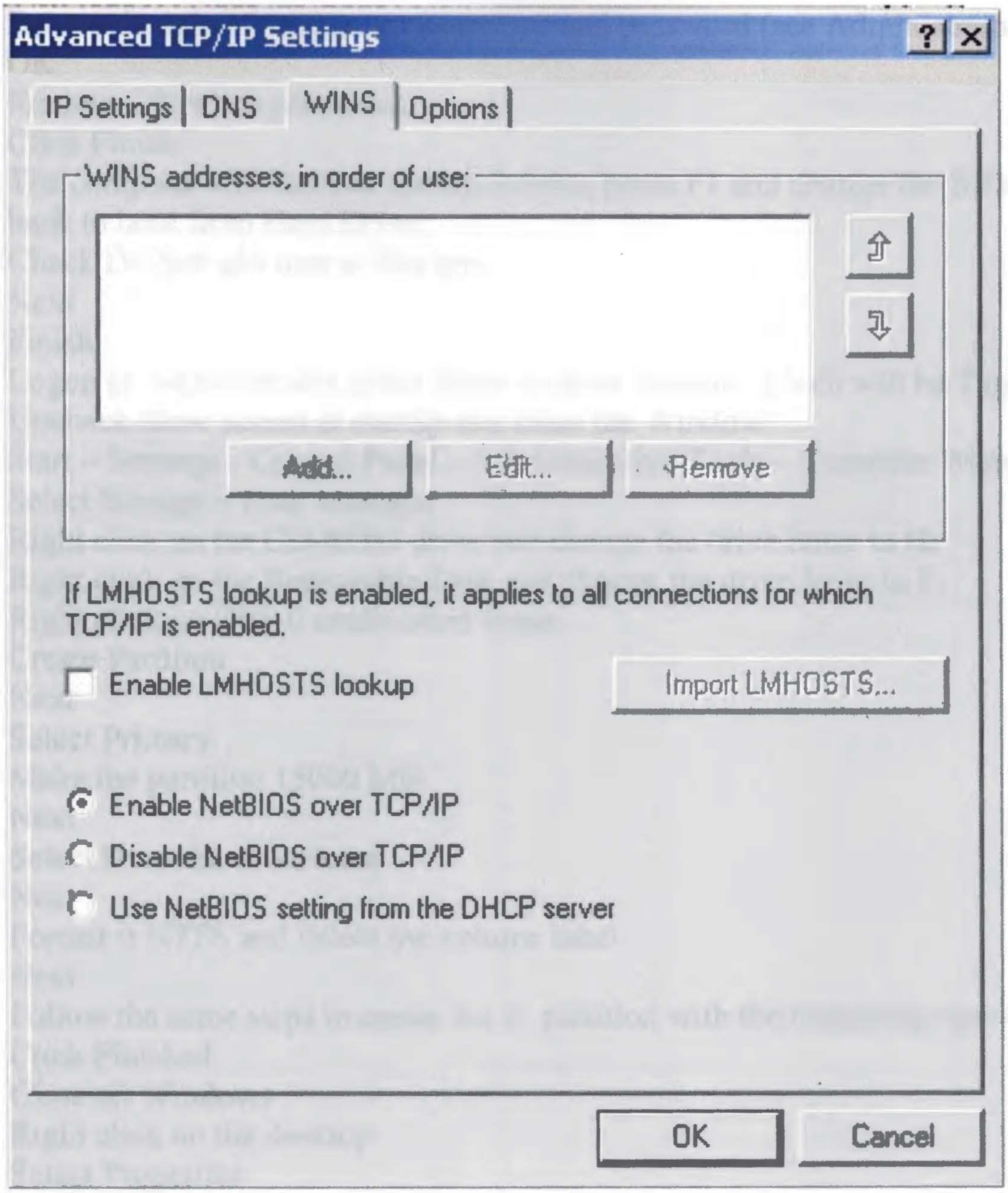
☑ Register this connection's addresses in DNS

□ Use this connection's DNS suffix in DNS registration

All information will be the same as shown above

After entering the above information, click on the WINS Tab

This screen will appear:



WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

□ Enable LMHOSTS lookup

● Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

○ Use NetBIOS setting from the DHCP server

Uncheck LMHOSTS lookup

Click OK to continue
Yes to the Empty Connection
OK
Next
Click Yes to make a Member of a Domain

Key in EIUCOM
Next
Enter a domain administrator username and password (see Administrator)
OK
Remove CD when prompted
Click Finish
The computer will Reboot, during Reboot, press F1 and change the BIOS back to boot from Hard Drive.
Check Do Not add user at this time
Next
Finish
Logon as Administrator (click More to show domain, which will be Tag#)
Uncheck show screen at startup and close the Window
Start – Settings - Control Panel - Administrative Tools – Computer Management
Select Storage – Disk Manager
Right click on the CD-ROM drive and change the drive letter to H:
Right click on the Removable Disk and change the drive letter to F:
Right click on Disk 0 unallocated space
Create Partition
Next
Select Primary
Make the partition 15000 MB
Next
Select D: as the drive letter
Next
Format it NTFS and delete the volume label
Next
Follow the same steps to create the E: partition with the remaining space.
Click Finished
Close all Windows
Right click on the desktop
Select Properties
Settings
Change Colors to True Color 32 Bit
Change screen to 800 by 600
Click on Screen Saver
Choose Mystify
OK
Go to Communications Software Installation Section

APPENDIX E

Windows NT Setup Procedures

Windows NT Installation Instructions

Turn on Power
Press F1 to enter BIOS
Password (see Administrator)

Setting should be as follows:

Main:

Leave all defaults

Advanced:

Plug+Play = No
Reset config data = No
Num Lock = On

Security:

User password = clear
Supervisor password = Set (see Administrator)

Power:

Power Management = Enabled
Hard drive = Disabled
VESA = Standby
Fan Always On = Yes
Power Button = On/Off

Boot:

Silent Boot = Enabled
Quick Boot = Enabled
Scan user flash area = Disabled
After power failure = Last state
On Modem Ring = Stay off
On LAN = stay on
On PME = stay off
First Boot = Hard Drive (CD-ROM for installation)
Second Boot = CD-ROM (Hard Drive for installation)
Third Boot = Removable Devices

Put in Windows NT CD (one with the windows symbol on CD) and press F10 (yes to accept)

At welcome screen press Enter to setup Windows NT
Press Enter to continue with current devices
Press Enter to continue

Press Page Down seven times on License Agreement

Press F8 to agree to license

Press N for fresh NT installation

Press Enter to accept devices

Delete all partitions by highlighting and pressing D

-Then press Enter followed by L

Press C to create a new partition

Change size to:	LH 1021	2400
	LH 1020	3012
	LH 1120	Linux Boot Partition

Press Enter to choose C: Partition

Select Format partition as NTFS file system

Press Enter to accept /WINNT as installation

Press Enter for an exhaustive examination

Remove CD-ROM and Floppy when prompted and Press Enter

During reboot press F1 and change boot back to boot from hard drive

Insert CD-ROM when Prompted and Click OK

Next on Gathering Information

Check Custom and Click Next

Name: Tag #

Organization: Eastern Illinois University

Enter License #

Computer Name: Tag #EIU

Enter Administrative Password (See Administrator)

Select No on Emergency Disk

Uncheck Communications

Double Click on Windows Messaging

Check Windows Messaging

Click OK

Click Next

Click Next on Installing Windows NT Networking

Leave wired to network checked and click next

Select from list

Insert NT Token-ring Driver Disk

Have Disk

Type A:\NT

Click OK on IBM PCI Token-ring Adapter

Click Next

Check TCP/IP Protocol + NetBEUI Protocol then click next

Next

Click Next to Install Selected Components

Leave Blank and Click OK

Select NO to DHCP

Enter the following:
IP Address: See Spreadsheet 139.67.xx.xxx
Subnet Mask: 255.255.248.0
Default Gateway: 139.67.24.1
Click on the DNS Tab:
Host Name: See Spreadsheet Panther…
Domain: eiu.edu
DNS: 139.67.8.3
139.67.9.2
Click on the WINS Address Tab
Check Enable DNS and Uncheck Enable LMHOSTS
Click OK
Click OK on Message
Click Yes to continue
Click Next on Bindings Page
Click Next to Start Network
Select Domain and Enter EIUCOM
Check Create Account and Click Next
See Administrator for User Name and Password
Click Finish
Set time zone to Central
Check for correct time
Click Close
Click OK in Display Message
Click OK on Display Settings
Remove Disks and Click Restart
Click Start/Programs/Administrative Tools/Disk Administrator
Right Click on the CD-ROM Drive
Assign Drive Letter H:
Right Click on Free Space
Create: LH1021 3400
LH1020 3008
Right Click on Free Space
Create: LH 1021
LH1020 (ALL LEFT)
LH 1120
Right Click on D:
Commit Changes Now
Right Click on D:
Format
Change to NTFS then Start
Repeat steps for drive E:
Continue to Communication Software Installation

APPENDIX F

Network Security Manual

NETWORK SECURITY MANUAL

Lumpkin Hall Computer Labs

10/19/00

by

Erik Quist

revised: 12/4/01

Section 1: User Groups

EIUCOM Domain

On the EIUCOM domain, all of the student users are in the EIUCOM User group. This group is made up of all of the workstation accounts, which are the tag #'s for each workstation. There is also a maintenance group called LCOBMAINT.

