OFFICE OF TECHNOLOGY SERVICES
CHICAGO PUBLIC SCHOOLS

Network Management Guidelines
Table of Contents

Table of Contents..................................................................................................................i

1 Overview............................................................................................................................. 1
  1.1 Purpose...................................................................................................................... 1
  1.2 Intended Audience ............................................................................................... 1
  1.3 Scope....................................................................................................................... 1

2 LAN and WAN Guidelines................................................................................................. 2
  2.1 Purpose...................................................................................................................... 2
  2.2 General Standards .................................................................................................. 2
  2.3 Workstation Requirements.................................................................................... 2
  2.4 Server Requirements............................................................................................. 3
  2.5 Anti-virus Software............................................................................................... 3
  2.6 Desktop Management ........................................................................................... 4
  2.7 CPS Security Provisions ...................................................................................... 4

3 Server Installation and Configuration.............................................................................. 6
  3.1 Purpose...................................................................................................................... 6
  3.2 Installation................................................................................................................ 6
  3.3 Server Configuration............................................................................................... 7
  3.4 Windows 2000 Server Configuration .................................................................. 8
  3.5 Final System Check ............................................................................................... 12
  3.6 Application-Specific Configurations .................................................................... 12
  3.7 Server Recommendations .................................................................................... 13

4 Naming Standards.......................................................................................................... 14
  4.1 Purpose...................................................................................................................... 14
  4.2 Workstation Naming Standard.............................................................................. 14
  4.3 Server Naming Standard ....................................................................................... 15
  4.4 Domain Naming Standard..................................................................................... 16

5 Security ............................................................................................................................ 17
  5.1 Purpose...................................................................................................................... 17
  5.2 System Installation................................................................................................... 17
  5.3 Post-Installation ...................................................................................................... 18
  5.4 Miscellaneous Security Settings ............................................................................ 20
  5.5 Recommendations for New Domains .................................................................... 20

6 Computer Imaging Requirements and Procedures ...................................................... 25
  6.1 Purpose...................................................................................................................... 25
  6.2 Requirements .......................................................................................................... 25
  6.3 Accounts.................................................................................................................. 25
  6.4 Required Image Software ......................................................................................... 26
  6.5 Installation Checklist................................................................................................. 28
  6.6 Joining a Domain ..................................................................................................... 28
  6.7 Creating School-Specific Images .......................................................................... 28

7 Refurbished or Donated Computers............................................................................... 32
  7.1 Purpose...................................................................................................................... 32
  7.2 Configuration Goal ................................................................................................ 32
  7.3 Workstation Requirements .................................................................................... 32

8 Asset Tagging .................................................................................................................. 33
1 Overview

1.1 Purpose
The Chicago Public Schools’ Network Management Guidelines define a network infrastructure that provides secure, available, and reliable data for all end-users connected to the Chicago Public Schools’ Wide Area Network (WAN).

In an effort to provide district-wide support, the Office of Technology Services (OTS) is currently implementing a district-wide technology management tool and an enterprise anti-virus (AV) solution designed to help school Technology Coordinators and OTS staff to troubleshoot, update, track, and otherwise manage our growing technology base.

As the Chicago Public Schools (CPS) continues to integrate technology into all facets of our schools, managing that technology becomes increasingly important. The following sections provide guidelines for servers, desktops, and laptops connected to the CPS network.

1.2 Intended Audience
This document is intended for Technology Coordinators, Network Administrators, Network Engineers, Strategic Sourcing vendors and all others who are responsible for the configuration, management, or support of the CPS network environment. It assumes that the reader has general knowledge about network technologies and is familiar with common computer terminology. Additionally, the reader should understand that these steps may vary based on the configuration of a particular system. It is assumed that the reader has enough knowledge to access and use the programs and tools discussed without explicit instruction.

1.3 Scope
The requirements set forth in this document will assist OTS and schools across the district in securing their desktops, laptops, and server operating systems for each site.

1.3.1 Network Standards
The CPS Policy for Network Standards describes computer equipment and network configurations supported in the CPS environment. The Minimum Hardware, Software and Network Standards describe both minimum and recommended configurations. The complete standards document is available online at http://www.cps.k12.il.us/Network_Standards.pdf.
2 LAN and WAN Guidelines

2.1 Purpose
CPS is following a business model to establish a centralized network that will provide continuous technology support for education. Any unit or school that connects machines to CPS’s WAN can affect connectivity at all other schools and units; therefore, everyone is responsible for network management and security.

2.2 General Standards
The guidelines provided in this document are based on the Policy for Network Standards. The following guidelines represent the recommended network requirements for all computer hardware and software configurations to function properly within CPS’s Local Area Network (LAN) and WAN environments. These guidelines represent the strategies necessary to take advantage of current and future computer and educational technologies.

2.2.1 Requirements
- Naming standards are required on all devices connected to the network (see Section 4).
- All computer equipment (network and standalone) must be asset-tagged and registered in the OTS database (see Section 8).
- IP addressing must follow CPS guidelines.
- The centralized anti-virus solution is the only anti-virus software allowed on the network.
- For computers attached to the network, the Systems Management Server (SMS) client must be on all PC machines, and NetOctopus and Timbuktu clients must be on all Macintosh machines.
- All new purchases must be from pre-qualified vendors named on the Strategic Sourcing vendors list. Contact the Office of Procurement and Contracts at 553-2280 or visit http://www.csc.cps.k12.il.us/purchasing/ss_Vendors.html (see Section 6).
- All donated equipment must first be received by External Resources and Partnerships to ensure that it meets minimum standards and that all required software is installed (see Section 7).

2.3 Workstation Requirements
- All computers attached to the network must be at least Pentium I class 100 MHz, Celerons and Power PC workstations or equivalent with at least 32 MB RAM.
- Logging on to a domain is required for full service support.
- All Administrative computers must be completely compatible with the WAN, capable of running the CPS administrative footprint, and hardwired for security purposes.
2.4 Server Requirements

- All servers attached to the network must be at least Pentium II class 233 MHz and Power PCs or equivalent with at least 128 MB RAM.
- All new servers need to be registered with OTS using the Server Request Form (see Appendix A).