The Default User for these groups is setup to manually point to a policy file located on the L7019PDC server in Netlogon\Lumpkin. There is a separate policy file for each of the labs. The lumpkin.adm template must be loaded into the Policy Editor prior to opening an of the policy files. This template is located at \\L7019PDC\Netlogon in a folder called Templates. A backup copy of the policy files is located on L7019BDC.

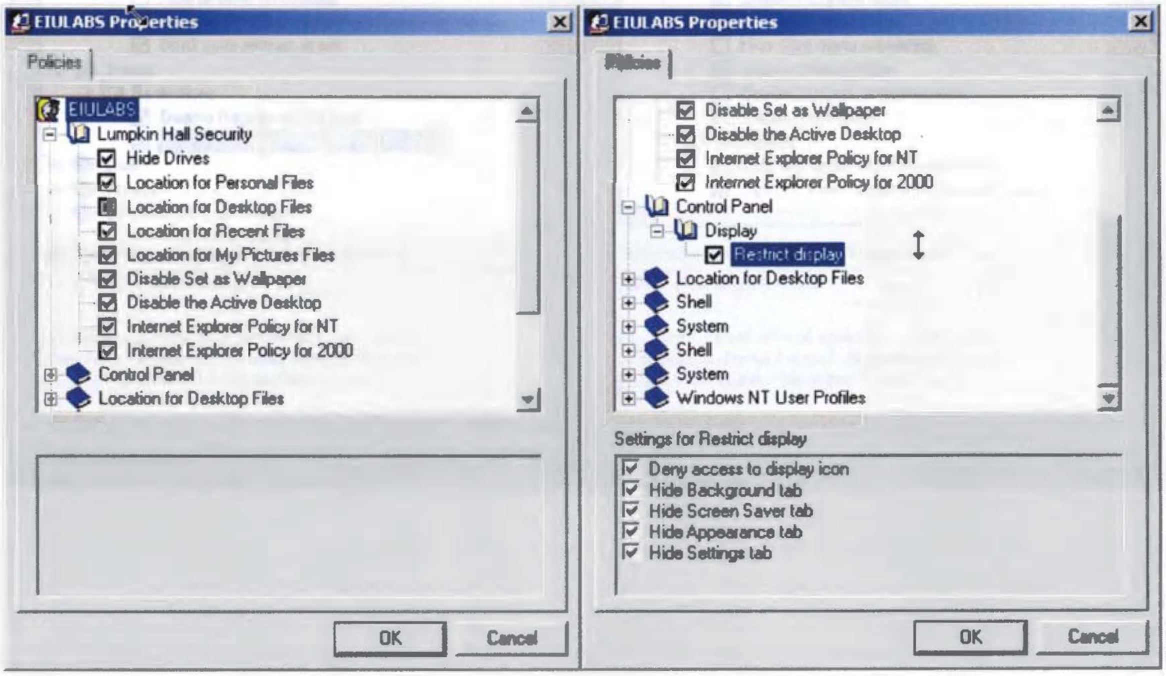
All user accounts have been setup to run a logon script called eiucom.bat during the authentication process. This batch file then calls tsm.bat, which is a script file for setting up the local printers (see tsm.bat).

BUSFACDM Domain

The BUSFACDM domain is for faculty and staff only. This domain contains two major groups, which provide crossover access to the shared folders on EIUCOM. These two groups are LCOBFAC and BUSFAC.

Section 2: Policies

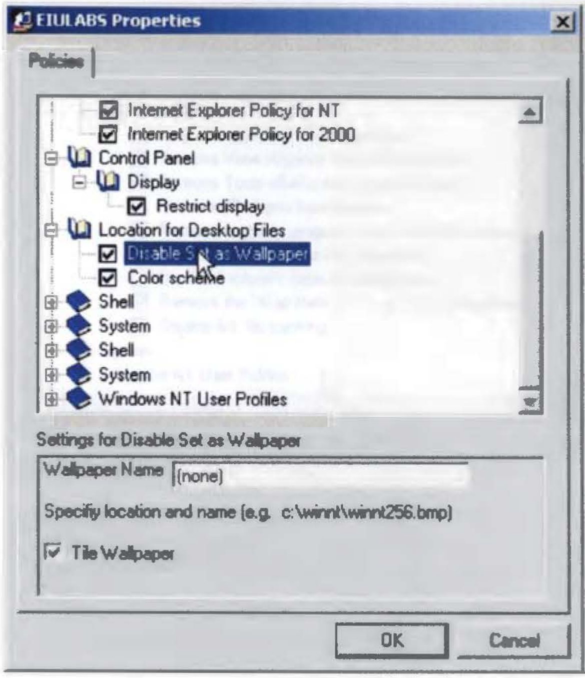
The following are screen shots of all of the settings within the policy files for the EIUCOM domain.



EIULABS
Lumpkin Hall Security
☑ Hide Drives
☑ Location for Personal Files
▨ Location for Desktop Files
☑ Location for Recent Files
☑ Location for My Pictures Files
☑ Disable Set as Wallpaper
☑ Disable the Active Desktop
☑ Internet Explorer Policy for NT
☑ Internet Explorer Policy for 2000
Control Panel
Location for Desktop Files

☑ Disable Set as Wallpaper
☑ Disable the Active Desktop
☑ Internet Explorer Policy for NT
☑ Internet Explorer Policy for 2000
Control Panel
Display
☑ Restrict display
Location for Desktop Files
Shell
System
Shell
System
Windows NT User Profiles

Settings for Restrict display
☑ Deny access to display icon
☑ Hide Background tab
☑ Hide Screen Saver tab
☑ Hide Appearance tab
☑ Hide Settings tab



EIULABS Properties

Policies

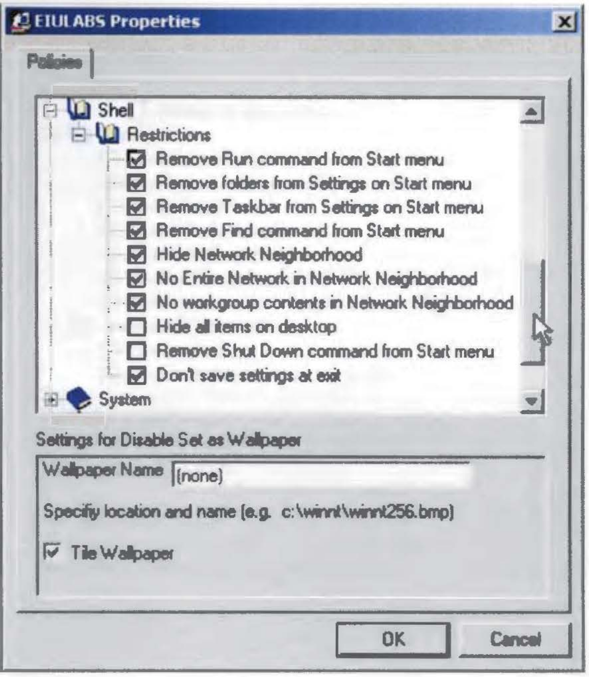
- ☑ Internet Explorer Policy for NT
- ☑ Internet Explorer Policy for 2000
- Control Panel
  - Display
    - ☑ Restrict display
- Location for Desktop Files
  - ☑ Disable Set as Wallpaper
  - ☑ Color scheme
- Shell
- System
- Shell
- System
- Windows NT User Profiles

Settings for Disable Set as Wallpaper

Wallpaper Name (none)

Specify location and name (e.g. c:\winnt\winnt256.bmp)

☑ Tile Wallpaper



EIULABS Properties

Policies

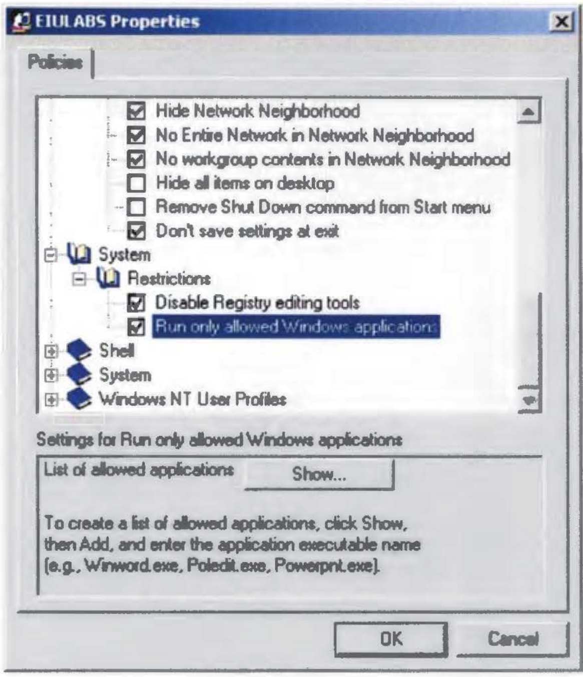
- Shell
  - Restrictions
    - ☑ Remove Run command from Start menu
    - ☑ Remove folders from Settings on Start menu
    - ☑ Remove Taskbar from Settings on Start menu
    - ☑ Remove Find command from Start menu
    - ☑ Hide Network Neighborhood
    - ☑ No Entire Network in Network Neighborhood
    - ☑ No workgroup contents in Network Neighborhood
    - ☐ Hide all items on desktop
    - ☐ Remove Shut Down command from Start menu
    - ☑ Don't save settings at exit
- System

Settings for Disable Set as Wallpaper

Wallpaper Name (none)

Specify location and name (e.g. c:\winnt\winnt256.bmp)

☑ Tile Wallpaper



EIULABS Properties

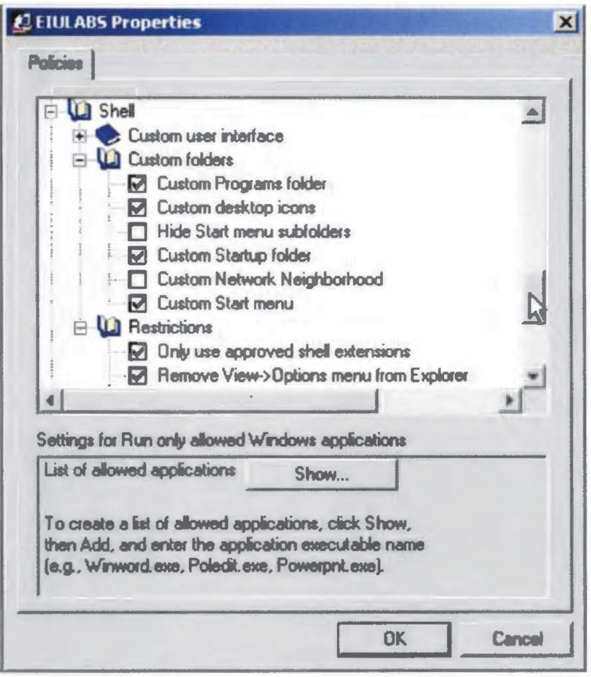
Policies

- ☑ Hide Network Neighborhood
- ☑ No Entire Network in Network Neighborhood
- ☑ No workgroup contents in Network Neighborhood
- ☐ Hide all items on desktop
- ☐ Remove Shut Down command from Start menu
- ☑ Don't save settings at exit
- System
  - Restrictions
    - ☑ Disable Registry editing tools
    - ☑ Run only allowed Windows applications
- Shell
- System
- Windows NT User Profiles

Settings for Run only allowed Windows applications

List of allowed applications Show...

To create a list of allowed applications, click Show, then Add, and enter the application executable name (e.g., Winword.exe, Poledit.exe, Powerpnt.exe).



EIULABS Properties

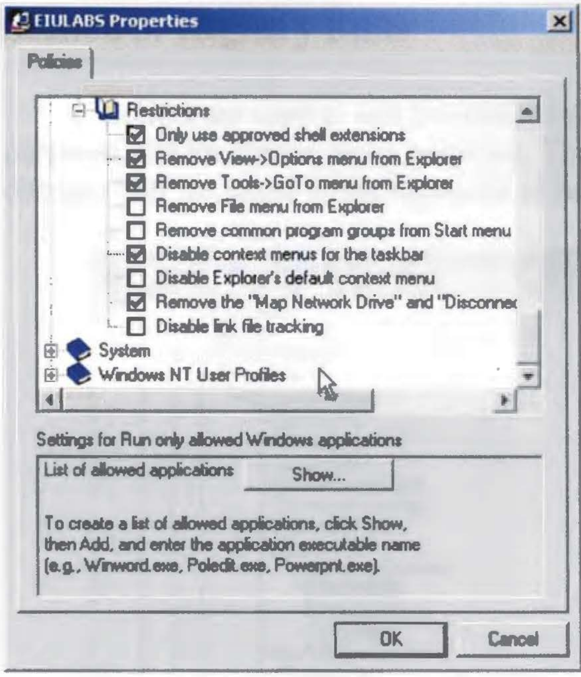
Policies

- Shell
  - Custom user interface
  - Custom folders
    - ☑ Custom Programs folder
    - ☑ Custom desktop icons
    - ☐ Hide Start menu subfolders
    - ☑ Custom Startup folder
    - ☐ Custom Network Neighborhood
    - ☑ Custom Start menu
  - Restrictions
    - ☑ Only use approved shell extensions
    - ☑ Remove View->Options menu from Explorer

Settings for Run only allowed Windows applications

List of allowed applications Show...

To create a list of allowed applications, click Show, then Add, and enter the application executable name (e.g., Winword.exe, Poledit.exe, Powerpnt.exe).



EIULABS Properties

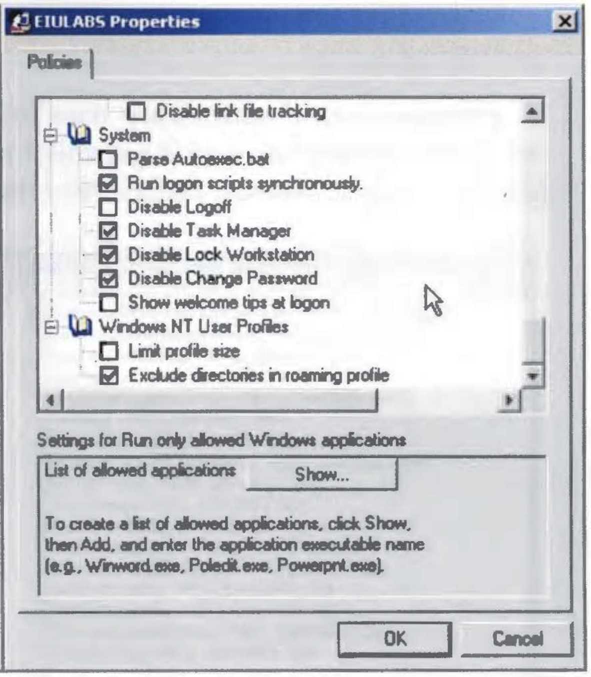
Policies

- Restrictions
  - ☑ Only use approved shell extensions
  - ☑ Remove View->Options menu from Explorer
  - ☑ Remove Tools->GoTo menu from Explorer
  - □ Remove File menu from Explorer
  - □ Remove common program groups from Start menu
  - ☑ Disable context menus for the taskbar
  - □ Disable Explorer's default context menu
  - ☑ Remove the "Map Network Drive" and "Disconnec
  - □ Disable link file tracking
- System
- Windows NT User Profiles

Settings for Run only allowed Windows applications

List of allowed applications

To create a list of allowed applications, click Show, then Add, and enter the application executable name (e.g., Winword.exe, Poledit.exe, Powerpnt.exe).



EIULABS Properties

Policies

- □ Disable link file tracking
- System
  - □ Parse Autoexec.bat
  - ☑ Run logon scripts synchronously.
  - □ Disable Logoff
  - ☑ Disable Task Manager
  - ☑ Disable Lock Workstation
  - ☑ Disable Change Password
  - □ Show welcome tips at logon
- Windows NT User Profiles
  - □ Limit profile size
  - ☑ Exclude directories in roaming profile

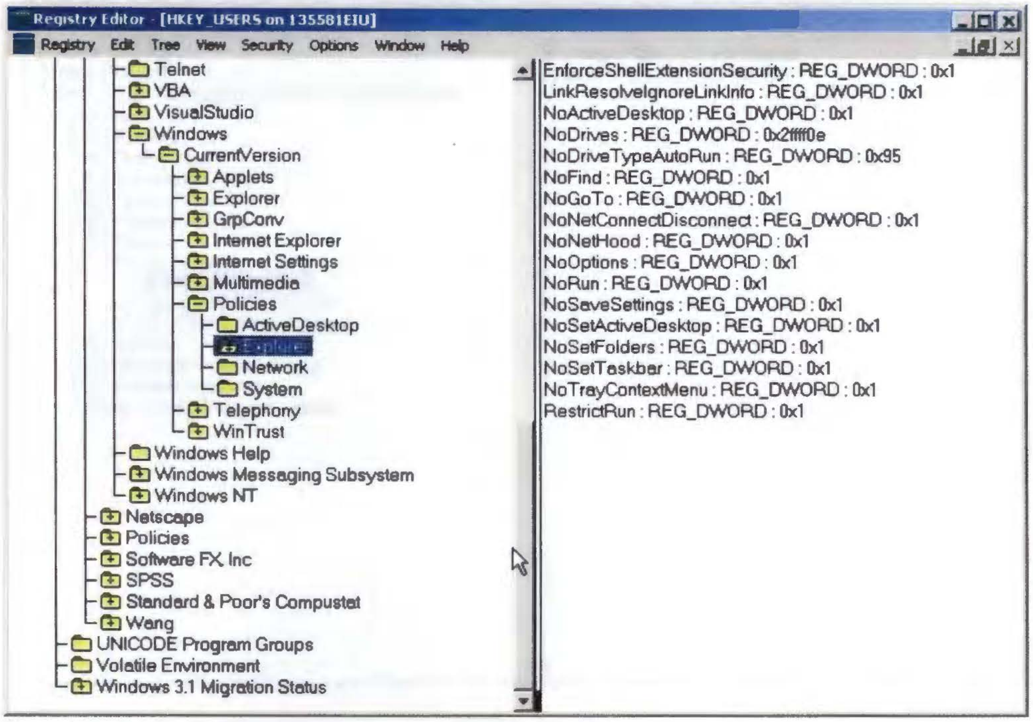
Settings for Run only allowed Windows applications