2.5 Anti-virus Software

It is imperative to install anti-virus software and to keep the most current virus signatures on all Internet and intranet systems. OTS has established an enterprise anti-virus solution that automatically updates systems at the schools. The products used are Trend Micro (Wintel) and McAfee Virex (Macintosh).

OTS will provide licenses for Trend Micro products. Licenses for McAfee Virex will be included in the cost of Macintosh equipment sold by Strategic Sourcing vendors.

2.5.1 Trend Micro

Trend Micro enterprise protection strategy delivers centralized deployment of outbreak detection, protection, assessment, and cleanup throughout the network.

2.5.1.1 Trend Micro OfficeScan

Trend Micro OfficeScan 5.01 or higher is required on all networked computers in order to keep the network virus-free. CPS has an enterprise license that will automatically update signatures whenever necessary to ensure a reliable and stable operating environment. Each school will be provided with Trend Micro anti-virus software, which will be continuously updated to provide comprehensive proactive protection for the entire network. Trend Micro is the district’s sole virus solution for the Wintel PC platform. Please note that all other anti-virus products must be removed from your computer.

2.5.1.2 Trend Micro ServerProtect

ServerProtect efficiently safeguards multiple servers and domains from virus attacks with next generation anti-virus software that can be installed and managed from a single secure console. Trend Micro ServerProtect is required on all servers.

2.5.1.3 Trend Micro ScanMail

ScanMail for Microsoft Exchange detects and removes viruses hidden in e-mail attachments and public folders in real time before infections can spread to the desktop. It is required on all Exchange Servers. Schools are responsible for finding, utilizing, and updating appropriate anti-virus software on non-Exchange mail servers.

2.5.1.4 Trend Micro OfficeScan for Standalone Machines

For machines that do not have Internet access, a process is available for administrators to manually update OfficeScan (see Appendix B).
2.5.2 McAfee Virex

Virex 7.x or higher is required on all Macintosh computer systems connected to the network. Virex completely protects your Macintosh from every source of virus infection whether you are downloading files from the Internet or copying files from a diskette or server. It features universal scans, scheduled scanning and compressed file scanning with a user-friendly interface. Virex will utilize its built-in eUpdate utility to ensure that all virus signature files are current.

2.6 Desktop Management

Desktop management software is required for both the Wintel and Macintosh platforms.

2.6.1 Systems Management Server (SMS)

Systems Management Server (SMS) is CPS’s network management tool for PCs. A SMS client file must be on all networked Wintel computers and servers to provide for remote support. Support includes, but is not limited to, computer maintenance, field support, updates, inventory, security, management, and administration. In order to ensure that SMS functions properly, Windows 9x clients will need to run a login script provided by OTS. For local domains, the SMSLS.bat file must be included in the login script for all users. Furthermore, local domains will need to establish a trust relationship with the enterprise domain.

2.6.2 NetOctopus and Timbuktu

NetOctopus and Timbuktu are CPS’s network management tools for the Macintosh platform. Timbuktu and a NetOctopus agent will be installed on all networked Macintosh computers. This will provide for remote support options, which include, but are not limited to, computer maintenance, field support, updates, security, management, and administration.

2.7 CPS Security Provisions

CPS is committed to providing and managing the following network security solutions.

2.7.1 CPS Virtual Private Network (VPN)

A VPN is a private network that uses a public network like the Internet to connect remote sites or users together. A VPN uses "virtual" connections to simulate real-world connections. For schools, a VPN provides connections to administrative services from workstations that are not connected to the administrative VLAN.

CPS’s VPN client is intended to be used on an as-needed basis to access internal resources such as Mapper. The VPN permits secure, encrypted connections between CPS’s private administrative network and remote users, and it insures that outside attackers cannot gain access through a connected client machine.

CPS utilizes CheckPoint SecurRemote and SecureClient software for the VPN. No other VPN software is supported.
VPN benefits include:
- Allowance of administrative access on instructional VLAN
- Extended geographic connectivity
- Improved productivity
- Improved security
- Provision of global networking opportunities
- Provision of broadband networking compatibility

For additional VPN information (VPN Request Form, installation instructions, licensing agreement, etc.), see http://vpn.cps.k12.il.us.

2.7.2 Content Filtering
CPS is responsible for providing content filtering for all users of our network; as such, schools may not have their own filtering systems. This includes all software and/or hardware solutions.

2.7.3 Firewalls
CPS provides the firewalls for all schools. Schools may not institute their own firewalls as they will disrupt communications, support, and network management.

2.7.4 New Servers
In order to add a new server to the network, schools should configure the server and then complete and forward a Server Request Form to OTS (see Appendix A).

All servers must be configured with static IP addresses according to the CPS IP addressing guidelines. IP addresses for schools can be viewed at http://erate.cps.k12.il.us. If a server will be used throughout the school, it is recommended that it be placed in the MDF room so it is secure and centrally located within the LAN.

2.7.5 Restrictions
Schools may not run:
- Proxy servers, which would conflict with required centralized content filtering
- Remote Access Servers (RAS) for security reasons
- WINS, which would conflict with services provided by the Central Office
- DNS (unless a local Active Directory domain is implemented), which would conflict with services provided by the Central Office
- DHCP, which would conflict with services provided by the Central Office
- Active Directory Services on any newly installed server without the approval of OTS

Note: Linux and UNIX servers are not supported.
3 Server Installation and Configuration

3.1 Purpose
The following guidelines explain the process by which Windows-based servers are to be setup on the CPS network. These steps ensure that the devices meet the requirements for connection to the WAN. Note that the only requirement for setting up Macintosh servers is that the NetOctopus, Timbuktu and Virex clients must be installed.

3.2 Installation
Minimum configurations on servers are 233 MHz or PowerPCs for Macintosh machines. See complete documentation on minimum server configurations at http://www.cps.k12.il.us/Network_Standards.pdf (see Section 5.2).