List of allowed applications

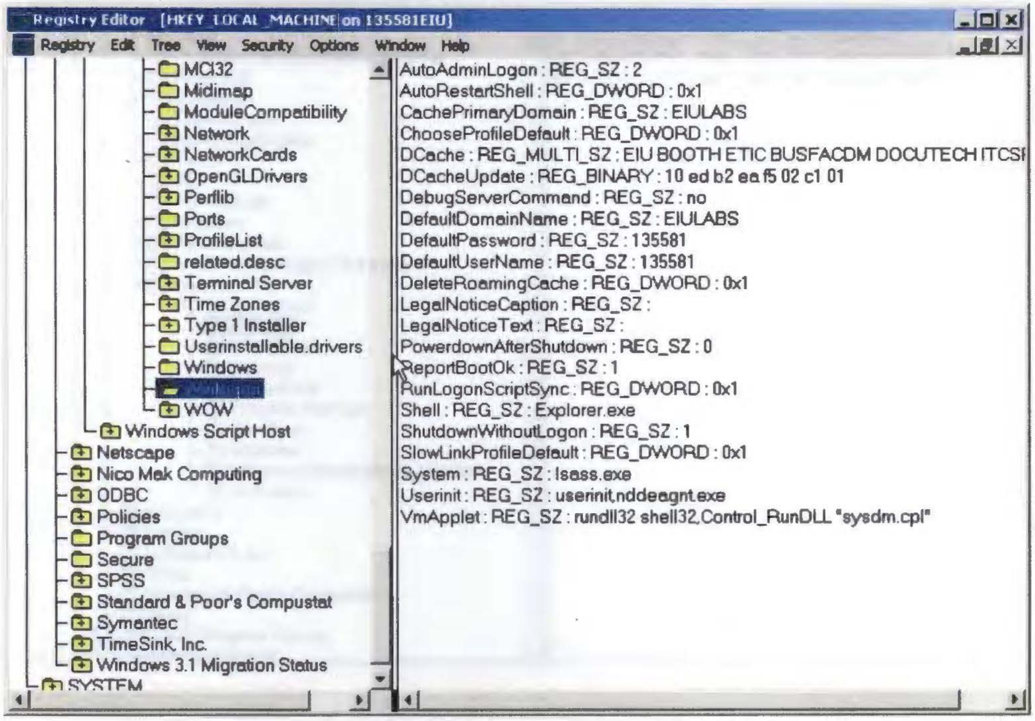
To create a list of allowed applications, click Show, then Add, and enter the application executable name (e.g., Winword.exe, Poledit.exe, Powerpnt.exe).

Section 3: Registry Edits

Scripts are used to edit the registries of each workstation both for security purposes and for device setup purposes. The following are screen shots showing the changes that are made to the registries of each workstation through the use of scripts.



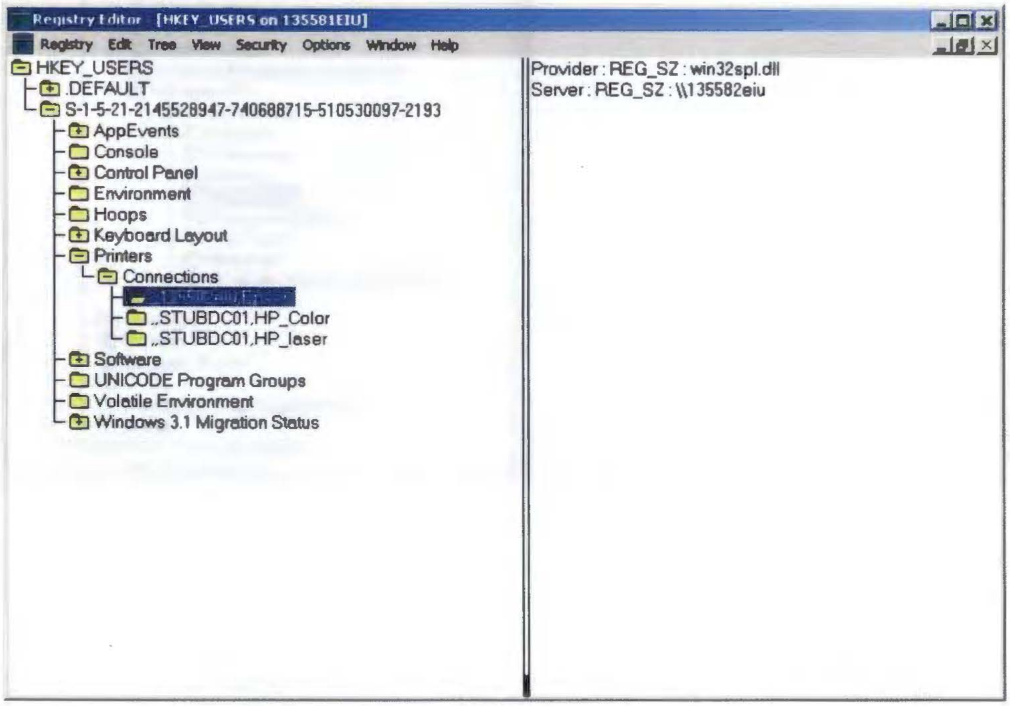
```
EnforceShellExtensionSecurity : REG_DWORD : 0x1
LinkResolveIgnoreLinkInfo : REG_DWORD : 0x1
NoActiveDesktop : REG_DWORD : 0x1
NoDrives : REG_DWORD : 0x2ffff0e
NoDriveTypeAutoRun : REG_DWORD : 0x95
NoFind : REG_DWORD : 0x1
NoGoTo : REG_DWORD : 0x1
NoNetConnectDisconnect : REG_DWORD : 0x1
NoNetHood : REG_DWORD : 0x1
NoOptions : REG_DWORD : 0x1
NoRun : REG_DWORD : 0x1
NoSaveSettings : REG_DWORD : 0x1
NoSetActiveDesktop : REG_DWORD : 0x1
NoSetFolders : REG_DWORD : 0x1
NoSetTaskbar : REG_DWORD : 0x1
NoTrayContextMenu : REG_DWORD : 0x1
RestrictRun : REG_DWORD : 0x1
```



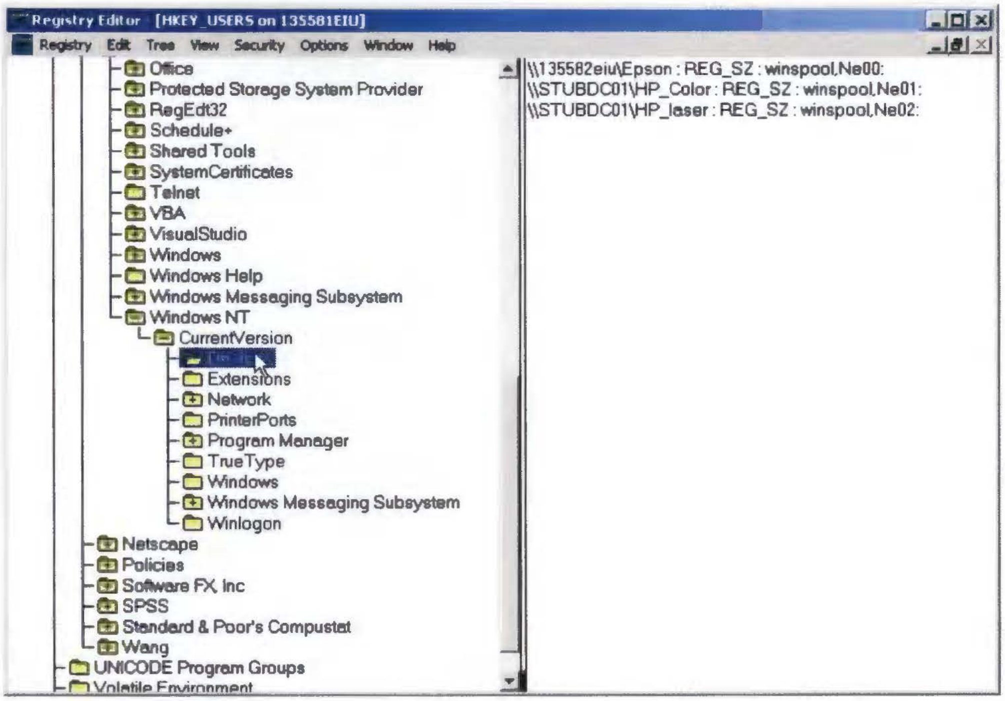
```
AutoAdminLogon : REG_SZ : 2
AutoRestartShell : REG_DWORD : 0x1
CachePrimaryDomain : REG_SZ : EIULABS
ChooseProfileDefault : REG_DWORD : 0x1
DCache : REG_MULTI_SZ : EIU BOOTH ETIC BUSFACDM DOCUTECH ITCSI
DCacheUpdate : REG_BINARY : 10 ed b2 ea f5 02 c1 01
DebugServerCommand : REG_SZ : no
DefaultDomainName : REG_SZ : EIULABS
DefaultPassword : REG_SZ : 135581
DefaultUserName : REG_SZ : 135581
DeleteRoamingCache : REG_DWORD : 0x1
LegalNoticeCaption : REG_SZ :
LegalNoticeText : REG_SZ :
PowerdownAfterShutdown : REG_SZ : 0
ReportBootOk : REG_SZ : 1
RunLogonScriptSync : REG_DWORD : 0x1
Shell : REG_SZ : Explorer.exe
ShutdownWithoutLogon : REG_SZ : 1
SlowLinkProfileDefault : REG_DWORD : 0x1
System : REG_SZ : lsass.exe
Userinit : REG_SZ : userinit,nddeagnt.exe
VmApplet : REG_SZ : rundll32 shell32,Control_RunDLL "sysdm.cpl"
```

The scripts used to make these edits are labsetup and autologon. Copies of these scripts are at the back of this manual.

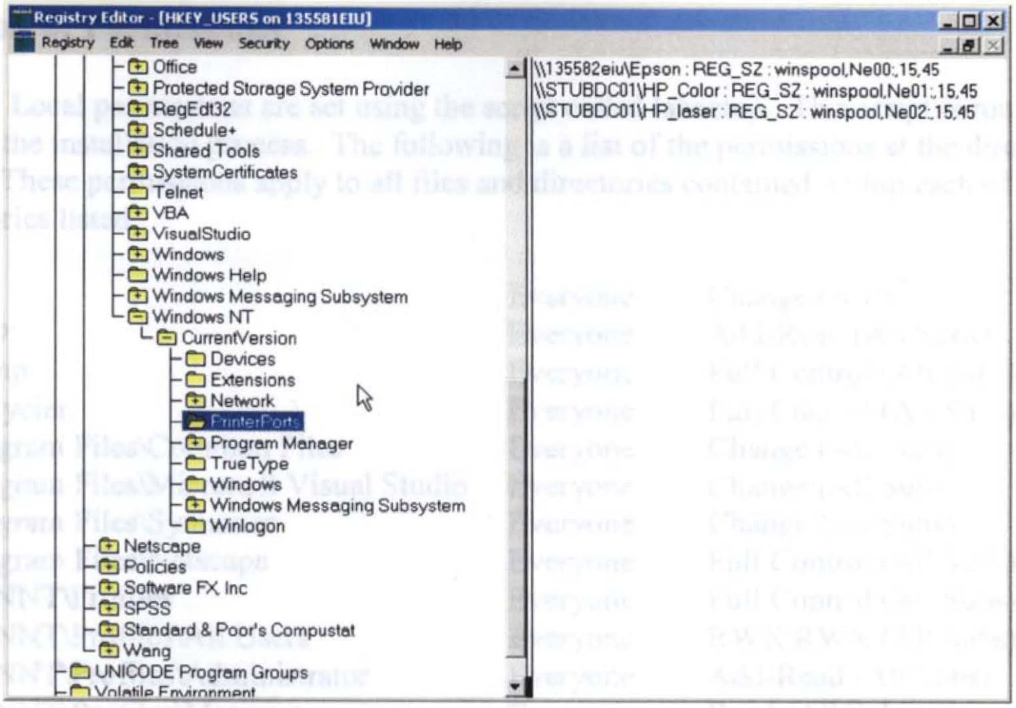
Another script is run at logon. This script is called tsm.bat. The following are screen shots of the registry edits made by this script.



Provider : REG_SZ : win32spl.dll
Server : REG_SZ : \\135582eiu



\\135582eiu\Epson : REG_SZ : winspool,Ne00:
\\STUBDC01\HP_Color : REG_SZ : winspool,Ne01:
\\STUBDC01\HP_laser : REG_SZ : winspool,Ne02:



```
\\135582eiu\Epson : REG_SZ : winspool,Ne00:,15,45
\\STUBDC01\HP_Color : REG_SZ : winspool,Ne01:,15,45
\\STUBDC01\HP_laser : REG_SZ : winspool,Ne02:,15,45
```

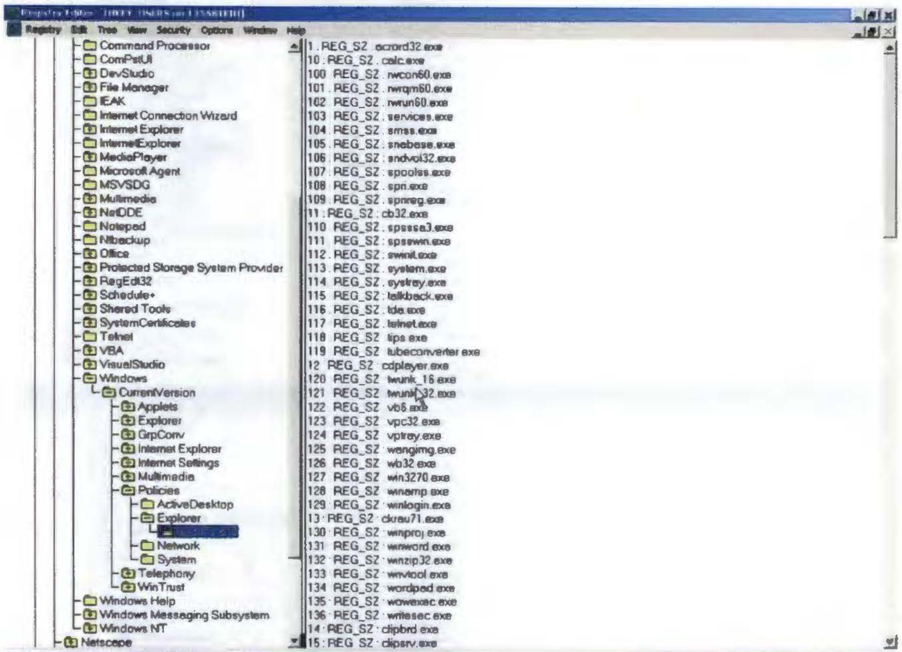
Section 4: Permissions

Local permissions are set using the script called labsetup. This script is run at the end of the installation process. The following is a list of the permissions at the directory level. These permissions apply to all files and directories contained within each of the directories listed.

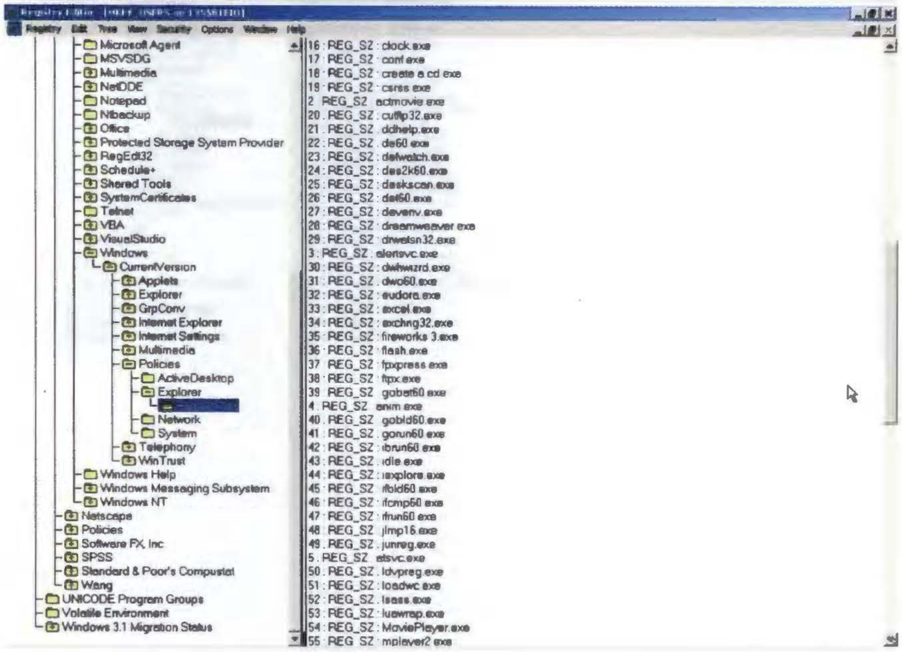
E:	Everyone	Change (All Subs)
C: & D:	Everyone	Add-Read (All Subs)
C:\Temp	Everyone	Full Control (All Subs)
C:\Recycler	Everyone	Full Control (All Subs)
C:\Program Files\Common Files	Everyone	Change (All Subs)
C:\Program Files\Microsoft Visual Studio	Everyone	Change (All Subs)
C:\Program Files\Symantec	Everyone	Change (All Subs)
C:\Program Files\Netscape	Everyone	Full Control (All Subs)
C:\WINNT\Profiles	Everyone	Full Control (All Subs)
C:\WINNT\Profiles\All Users	Everyone	RWX RWX (All Subs)
C:\WINNT\Profiles\Administrator	Everyone	Add-Read (All Subs)
C:\WINNT\Profiles\Manager	Everyone	Read (All Subs)
C:\WINNT\System32	Everyone	Change (All Subs)
C:\WINNT\System	Everyone	Change (All Subs)
D:\Recycler	Everyone	Full Control (All Subs)
D:\Download	Everyone	Full Control (All Subs)
D:\Program Files\MSOffice	Everyone	Full Control (All Subs)
D:\Program Files\Netscape	Everyone	Full Control (All Subs)
D:\Program Files\Navnt	Everyone	Full Control (All Subs)
D:\Program Files\Research Insight	Everyone	Full Control (All Subs)