3.2.1 Pre-Windows Setup
1. Windows 2000 is the standard CPS Windows OS, unless an application specifically requires otherwise.
2. Make sure hardware is updated with the latest BIOS and firmware revisions.
3. Make sure all RAID and SCSI drivers are obtained and loaded automatically during the initial Windows setup screens. If not detected by the setup disks, press F6 before setup runs.
4. General RAID Guidelines:
   a. RAID0: I/O intensive functions
   b. RAID1: Lots of disk space; fault tolerance (mirror)
   c. RAID5: Lots of physical disks and local data storage/retrieval
5. Delete all existing partitions, unless a vendor system utility partition exists.
6. Partition Recommendations:
   a. 8GB=C:\; Remaining space=D:\; if>40GB, create another logical drive
7. Format all partitions to be NTFS.
8. Name and registration should be: [name of school]/CPS.
9. Server licensing should be per server, unless otherwise specified.

3.2.2 Add-On/Removal During Install
1. Remove all default selections, e.g., Index Services, Accessories, etc.
2. For remote accessibility, install Terminal Services.

3.2.3 Security Updates and Patches
1. Install the latest OS Service Pack - currently SP3 for Windows 2000.
2. Install the latest OS critical updates.
3. Install the necessary OS hotfixes.
4. Install the latest CPS tested and approved IE, currently IE 6 for servers.
5. Install the latest IE updates.
6. For IIS, see Section 3.6.1 for detailed instructions on updates, patches, checklists and lockdown tools.
8. Rename the default Administrator account to a non-descriptive account name, e.g., ‘architect’.
9. Create a separate administrator account for those who need local administrator rights and are not Domain/Network Administrators.
10. Review the Windows 2000 Baseline Security Checklist for any additional setup steps needed. The most current checklist is available on Microsoft’s TechNet site.

3.3 Server Configuration

3.3.1 Computer Properties
1. Change display time to 0 seconds.
2. If the server crashes, set to automatically reboot.
3. Optimize performance for background services, if server’s role is to run background network services such as IIS.
4. Optimize performance for applications if server’s role is to host heavily used applications.
5. Optimize performance for file sharing.
6. Partition volume names should be: C=System, D=Data, E=Data2.
7. Page File should be set to:
   a. C:\=default minimum; set min and max to the same; ignore windows warnings.
   b. D:\=1.5-2x Physical memory; set min and max to the same.

3.3.2 Network Properties
1. Identify designation network segment and configure appropriate TCP/IP network properties.
2. Server optimization (file and print sharing properties):
   a. Maximize data throughput for file-sharing (user data, file storage).
   b. Maximize data throughput for network applications (client/server sharing applications).
3. Make sure NICs are running at 100Mbps/Full Duplex.
4. If only using one NIC, uninstall any teaming functions.
5. Uninstall any unnecessary network protocols and components, e.g., NetBEUI.

3.3.3 Miscellaneous
1. Set Display Properties to:
   a. 256 or 16-bit Color
   b. No themes or screensavers
2. “My Computer” text = COMPUTERTNAME
3. “Network Places” text = CPS Network
3.4 Windows 2000 Server Configuration

This section outlines the steps necessary to secure computers running Windows 2000 Server either on their own or as part of a Windows NT or Windows 2000 domain. These steps apply to Windows 2000 Server and Windows 2000 Advanced Server.

3.4.1 File System

NTFS partitions offer access controls and protections that are not available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your server are formatted using NTFS. If necessary, use the CONVERT.exe utility to non-destructively convert your FAT partitions to NTFS.

Warning: If the CONVERT.exe utility is being used, it will set the security permissions (ACLs) for the converted drive to “Everyone: Full Control.” Use the FIXACLs.exe utility from the Windows 2000 Server Resource Kit to reset the security permissions to values that are more appropriate.

Remove all unnecessary file shares

All unnecessary file shares on the system should be removed to prevent possible information disclosure and to prevent malicious users from using the shares as an entry to the local system (see Section 5.3.2.2).

3.4.2 Accounts

3.4.2.1 Administrator Account Password

Windows 2000 allows passwords of up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and non-printing ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or non-printing ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronized across multiple servers. Different passwords should be used on each server to raise the level of security in the workgroup or domain.

3.4.2.2 Disable or Delete Unnecessary Accounts

The list of active accounts for both users and applications on the system in the Computer Management snap-in should be reviewed regularly. Any non-active accounts should be disabled and accounts that are no longer required should be deleted.

3.4.2.3 Disable Guest Account

By default, the Guest account is disabled on systems running Windows 2000 Server. If the Guest account is enabled, disable it.
3.4.2.4 Administrator Account Configurations
Because the Administrator account is built-in to every copy of Windows 2000, it presents a well-known objective for attackers. To make it more difficult to attack the Administrator account, follow the steps below for the domain Administrator account and the local Administrator account on each server:
1. Rename the account to a non-obvious name, e.g., not "admin," "root," etc.
2. Create a new Administrator account.
3. Disable the local computer's Administrator account.
4. Establish a decoy account named "Administrator" with no privileges. Scan the event log regularly looking for attempts to use this account.
5. Enable account lockout on the real Administrator accounts by using the PASSPROP.exe utility.

3.4.3 Access Control List

3.4.3.1 Directory and File Protection
Clean-installed Windows 2000 systems have secure default ACLs on the file system and the registry. However, upgrades from previous versions, e.g., Windows NT 4, do not modify the previous security settings and should have the default Windows 2000 settings applied manually. For details on the default Windows 2000 file system ACLs and modifications, refer to the Default Access Control Settings in Windows 2000 document on the Microsoft TechNet Security website.

3.4.3.2 Set Appropriate ACLs on all Necessary File Shares
By default, all users have Full Control permissions on newly created file shares. All shares that are required on the system should have permissions modified such that users have the appropriate share-level access, e.g., Everyone = Read (see Section 5.3.2.2).

Note: The NTFS file system must be used to set ACLs on individual files in addition to share-level permissions.