Section 5: Restrict Run List

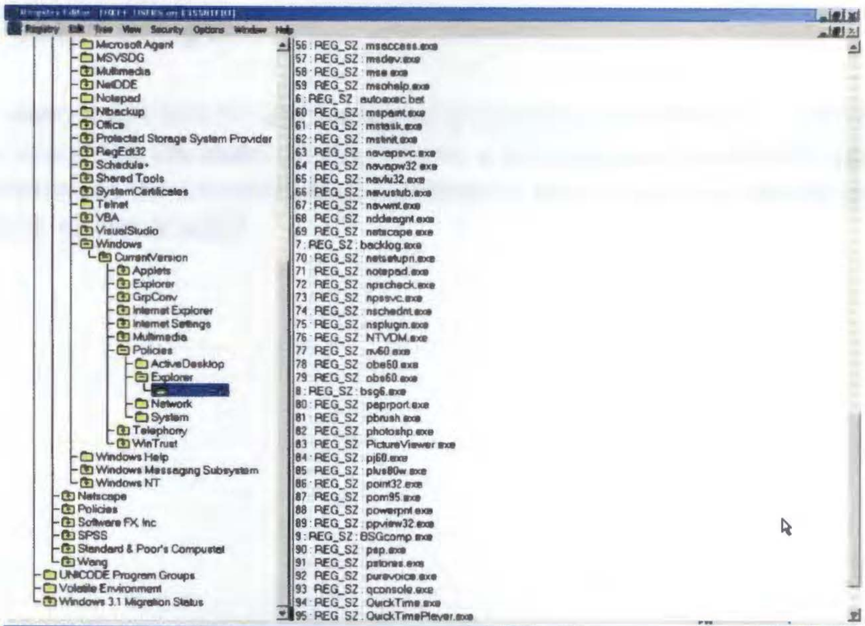
The following are screen shots of the restrict run as found in the registry. This list must be updated as new software is added. This is the restrict run list as of October 19, 2000.



```
1 : REG_SZ : acrord32.exe
10 : REG_SZ : calc.exe
100 : REG_SZ : rwcon60.exe
101 : REG_SZ : rwrqm60.exe
102 : REG_SZ : rwrun60.exe
103 : REG_SZ : services.exe
104 : REG_SZ : smss.exe
105 : REG_SZ : snebase.exe
106 : REG_SZ : sndvol32.exe
107 : REG_SZ : spoolss.exe
108 : REG_SZ : spri.exe
109 : REG_SZ : spnreg.exe
11 : REG_SZ : cb32.exe
110 : REG_SZ : spsssa3.exe
111 : REG_SZ : spsswn.exe
112 : REG_SZ : swinit.exe
113 : REG_SZ : system.exe
114 : REG_SZ : systray.exe
115 : REG_SZ : talkback.exe
116 : REG_SZ : tde.exe
117 : REG_SZ : telnet.exe
118 : REG_SZ : tips.exe
119 : REG_SZ : tubeconverter.exe
12 : REG_SZ : cdplayer.exe
120 : REG_SZ : twunk_16.exe
121 : REG_SZ : twunk_32.exe
122 : REG_SZ : vb6.exe
123 : REG_SZ : vpc32.exe
124 : REG_SZ : vptray.exe
125 : REG_SZ : wangimg.exe
126 : REG_SZ : wb32.exe
127 : REG_SZ : win3270.exe
128 : REG_SZ : winamp.exe
129 : REG_SZ : winlogin.exe
13 : REG_SZ : ckrau71.exe
130 : REG_SZ : winproj.exe
131 : REG_SZ : winword.exe
132 : REG_SZ : winzip32.exe
133 : REG_SZ : winvtool.exe
134 : REG_SZ : wordpad.exe
135 : REG_SZ : wowexec.exe
136 : REG_SZ : writesec.exe
14 : REG_SZ : clipbrd.exe
15 : REG_SZ : clipsrv.exe
```

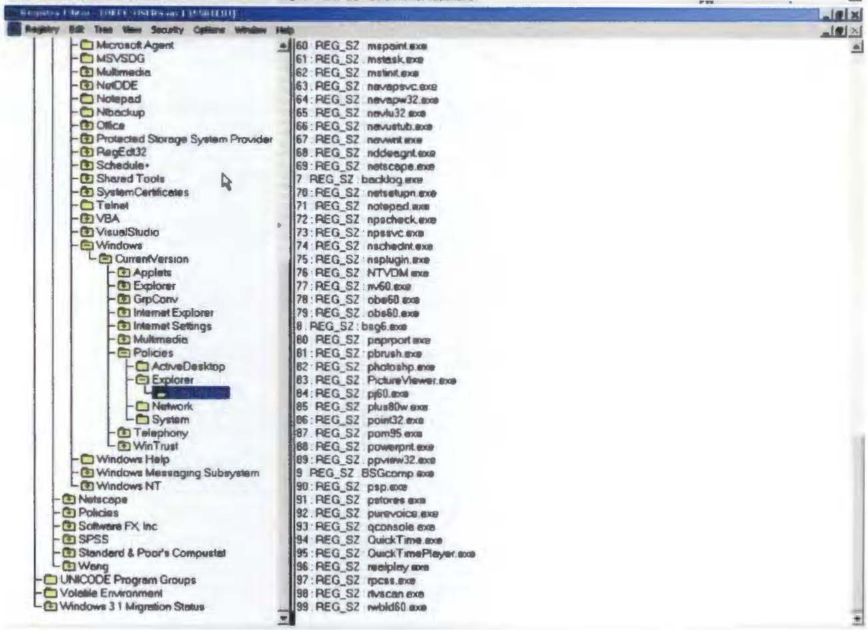


```
16 : REG_SZ : clock.exe
17 : REG_SZ : conf.exe
18 : REG_SZ : create a cd.exe
19 : REG_SZ : csrss.exe
2 : REG_SZ : actmovie.exe
20 : REG_SZ : cutlip32.exe
21 : REG_SZ : ddhelp.exe
22 : REG_SZ : de60.exe
23 : REG_SZ : defwatch.exe
24 : REG_SZ : des2k60.exe
25 : REG_SZ : deskscan.exe
26 : REG_SZ : det60.exe
27 : REG_SZ : devenv.exe
28 : REG_SZ : dreamweaver.exe
29 : REG_SZ : drwatsn32.exe
3 : REG_SZ : alertsvc.exe
30 : REG_SZ : dwhwizrd.exe
31 : REG_SZ : dwo60.exe
32 : REG_SZ : eudora.exe
33 : REG_SZ : excel.exe
34 : REG_SZ : exchng32.exe
35 : REG_SZ : fireworks 3.exe
36 : REG_SZ : flash.exe
37 : REG_SZ : fpxpress.exe
38 : REG_SZ : ftpx.exe
39 : REG_SZ : gobet60.exe
4 : REG_SZ : anim.exe
40 : REG_SZ : gobld60.exe
41 : REG_SZ : gorun60.exe
42 : REG_SZ : ibrun60.exe
43 : REG_SZ : idle.exe
44 : REG_SZ : iexplore.exe
45 : REG_SZ : ifbld60.exe
46 : REG_SZ : ifcmp60.exe
47 : REG_SZ : ifrun60.exe
48 : REG_SZ : jlmp16.exe
49 : REG_SZ : junreg.exe
5 : REG_SZ : atsvc.exe
50 : REG_SZ : ldvpreg.exe
51 : REG_SZ : loadwc.exe
52 : REG_SZ : lsass.exe
53 : REG_SZ : luawrap.exe
54 : REG_SZ : MoviePlayer.exe
55 : REG_SZ : mplayer2.exe
```



```
      ├─Microsoft Agent
      ├─MSVSDG
      ├─Multimedia
      ├─NetDDE
      ├─Notepad
      ├─Ntbackup
      ├─Office
      ├─Protected Storage System Provider
      ├─RegEdt32
      ├─Schedule+
      ├─Shared Tools
      ├─SystemCertificates
      ├─Telnet
      ├─VBA
      ├─VisualStudio
      ├─Windows
      │  └─CurrentVersion
      │     ├─Applets
      │     ├─Explorer
      │     ├─GrpConv
      │     ├─Internet Explorer
      │     ├─Internet Settings
      │     ├─Multimedia
      │     ├─Policies
      │     │  ├─ActiveDesktop
      │     │  ├─Explorer
      │     │  │  └─
      │     │  ├─Network
      │     │  └─System
      │     ├─Telephony
      │     └─WinTrust
      ├─Windows Help
      ├─Windows Messaging Subsystem
      └─Windows NT
   ├─Netscape
   ├─Policies
   ├─Software FX Inc
   ├─SPSS
   ├─Standard & Poor's Compustat
   └─Wang
├─UNICODE Program Groups
├─Volatile Environment
└─Windows 3.1 Migration Status
```

```
56 : REG_SZ : msaccess.exe
57 : REG_SZ : msdev.exe
58 : REG_SZ : mse.exe
59 : REG_SZ : msohelp.exe
6 : REG_SZ : autoexec.bat
60 : REG_SZ : mspaint.exe
61 : REG_SZ : mstask.exe
62 : REG_SZ : mstinit.exe
63 : REG_SZ : navapsvc.exe
64 : REG_SZ : navapw32.exe
65 : REG_SZ : navlu32.exe
66 : REG_SZ : navustub.exe
67 : REG_SZ : navwnt.exe
68 : REG_SZ : nddeagnt.exe
69 : REG_SZ : netscape.exe
7 : REG_SZ : backlog.exe
70 : REG_SZ : netsetupn.exe
71 : REG_SZ : notepad.exe
72 : REG_SZ : npscheck.exe
73 : REG_SZ : npssvc.exe
74 : REG_SZ : nschednt.exe
75 : REG_SZ : nsplugin.exe
76 : REG_SZ : NTVDM.exe
77 : REG_SZ : nv60.exe
78 : REG_SZ : obe60.exe
79 : REG_SZ : obs60.exe
8 : REG_SZ : bsg6.exe
80 : REG_SZ : paprport.exe
81 : REG_SZ : pbrush.exe
82 : REG_SZ : photoshp.exe
83 : REG_SZ : PictureViewer.exe
84 : REG_SZ : pj60.exe
85 : REG_SZ : plus80w.exe
86 : REG_SZ : point32.exe
87 : REG_SZ : pom95.exe
88 : REG_SZ : powerpnt.exe
89 : REG_SZ : ppview32.exe
9 : REG_SZ : BSGcomp.exe
90 : REG_SZ : psp.exe
91 : REG_SZ : pstores.exe
92 : REG_SZ : purevoice.exe
93 : REG_SZ : qconsole.exe
94 : REG_SZ : QuickTime.exe
95 : REG_SZ : QuickTimePlayer.exe
```



```
      ├─Microsoft Agent
      ├─MSVSDG
      ├─Multimedia
      ├─NetDDE
      ├─Notepad
      ├─Ntbackup
      ├─Office
      ├─Protected Storage System Provider
      ├─RegEdt32
      ├─Schedule+
      ├─Shared Tools
      ├─SystemCertificates
      ├─Telnet
      ├─VBA
      ├─VisualStudio
      ├─Windows
      │  └─CurrentVersion
      │     ├─Applets
      │     ├─Explorer
      │     ├─GrpConv
      │     ├─Internet Explorer
      │     ├─Internet Settings
      │     ├─Multimedia
      │     ├─Policies
      │     │  ├─ActiveDesktop
      │     │  ├─Explorer
      │     │  │  └─
      │     │  ├─Network
      │     │  └─System
      │     ├─Telephony
      │     └─WinTrust
      ├─Windows Help
      ├─Windows Messaging Subsystem
      └─Windows NT
   ├─Netscape
   ├─Policies
   ├─Software FX Inc
   ├─SPSS
   ├─Standard & Poor's Compustat
   └─Wang
├─UNICODE Program Groups
├─Volatile Environment
└─Windows 3.1 Migration Status
```

```
60 : REG_SZ : mspaint.exe
61 : REG_SZ : mstask.exe
62 : REG_SZ : mstinit.exe
63 : REG_SZ : navapsvc.exe
64 : REG_SZ : navapw32.exe
65 : REG_SZ : navlu32.exe
66 : REG_SZ : navustub.exe
67 : REG_SZ : navwnt.exe
68 : REG_SZ : nddeagnt.exe
69 : REG_SZ : netscape.exe
7 : REG_SZ : backlog.exe
70 : REG_SZ : netsetupn.exe
71 : REG_SZ : notepad.exe
72 : REG_SZ : npscheck.exe
73 : REG_SZ : npssvc.exe
74 : REG_SZ : nschednt.exe
75 : REG_SZ : nsplugin.exe
76 : REG_SZ : NTVDM.exe
77 : REG_SZ : nv60.exe
78 : REG_SZ : obe60.exe
79 : REG_SZ : obs60.exe
8 : REG_SZ : bsg6.exe
80 : REG_SZ : paprport.exe
81 : REG_SZ : pbrush.exe
82 : REG_SZ : photoshp.exe
83 : REG_SZ : PictureViewer.exe
84 : REG_SZ : pj60.exe
85 : REG_SZ : plus80w.exe
86 : REG_SZ : point32.exe
87 : REG_SZ : pom95.exe
88 : REG_SZ : powerpnt.exe
89 : REG_SZ : ppview32.exe
9 : REG_SZ : BSGcomp.exe
90 : REG_SZ : psp.exe
91 : REG_SZ : pstores.exe
92 : REG_SZ : purevoice.exe
93 : REG_SZ : qconsole.exe
94 : REG_SZ : QuickTime.exe
95 : REG_SZ : QuickTimePlayer.exe
96 : REG_SZ : realplay.exe
97 : REG_SZ : rpcss.exe
98 : REG_SZ : rtvscan.exe
99 : REG_SZ : rwbld60.exe
```

Section 6: Other Scripts

One other script that is used for security purposes is listkill.scr. This script allows the administrator to list the tasks on any remote workstation and terminate applications that are disallowed in the Lumpkin Hall Computer Labs. A copy of this script can be seen in the back of this manual.

Labsetup.bat

```
@echo off
xcacls c:\ /t /c /g administrator:f everyone:r;exw "eiucom\Domain Admins":F /y
xcacls "c:\Temp" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f /y
xcacls "c:\download" /t /c /g administrator:f "eiucom\Domain Admins":FF everyone:f /y
xcacls "c:\Recycler" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f /y
xcacls "c:\Program Files\Common Files" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f /y
xcacls "c:\Program Files\Symantec" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f /y
xcacls "c:\Program Files\Netscape" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f /y
xcacls "c:\Program Files\Navnt" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f /y
xcacls "c:\Program Files\Research Insight" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:c
/y
xcacls "c:\Program Files\Microsoft Visual Studio" /t /c /g administrator:f "eiucom\Domain Admins":F
everyone:c /y
xcacls "c:\winnt\*.*" /c /g administrator:f "eiucom\Domain Admins":F everyone:c;ex /y
xcacls "c:\winnt\profiles" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f /y
xcacls "c:\winnt\profiles\All Users" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:rw /y
xcacls "c:\winnt\profiles\All Users\Desktop" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:r
/y
xcacls "c:\winnt\profiles\All Users\Start Menu" /t /c /g administrator:f "eiucom\Domain Admins":F
everyone:r /y
xcacls "c:\winnt\profiles\administrator" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:rw /y
xcacls "c:\winnt\system" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:c /y
xcacls "c:\winnt\system32" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:c /y
xcacls d:\ /t /c /g administrator:f everyone:r;exw "eiucom\Domain Admins":F /y
xcacls "d:\Program Files\Microsoft Office" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f
/y
xcacls "d:\Program Files\Microsoft Visual Studio" /t /c /g administrator:f "eiucom\Domain Admins":F
everyone:c /y
xcacls "c:\Program Files\Research Insight" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:c
/y
xcacls "d:\tda" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:c /y
xcacls "d:\recycler" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f /y
xcacls "d:\orant" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:f /y
xcacls e:\ /T /C /G administrator:F everyone:C "eiucom\Domain Admins":F /Y
xcacls "c:\winnt\Netscape Wallpaper.*" /t /c /g administrator:f "eiucom\Domain Admins":F everyone:r /y
reg -DeleteTree \HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\Namespace
reg -Set REG_DWORD
\HKLM\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword=1
reg -Set REG_DWORD "\HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\"DeleteRoamingCache=1
reg -Set REG_DWORD "\HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\"RunLogonScriptSync=1
reg -Set REG_DWORD "\HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\"SlowLinkProfileDefault=1
reg -Set REG_DWORD "\HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\"ChooseProfileDefault=1
reg -set
\HKLM\System\ControlSet001\Control\Update\NetworkPath="\\l7019pdc\netlogon\lumpkin\lump34.pol"
reg -set REG_DWORD \HKLM\System\ControlSet001\Control\Update\UpdateMode=2
md "c:\winnt\profiles\all users\start menu\programs\Courselabs"
net use z: \\l7019pdc\utilities
copy z:\scripts\lh034\*.lnk "c:\winnt\profiles\all users\start menu\programs\Courselabs"
copy z:\scripts\eiucom.bat c:\winnt
```

```
md "c:\winnt\profiles\all users\start menu\programs\Accessories"
xcopy /e /r z:\scripts\lh034\accessories "c:\winnt\profiles\all users\start menu\programs\Accessories"
md "c:\winnt\eiucom"
net use z: /d
rename "c:\program files\netscape\communicator\program\"prefui32.dll prefui32!.dll
del "c:\winnt\profiles\all users\start menu\programs\startup\m*.lnk"
call autologon.bat
exit
```