3.4.4 Security

3.4.4.1 Disable Unnecessary Services
After installing a Windows 2000 Server, any network services not required for the server role should be disabled. In particular, consider whether the server needs any IIS components and whether it should be running the server service for file and print sharing. Disable the following unnecessary services:
- IPSEC
- DNS
- DHCP
- SNMP
- Indexing Services
Avoid installing applications on the server unless they are necessary to the server's function. For example, do not install e-mail clients, office productivity tools, or utilities that are not strictly required for the server to do its job.

### 3.4.4.2 Protect the Registry from Anonymous Access

The Windows 2000 registry editing tools support remote access by default. Only administrators, however, should have remote access to the registry. To restrict network access to the registry, add the following key to the registry:

**Hive**
```
HKEY_LOCAL_MACHINE \SYSTEM
```

**Key**
```
CurrentControlSet\Control\SecurePipeServers
```

**Value Name**
```
winreg
```

- Select winreg, click the Security menu, and then click Permissions.
- Set the Administrators permission to Full Control; make sure no other users or groups are listed; and then click OK.

The security permissions (ACLs) set on this key define which users or groups can connect to the system for remote registry access. In addition, the Allowed Paths subkey contains a list of keys to which members of the Everyone group have access, notwithstanding the ACLs on the winreg key. This allows specific system functions, such as checking printer status, to work correctly regardless of how access is restricted via the winreg registry key. The default security on the AllowedPaths registry key grants only Administrators the ability to manage these paths. The AllowedPaths key and its proper use is documented in Microsoft Knowledge Base article Q155363, *How to Restrict Access to the Registry from a Remote Computer* available at http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q153183&sd=tech&.

### 3.4.4.3 Restrict Access to Public Local Security Authority (LSA) Information

The LSA handles aspects of security administration on the local computer, including access and permissions. All users on each system should be identified and anonymous users should be restricted in order to reduce the amount of public information that may be obtained about the LSA component of the Windows NT Security subsystem. To implement this restriction, create and set the following registry entry:

**Hive**
```
HKEY_LOCAL_MACHINE \SYSTEM
```

**Key**
```
CurrentControlSet\Control\LSA
```

**Value Name**
```
Restrict Anonymous
```

**Type**
```
REG_DWORD
```

**Value**
```
1
```
3.4.4.4 Set Stronger Password Policies
To reinforce the system policies for password acceptance, use the Domain or Local Security Policy snap-in.
1. Set the minimum password length to at least six (6) characters.
2. Set a minimum password age appropriate to your network (typically between one (1) and seven (7) days).
3. Set a maximum password age appropriate to your network (typically no more than 240 days).
4. Set a password history maintenance (using the "Remember passwords" option) of at least four (4).
5. No three (3)-character sequences can be the same as the login name.
6. Three (3) of the following four (4) requirements must be met:
   a. Must contain an upper case letter (A – Z)
   b. Must contain a lower case letter (a – z)
   c. Must contain a numeric character (0 – 9)
   d. Must contain a special character (! #, ; : …)

3.4.4.5 Additional Security Settings
There are additional security features not covered in this document that should be used when securing servers running Windows 2000. Information about these security features such as Encrypting File System (EFS), Kerberos, IPSEC, PKI, and IE security is available on the Microsoft TechNet Security website.

3.4.5 Service Packs

3.4.5.1 Install the Latest Service Pack
Each Service Pack for Windows includes all security fixes from previous Service Packs. Microsoft recommends that you keep up-to-date on Service Pack releases and install the correct Service Pack for your servers as soon as your operational circumstances allow. The current Service Pack for Windows 2000, SP3, is available on the Microsoft website.

Service Packs are also available through Microsoft Product Support. More information is available on the Microsoft website.

3.4.5.2 Install the Appropriate Post-Service Pack Security Hotfixes
Microsoft issues security bulletins through its Security Notification Service. When a new security hotfix is announced, it should be immediately downloaded and installed on all servers. For information on automatic notification about hotfixes, see http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp.

3.4.5.3 Verify Patches
The Microsoft Baseline Security Analyzer (MBSA) is available via Microsoft’s download site at http://download.microsoft.com. It is the appropriate utility to verify up-to-date Windows patches and should be run periodically after configuration changes or software updates, etc.
3.5 **Final System Check**

1. Run MBSA/HFNETCHECK to verify up-to-date Windows patches.
2. Request a NESSUS scan for a thorough security check if running IIS (request a *Firewall Rule Request Form* from 3-HELP).
3. Create a system Emergency Recovery Disk and label it with the machine name and date.
4. Synchronize clocks with the appropriate central timeserver as defined below.

   ```
   NET TIME \<TIMESERVER> /SET /YES
   ```

5. The following are the CPS timeservers:
   a. 10.129.161.35 [cospcws01.csc.cps.k12.il.us] – Timeserver behind the firewall (Central Office machines)
   b. 10.128.5.45 [ilspcws01.soib.cps.k12.il.us] – Timeserver for school servers

3.6 **Application-Specific Configurations**

3.6.1 **IIS**

1. Install on data partition, i.e., D\, E\, etc.
2. If only using one IP address, make sure to unselect “Use all assigned IP addresses.”
3. Select the assigned IP (do this for both WWW and FTP services options).
4. Install the default Web/FTP directories to the data partition (D:\inetpub).
7. Install the *IIS Lockdown Tools* (see Appendix C).

3.6.2 **TS (Terminal Services)**

Under the Connections menu, select RDP Protocol Properties. If only using one IP address, be sure to unselect the default “Use all network adapters” option. Select the assigned IP.

3.6.3 **Oracle**

Install Oracle to the data partition.

3.6.4 **SQL**

1. Install to the data partition.
2. Install the latest Service Pack (currently SP2).
3. For security, assign an administrator account to the SQL Service instead of accepting the default.
3.7 Server Recommendations

3.7.1 Recommended Applications
CPS recommends specific software to extend server functionality as noted in the following chart:

<table>
<thead>
<tr>
<th>Function</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Space Management</td>
<td>Quota Manager</td>
</tr>
<tr>
<td>Tape Backup/Restore School servers</td>
<td>Veritas NetBackup or Veritas BackupExec</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>Nagios</td>
</tr>
<tr>
<td>E-mail Server</td>
<td>Microsoft Exchange</td>
</tr>
<tr>
<td>Anti-virus Software</td>
<td>Trend Micro ServerProtect</td>
</tr>
</tbody>
</table>

Table 1: Recommended Applications

3.7.2 Data Backups
1. Nagios is recommended for server monitoring. Send the WAN team notification of who should be sent pages/e-mail alerts.
   a. **Monitor critical system services** (IIS, TS, Oracle, etc.).
2. The Veritas NetBackup solution is recommended for critical data backups.
   a. **Note any database instances to backup.**
3. **OPTIONAL:** Install BGINFO for server-displayed information.
4. Join network domain (see Section 6.6).

3.7.3 Data Tracking
- Record system information (IP, MAC, port, serial number).
- Record vendor support and main contact information.
- Update KVM (keyboard, video, monitor) control unit if applicable.
- All server administrators should subscribe to the MS security bulletins.
4 Naming Standards

4.1 Purpose
Deployment of enterprise e-mail, anti-virus software, and desktop management will require that all Windows users “login” to a central domain, or domain trusted by a central domain, and thus follow enterprise-wide naming standards. Each school previously maintained its own naming conventions for domains, servers, workstations, and users. This situation created potential name collisions between schools and inherently limited the ability to provide centralized services. In addition, administration of a large environment also requires a naming convention that facilitates troubleshooting and account management. While a perfect naming convention does not exist, the recommended standards were developed to provide ease of use and unobtrusive renaming.

All computers and servers connected to the network must adhere to these naming standards. All local domains must follow a naming standard and must have a one-way trust with Central Office in order to comply with proper security and maintenance. The specific standards follow.

4.2 Workstation Naming Standard
Each workstation name is a 15-character fixed-length name composed of four fields, each serving a distinct purpose:

[admin/ins] [school unit number] [machine type] [asset tag number]

<table>
<thead>
<tr>
<th>Character Position</th>
<th>Field Width</th>
<th>Field Name</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Admin/Ins</td>
<td>A = Administrative Image I = Instructional Image</td>
</tr>
<tr>
<td>2-5</td>
<td>4</td>
<td>School unit number</td>
<td>Numeric only unit number left padded with zeros if necessary: 0000-9999</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>Machine type</td>
<td>W = Windows Workstation L = Windows Laptop M = Macintosh Workstation P = Macintosh Laptop</td>
</tr>
<tr>
<td>7-15</td>
<td>9</td>
<td>Asset tag number</td>
<td>CPS asset tag number applied to machine: 000000001-999999999</td>
</tr>
</tbody>
</table>

Table 2: Workstation Naming Table

For example, A1500W000000001 would indicate the following:

A = Admin image
1500 = Gwendolyn Brooks unit #
W = Workstation
000000001 = matches asset tag sticker applied to device
4.3 Server Naming Standard

Server names, which are seen and referenced frequently by end-users, need to be less cryptic and more intuitive than workstation names. Server names are composed of four fields, each serving a distinct purpose.

[site] [constant] [function] [sequence number]

The location is based on the existing DNS site suffix used at each school, excluding any dashes, and truncated to nine characters. DNS suffixes are available at http://erate.cps.k12.il.us under each school’s secure username and password.

The constant is the dash (-), which is used to separate the location and function of each server in the server naming standard.

4.3.1 Functional Naming Table

Functional names are always three characters. The most common are presented in the table below. Additional functional names may be created as necessary but they must be restricted to three (3) characters.

<table>
<thead>
<tr>
<th>Functional Convention</th>
<th>Naming Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVU</td>
<td>Anti-Virus Update Server</td>
</tr>
<tr>
<td>APP</td>
<td>Application Server</td>
</tr>
<tr>
<td>DBS</td>
<td>Database Server</td>
</tr>
<tr>
<td>DNS</td>
<td>DNS Server</td>
</tr>
<tr>
<td>XMB</td>
<td>Exchange Mail Server</td>
</tr>
<tr>
<td>SRV</td>
<td>File and Print Server</td>
</tr>
<tr>
<td>PSV</td>
<td>Print Server</td>
</tr>
<tr>
<td>ADM</td>
<td>Remote Administrative Management (currently SMS or NetOctopus/Timbuktu plus anti-virus)</td>
</tr>
<tr>
<td>SMS</td>
<td>SMS Server</td>
</tr>
<tr>
<td>SQL</td>
<td>SQL Database Server</td>
</tr>
<tr>
<td>VCS</td>
<td>Trend Virus Control Server</td>
</tr>
<tr>
<td>WEB</td>
<td>Web Server</td>
</tr>
<tr>
<td>WDC</td>
<td>Windows 2000 Domain Controller – Generic</td>
</tr>
<tr>
<td>IDC</td>
<td>Windows 2000 Domain Controller – INSTR Domain</td>
</tr>
<tr>
<td>RDC</td>
<td>Windows 2000 Domain Controller – ROOT Domain</td>
</tr>
<tr>
<td>ADC</td>
<td>Windows 2000 Domain Controller – ADMIN Domain</td>
</tr>
<tr>
<td>BDC</td>
<td>Windows NT 4 BDC</td>
</tr>
<tr>
<td>PDC</td>
<td>Windows NT 4 PDC</td>
</tr>
<tr>
<td>WIN</td>
<td>WINS Server</td>
</tr>
</tbody>
</table>

Table 3: Functional Server Naming Table
4.3.2 Server Naming Table

Server names can vary in length up to 15 characters according to the following table:

<table>
<thead>
<tr>
<th>Character Position</th>
<th>Field Width</th>
<th>Field Name</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2-9</td>
<td>Site Name</td>
<td>See DNS site name at <a href="http://erate.cps.k12.il.us">http://erate.cps.k12.il.us</a></td>
</tr>
<tr>
<td>V</td>
<td>1</td>
<td>Constant</td>
<td>“-”</td>
</tr>
<tr>
<td>V+1</td>
<td>3</td>
<td>Function</td>
<td>See Functional Naming Table above</td>
</tr>
<tr>
<td>V+4</td>
<td>2</td>
<td>Sequence Number</td>
<td>Numeric only sequence number to guarantee uniqueness within a site: 01-99</td>
</tr>
</tbody>
</table>

Table 4: Server Naming Table

For example, BOGAN-ADM01 would indicate the following:

BOGAN = DNS suffix for Bogan High School
ADM = Administrative management server e.g., SMS and anti-virus update
01 = First administrative management server at Bogan High School.

4.4 Domain Naming Standard

The domain architecture will provide CPS with a foundation for initiatives that will facilitate greater reliability, expanded end-user services, and more cost-effective and efficient management. The architecture will be designed to accommodate our existing needs while providing scalability for future growth.

Many schools have existing NT 4 or Active Directory (AD) domains. To prevent domain name collisions, all duplicate domains will need to be renamed according to the Domain Naming Standard. The Standard described below applies to all renaming situations as well as naming new domains.

[site] [purpose]

<table>
<thead>
<tr>
<th>Character Position</th>
<th>Field Width</th>
<th>Field Name</th>
<th>Acceptable Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2-9</td>
<td>Site Name</td>
<td>See DNS site suffix table, truncated to 9 characters</td>
</tr>
<tr>
<td>V</td>
<td>6</td>
<td>Purpose</td>
<td>Freeform: any character suffix up to 6 characters denoting purpose of domain, e.g., LAB1, TEST, etc.</td>
</tr>
</tbody>
</table>

Table 5: Domain Naming Table

For example, BOGANLAB1 would indicate the following:

BOGAN = DNS suffix for Bogan HS
LAB1 = Domain used to hold machine accounts and user accounts in a lab
5 Security

The Windows operating system provides two main networking models for connecting computers. The first model is the workgroup model. This model is intended for connecting small groups of computers and users together. There is no shared security information and no centralized management. Each user must have an account on each computer to which they need access.

The second model is the domain model. A domain employs centralized security and policy administration. Users are usually issued accounts at the domain level and those accounts can be used to access various computers and resources in the domain. The domain model is CPS’s preferred method of administering its network environment.

The two domain models currently available are NT 4.0 domains and the Active Directory integrated domains. The domain model provides more control over users and security than the workgroup model, and it is the recommendation of the OTS LAN Management Team that an Active Directory domain model be used across the district.

5.1 Purpose

Security is becoming more important as society relies more on information technology. It is important that assets be identified and classified both for security and for privacy considerations. The questions of availability and integrity must also be addressed.

Standards are created as guidelines to ensure that each unit is aware of its responsibility to the security of all other units. This ensures that the network environment will be secure from unauthorized external and internal attacks, and contingency plans can be put in place to minimize the impact of potential attacks to the total organization.

Due to customer-driven requirements, site-operating environments vary across the district; therefore, a cookie-cutter approach to security is not practical. Technology Coordinators, in conjunction with OTS, must weigh security with operational necessities. This section specifies the minimum requirements for securing a Windows operating system. Each school or site administrator may implement additional security measures as necessary to optimize and ensure a secure environment overall.

In addition to settings that may be specified through group policy or registry settings, there are several physical and operational requirements to a secure operating environment. This section details the necessary operational policies and physical security measures that should be in place.

5.2 System Installation

The following sections detail the steps that should be performed before, during, and directly after installation of servers, workstations, or laptops in order to ensure security.
5.2.1 Pre-Installation
Before connecting servers, workstations, or laptops to CPS’s WAN, installers should ensure that all systems meet the minimum hardware requirements and that all systems are configured appropriately according to these guidelines.

For all new systems, vendors who supply custom software should also ensure that their software is compatible with CPS-approved images, i.e., pre-loaded software.

Virus protection is essential to maintaining a secure environment; therefore, the appropriate Trend Micro component for Wintel machines and McAfee Virex for Macintosh machines should be installed and current at all times. OTS will provide licenses for Trend Micro products; however, licenses for McAfee Virex will not be provided by CPS and should be purchased separately.

5.2.2 Installation
Installations should be tested for a reinstall prior to rollout. In addition, for a reinstall a full backup of the existing system is recommended before installation to safeguard against any potential problems.

5.3 Post-Installation
After installation, several actions must be performed. Many of these steps may be performed during the installation if a custom installation script is used, but the creation of such a script is beyond the scope of this document.

5.3.1 Account Requirements
Several new accounts are created as part of the default installation of NT, 2000, and XP machines. As these accounts are well-known, they may represent prime attack targets. To help prevent attacks, the following accounts should be renamed or disabled: Help Assistant, Guest, Support_xxxxxxxx and Administrator.

___ The Help Assistant, Guest, and Support_xxxxxxxx accounts should be disabled.
___ The Administrator account should be renamed to Architect.

The proper maintenance of user accounts is essential to the secure operating environment; therefore, all new accounts not utilized for more than 90 days should be disabled or deleted.

5.3.2 Recommendations for Local Computer Security
There are two necessary requirements for centralized services, such as desktop management and anti-virus protection: all devices must be visible and well-known to the network, and all must be in a domain. A by-product of this requirement is that all devices will be visible to each other in the Windows network neighborhood. Since this greatly simplifies the ability for someone to view machines at other schools, it is important that proper security is configured on all devices to prevent inappropriate remote access to
files. This section discusses known security deficiencies that are being addressed as the C.L.E.A.R. remediation project moves forward.

5.3.2.1 Network Neighborhood
The view in Network Neighborhood has changed now that all machines are in the INSTR domain or in a domain trusted by INSTR. In Network Neighborhood, the list of computers is based on the domain of the workstation or server. For example, all devices in the VAUGHN domain would be visible under VAUGHN. Devices in INSTR are placed in a workgroup based on their school’s short name in an effort to keep the list of computers in the INSTR domain to a manageable level. All schools, however, will be able to see the domains and workgroups of all other schools in the INSTR domain.

5.3.2.2 Windows 9x File and Print Sharing
A large number of Windows 95/98 systems have been discovered with File and Print Sharing enabled without requiring authentication. This security exposure was present prior to the C.L.E.A.R. project but now presents an increased risk due to the ease in which systems can be seen across school boundaries. In particular, the long-term risk is that systems can be compromised in one of the following ways:

- New viruses on unprotected machines can use open network shares to infect systems.
- Users who should not have access to the data on the system have free access to read or copy files from their location as well as from other schools.
- Malicious users can erase files or data if the permissions allow Read and Write access.

To facilitate resolution of this issue while not adversely affecting local school applications or processes dependent on 9x File and Print Sharing, a report will be generated after the school is remediated, detailing all of the Windows 9x systems that have File and Print Sharing enabled without authentication. The recommendation is to enable password or user-level authentication with the lowest privilege level possible, as listed below in the order of preference:

<table>
<thead>
<tr>
<th>Read only access</th>
<th>User level security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read and Write access</td>
<td>User level security</td>
</tr>
<tr>
<td>Read only access</td>
<td>Share mode security (i.e., password protected)</td>
</tr>
<tr>
<td>Read and Write access</td>
<td>Share mode security (i.e., password protected)</td>
</tr>
<tr>
<td>No authentication</td>
<td>Not recommended due to security exposure</td>
</tr>
</tbody>
</table>

Table 6: Recommended Share Permissions

5.3.2.3 Techco Administrator Account
The C.L.E.A.R. remediation process installs a techco account for the local school Technology Coordinator in order to manage their local Windows NT, 2000, and XP workstations. This allows the Technology Coordinator to create local accounts, join the device to a domain, install new hardware/software, and reinstall corrupt components, e.g.,
software, drivers, etc. Servers should be locked down more securely than workstations and should not have the same accounts for administrator access. Recommendations are:

- Disable techco on all servers, if it exists.
- Reset the techco password on workstations to be school specific.
- The new techco password will be stored in a protected area of the LDAP database and only viewable by the Help Desk.
- The techco password will only be released to the Technology Coordinator or Principal.

5.4 Miscellaneous Security Settings

The following security settings will ensure optimal protection against unauthorized PC and/or network access.

5.4.1 Disable Remote Desktop Sharing

Remote desktop sharing enables several users to interact and control one desktop. This could allow unauthorized users to control the system; therefore, remote desktop sharing should be disabled.

5.4.2 Do Not Automatically Start Windows Messenger Initially

This setting prevents the automatic launch of Windows Messenger at user logon.

5.4.3 Always Wait for the Network at Computer Startup and Logon

This setting determines if Windows waits for complete network initialization before allowing the user to logon. Part of this initialization is the application of Group Policy. If the setting is not enabled, then a user may logon before all Group Policy Objects (GPO) are obtained and processed, causing the user to temporarily operate under an incorrect security context. To prevent this from occurring, the setting should be enabled.

5.5 Recommendations for New Domains

Because every domain that is added to the infrastructure introduces increased overhead, complexity, and cost, it is important to fully understand the business drivers associated with the decision to introduce a new domain. The table below outlines the business drivers behind requests for local school domains along with recommendations when a new domain represents the best alternative to utilizing existing INSTR AD infrastructure. In general, most business requirements can be accommodated simply through delegation of administrative rights at the school Organizational Unit (OU) level.

5.5.1 Domain Business Drivers

The following table lists the known business drivers for utilizing a domain at a school and describes how each driver would be implemented within the INSTR domain. From a security standpoint, the primary goal is to provide the necessary functionality to the school without necessitating full INSTR domain-level privileges. Where this cannot be achieved, a separate domain would be required. Note that the global groups (GG) listed below are specific to a school OU within the INSTR domain.
<table>
<thead>
<tr>
<th>Driver</th>
<th>Description</th>
<th>How this would be achieved for a school using INSTR domain</th>
<th>Separate Domain Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add printers, workstations, and member servers to a pool of shared resources at a school OU in INSTR.</td>
<td>Members of global groups GG-Tech and GG-Computer Managers have rights to add and share resources.</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Create user accounts for access to shared resources (see Section 5.5.3).</td>
<td>Accounts are created automatically through LDAP and GG-Tech and GG-User Managers have rights to provide access to resources.</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>Create accounts in a timely manner, which are not automatically created through LDAP.</td>
<td>GG-Tech and GG-User Managers can create accounts in Local Temporary OU under the school OU.</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>Create home directories and establish disk quotas.</td>
<td>GG-Tech is given membership in local servers’ Administrators groups.</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>Manage user profiles, group policies, and school specific login scripts.</td>
<td>GG-Tech can create and modify external templates that can be used for these management tasks.</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>Require fault tolerance or increased performance of local DC.</td>
<td>INSTR domain controller could be installed in MDF of school as “appliance” with no direct access allowed or required for the school.</td>
<td>No</td>
</tr>
<tr>
<td>7</td>
<td>Implement student e-mail and have access to the full Outlook client as opposed to existing OWA.</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>8</td>
<td>Isolated LAN or test environment.</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 7: Domain Business Drivers

5.5.2 School OU Ownership

The INSTR domain is designed to offer key centralized services while maintaining a distributed support model. As a result, each school is given full rights to its own OU container and sub-containers within the INSTR Active Directory tree with the following exceptions:

- User accounts cannot be created or deleted from the following OU containers since these are managed through an automated LDAP interface:
  - Users
  - Users\Staff
  - Users\Students
- Schools requiring the ability to create user accounts outside of the LDAP process may do so by creating them in the Local Temporary OU under the school OU.
- All user account attributes such as group membership, passwords, logon hours, etc., are settable through AD. To facilitate automated management of accounts created through LDAP, however, external templates can be provided to pre-populate the following attributes individually by school:
  - User home directory
Each school may create two templates, one for students and one for staff. In addition, the school will be able to freely modify attributes of the template accounts.

- Schools will be unable to create new OU containers within AD but can request OTS to create additional containers on an exception basis to satisfy a valid business requirement.

The rights automatically given to the school include, but are not limited to, the creation and management of workstation accounts, printers, groups, group policies, and shared folders for their school.

5.5.3 Account Management

One of the largest burdens organizations must bear when managing domains is user account maintenance. This includes user account creation, deletion, password resets, group membership, group policies, and associated rights. This is especially true for student accounts where a large percentage of the accounts must be deleted for graduating students and added for incoming and new students. To help alleviate this burden, an automated LDAP-based account management system has been integrated with centrally provided INSTR domain access. It maintains automatic synchronization with the Human Resources (HR) and student databases by creating/deleting accounts as necessary. The characteristics of this system are as follows:

- Domain accounts are created for all employees based on HR information.
- Domain accounts are created/deleted for all high school students automatically.
- Domain accounts are created for elementary and middle school students on a per-school basis, based on requests from the school.
- All domain accounts are located in the INSTR domain under the appropriate school OU Users container. For system integrity, schools will be restricted from creating and deleting user accounts under the school Users container.
- Additional accounts outside the automated process may be requested through the Help Desk (3-HELP).
- A Local Temporary container exists for each school to provide the ability to create accounts outside of the automated LDAP process. The management of the Local Temporary container is the responsibility of the school.
- Domain accounts will be created once the account is entered into the legacy HR or SI systems.

5.5.4 Exchange 2000

Exchange 2000 Outlook Web Access offers similar functionality to Outlook such as shared calendar support and an attractive user interface. As a result, it is unnecessary to create a local domain solely to address Exchange functionality concerns.

5.5.5 Student E-mail

Currently, student e-mail is not centrally supported.
5.5.6 Domain Scenarios

Below are several tradeoffs that must be considered when determining the best approach for implementing additional domains:

- **Account Management:** A domain requires someone to add, create, and modify user accounts, passwords, profiles, security and other attributes. A major goal of the centralized INSTR domain is to automate the creation of employee and student accounts using an interface connected to the master employee and student databases. This mitigates the large task of managing user account creation/deletion for all users contained in the INSTR domain. In contrast, the burden of account management for local school domains would fall on the school. In some cases, schools may want to perform account management to meet business needs regardless of the account management overhead.

- **Explicit Trusts:** Each domain in another forest requires a manual trust be established with the INSTR domain. Trusts can break during WAN outages, requiring periodic maintenance. As the number of trusts increases, the probability also increases that users and support staff will be impacted by a trust breaking.

- **Security:** Managing a domain controller requires significant responsibility. Inadvertent schema changes or mass object creation on an enterprise domain can cause excessive replication traffic and can create a denial of service condition. In addition, a domain administrator has full access to all directory objects on a domain controller and can take ownership of objects in the configuration and schema using services on the domain controller. Therefore, domain administrators should be trusted individuals within schools and the CPS environment. In general, the chance for security vulnerabilities to be discovered and exploited is increased as the number of domains increases.

- **DNS Configuration:** Separate forests require special DNS settings in order to establish trusts properly with the INSTR domain. These settings can be problematic to manage and may depend on individualized workstation settings.

- **WAN Traffic:** Implicit and explicit trusts require additional WAN traffic and therefore, latency, to authenticate users for inter-domain resource access. There is always a balance between user logon/authentication traffic and replication traffic. Many schools may warrant the local placement of an INSTR Domain Controller (DC) to offset the logon traffic of a large user base.

- **Fault Tolerance:** With no local DC, the WAN link is a single point of failure.

- **Additional Hardware Required:** Active Directory represents a single point of failure and as such, a minimum of two DCs should be utilized to maintain a database. Alternatives such as restoring AD from tape can be problematic since all existing information such as user/group account changes, passwords, trusts, etc., can be lost from the time of the most recent backup. Workstations may require a technician visit to rejoin them to the domain due to secure channel synchronization failure. In addition, it is not best practice to host web services from a DC due to the security risks present in most web applications.

The following table presents additional information about domain scenarios available for schools.
<table>
<thead>
<tr>
<th>CASE</th>
<th>Description</th>
<th>Forest Implications</th>
<th>User Account Management</th>
<th>Forest/Domain Management</th>
<th>Kerberos Trust</th>
<th>NT/Explicit Trust</th>
<th>Security</th>
<th>DHCP/show margins</th>
<th>Scalability/WAN Traffic</th>
<th>Add'l Local DCs</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Utilize INSTR domain without local DC</td>
<td>Shared Global Catalog means objects in enterprise can be located easier</td>
<td>Burden is on enterprise - school can perform most administrative tasks based on delegations to their school OU</td>
<td>Burden is on enterprise</td>
<td>No additional trusts are required</td>
<td>None</td>
<td>Security is maintained at the Central Office</td>
<td>Standard</td>
<td>Least replication traffic, most authentication traffic</td>
<td>0</td>
<td>Use for most small to medium size schools that do not need burden of local account management or e-mail</td>
</tr>
<tr>
<td>2</td>
<td>Utilize INSTR domain with local DC (DC maintained by Central Office)</td>
<td>Shared Global Catalog means objects in enterprise can be located easier</td>
<td>Burden is on enterprise - with each new DC, CPS/OTS administration overhead increases</td>
<td>Burden is on enterprise</td>
<td>No additional trusts are required</td>
<td>None</td>
<td>Moderate risk even if local DC is physically secure - schools maintain administrative authority at their own school only</td>
<td>Standard</td>
<td>Most replication traffic, least authentication traffic</td>
<td>1+</td>
<td>Use for medium to large schools that do not need burden of local account management or e-mail but want additional fault tolerance or logon performance</td>
</tr>
<tr>
<td>3</td>
<td>Utilize existing local school domain or establish a new one (DC is maintained by the school)</td>
<td>Separate from INSTR - separate Global Catalog</td>
<td>