Tsm.bat

```
@echo off
net use p: /d
net use q: /d
net use l: /d
net use o: /d
net use p: \\l7019bdc\compstat /persistent:no
net use q: \\l7019bdc\compdata /persistent:no
net use o: \\l7019bdc\apps /persistent:no
net use l: \\l7019s01\courselab /persistent:no
set x=,,135583eiu,Epson
set y=,,l7019s01,HP_Color
set z=,,l7019s01,HP_laser
c:\winnt\eiucom\writesec -deletetree \HKCU\Printers
c:\winnt\eiucom\writesec -deletetree "\HKCU\Software\Microsoft\Windows NT\CurrentVersion\Devices"
c:\winnt\eiucom\writesec -addkey "\HKCU\Software\Microsoft\Windows NT\CurrentVersion\Devices"
c:\winnt\eiucom\writesec -addkey \HKCU\Printers
c:\winnt\eiucom\writesec -addkey \HKCU\Printers
c:\winnt\eiucom\writesec -addkey \HKCU\Printers\Connections
c:\winnt\eiucom\writesec -addkey "\HKCU\Printers\Connections\%x%"
c:\winnt\eiucom\writesec -addkey "\HKCU\Printers\Connections\%y%"
c:\winnt\eiucom\writesec -addkey "\HKCU\Printers\Connections\%z%"
c:\winnt\eiucom\writesec -addkey "\HKCU\Software\Microsoft\Windows NT\CurrentVersion\"Devices
c:\winnt\eiucom\writesec -addkey "\HKCU\Software\Microsoft\Windows NT\CurrentVersion\"PrinterPorts
c:\winnt\eiucom\writesec -set \HKCU\Printers\DeviceOld="\\135583eiu\Epson,winspool,Ne00:"
c:\winnt\eiucom\writesec -set REG_dword \HKCU\Printers\ShowLogonDomain=1
c:\winnt\eiucom\writesec -set "\HKCU\Printers\Connections\%x%\"Provider="win32spl.dll"
c:\winnt\eiucom\writesec -set "\HKCU\Printers\Connections\%x%\"Server="\\135583eiu"
c:\winnt\eiucom\writesec -set "\HKCU\Printers\Connections\%y%\"Provider="win32spl.dll"
c:\winnt\eiucom\writesec -set "\HKCU\Printers\Connections\%y%\"Server="\\l7019s01"
c:\winnt\eiucom\writesec -set "\HKCU\Printers\Connections\%z%\"Provider="win32spl.dll"
c:\winnt\eiucom\writesec -set "\HKCU\Printers\Connections\%z%\"Server="\\l7019s01"
c:\winnt\eiucom\writesec -set -ValueDeLiMiter $ -set "\HKCU\Software\Microsoft\Windows
NT\CurrentVersion\Devices$\\l7019s01\HP_laser"="winspool,Ne02:"
c:\winnt\eiucom\writesec -set -ValueDeLiMiter $ -set "\HKCU\Software\Microsoft\Windows
NT\CurrentVersion\Devices$\\l7019s01\HP_Color"="winspool,Ne01:"
c:\winnt\eiucom\writesec -set -ValueDeLiMiter $ -set "\HKCU\Software\Microsoft\Windows
NT\CurrentVersion\Devices$\\135583eiu\Epson"="winspool,Ne00:"
c:\winnt\eiucom\writesec -set "\HKCU\Software\Microsoft\Windows
NT\CurrentVersion\Windows\"Device="\\135583eiu\Epson,winspool,Ne00:"
exit
```

Autologon.scr

```
;
; autologon.SCR
;
;


cls                         ; clear the screen



$x = %computername%
$y = substr("$x",1,6)
$z = "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon"
? "Computer Name is: $y"
?
writevalue("$z","DefaultUserName","$y","reg_sz")
writevalue("$z","DefaultPassword","$y","reg_sz")
writevalue("$z","DefaultDomainName","EIUCOM","reg_sz")
writevalue("$z","AutoAdminLogon","2","reg_sz")
if @error = 0
        SHELL"cmd /c xcacls c:\winnt\profiles\$y\Desktop /e /c /p everyone:r /y"
        SHELL"cmd /c xcacls c:\winnt\profiles\$y\startm~1 /e /c /p everyone:r /y"
        SHELL"net use z: \\l7019pdc\utilities"
        SHELL"cmd /c copy z:\scripts\1020printers\$y\*.* c:\winnt\eiucom\"
        SHELL"net use z: /d"
        SHELL"cmd /c xcacls c:\winnt\profiles\$y\applic~1\microsoft\intern~1 /e /c /p everyone:r /y"
else
  ? "error in registry edit"
endif
get $x
goto end

:end
? "END"
```

Listkill.scr

```
;
; listkill.SCR
;
;

cls                         ; clear the screen

set $x = "y"

:start
if $x = "Y"
   goto loop1
else
   goto end

:loop1
? "Enter the Tag# that you would like to list tasks on: "
GETS $Input
$Address = "\\" + $Input
SHELL "e:\erik\tools\pslist $Address"
$name = readvalue("$Address\HKEY_Local_Machine\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon","DefaultUserName")
? "The current user is $name"
? "Would you like to kill a task (Y/N)? "
GETS $Question
:loop2
if $Question = "Y"
     ? "Enter the task to be killed: "
     GETS $Input2
     SHELL "e:\erik\tools\pskill $Address $Input2"
     sendmessage("$Input","$Input2 Aborted by Network Administrator")
     ? "Would you like to kill another task on $Input ? "
     GETS $Question
     goto loop2
endif
? "Would you like to list another computers tasks? "
GETS $Question
if $Question = "Y"
  cls
  goto start
else
  goto end
:end
? "END"
```

APPENDIX G

Network Security Checksheet

Network Security Checksheet
Lumpkin Hall Computer Labs

		COMMENTS
Start Menu		
	Run Disabled	
	Search/Find Disabled	
	Settings Disabled	
My Computer		
	C: Drive Hidden	
	D: Drive Hidden	
	Mapped Drives Hidden	
	Control Panel Disabled	
Desktop		
	Network Neighborhood Disabled/Hidden	
	Ability to Create Folders on Desktop Disabled	
	Ability to Save Files to Desktop Disabled	
Mouse Functions		
	Ability to Change Display Properties Disabled (Right Click - Properties)	
Hot Keys		
	Win + R (Run) Disabled	
	Win + E (Explorer) Disabled	
	Win + F (Find/Search) Disabled	
	Win + Break (Systems Properties) Disabled	
	Win + U (Utility Manager) Disabled	
	Ctrl + Shift + Esc (Task Manager) Disabled	
Shells		
	Access to Command Line Disabled	
	FTP Shells Disabled (WS-FTP)	
	Disable File Browsing in IE	
Locate and Test:		
(Check for ablity	Office2000 (Word, Excel, PowerPoint, Access)	
to print to the epson,	Research Insight	
HP_laser and HP_color	Courselabs (Student Data Files)	
as well as proper	SPSS 10.0	
operation)	ESHA - Total Diet Assessment	
	Visual Studio 6.0 (Visual Basic, Visual C++)	
	Norton CE 4.51	
	Internet Explorer 5.5 SP1	
	Netscape 4.77	
	Quicktime 5.0	
	Adobe Acrobat 5.0	
	Cute FTP	
	Winzip	
	Dreamweaver (Versions 3.0 and 4.0)	
	Flash (Versions 4.0 and 5.0)	
	Fireworks (Versions 3.0 and 4.0)	
	Photoshop 6.0	
	MS Publisher 2000	
	MS Project 2000	
	EMACS - JDE	
	ProMatch2000	
	Linux Logon	

Workstation Tag #: ______________________

Checked by: ___________________________ **Date:** ____________

APPENDIX H

Sample Survey

Accessibility Survey
Lumpkin Hall Computer Labs

The purpose of this survey is to determine how accessible the workstations are in the Lumpkin Hall Computer Labs. This information will be used in the continuing development process of the workstation setup in the Lumpkin Hall Open Lab facility. All responses are completely confidential.

Please drop off all surveys at the Help Desk in Lumpkin Hall, LH1015.

Thank you for your responses.

1) Which of the following age groups are you in?

a. 18 and under b. 19 to 21 c. 22 to 26 d. 27 and over

2) What year are you in college?

a. Freshman
b. Sophomore
c. Junior
d. Senior
e. Graduate
f. Other

3) How many hours per week do you typically spend using computers?________

4) What Operating Systems are you familiar with? (Circle all applicable)

a. Win95 b. Win98 c. WinNT d. Win2000 e. WinME Other:____________

5) On Average, how many hours per week do you spend using computers in Lumpkin Hall?

a. None b. 1 - 5 hours c. 6 - 10 hours d. 11 or more hours

6) Do you ever use other open lab facilities? Yes / No

7) If so, approximately how many hours per week do you spend in Open Lab Facilities other than Lumpkin Hall?

a. None b. 1 - 5 hours c. 6 - 10 hours d. 11 or more hours

8) How would you rate your satisfaction with Open Lab Facilities other than Lumpkin Hall?

Poor	Average	Good	Great
1	2	3	4

9) How would you rate your satisfaction with the Lumpkin Hall Computer Labs?

Poor	Average	Good	Great
1	2	3	4

10) What do you typically use computers for? (Circle all applicable)

a. Word processing
b. Spreadsheets
c. Databases
d. Programming
e. Email
f. Internet
g. Games
h. Chat
i. E-learning
j. Web Design
k. SPSS

Other: ______________________________________

11) Have you taken any computer related courses? Yes / No

12) How would you rate your skill level with a computer?

Beginner	Moderate	Expert	Guru
1	2	3	4

13) How would you rate the accessibility to Word Processing Software in the Lumpkin Hall Computer Labs?

Poor	Average	Good	Great
1	2	3	4

14) How would you rate the accessibility to Spreadsheet Software in the Lumpkin Hall Computer Labs?

Poor	Average	Good	Great
1	2	3	4

15) How would you rate the accessibility to Database Software in the Lumpkin Hall Computer Labs?

Poor	Average	Good	Great
1	2	3	4

16) How would you rate the accessibility to Email in the Lumpkin Hall Computer Labs?

Poor	Average	Good	Great
1	2	3	4

17) How would you rate the accessibility to the Internet in the Lumpkin Hall Computer Labs?

Poor	Average	Good	Great
1	2	3	4

18) How would you rate the accessibility of Printing in the Lumpkin Hall Computer Labs?

Poor	Average	Good	Great
1	2	3	4

19) How would you rate the Help Desk Staff at the Lumpkin Hall Computer Labs?

Unfriendly	Acceptable	Good	Great
1	2	3	4

20) Please list any suggestions for improving the Lumpkin Hall Computer Labs: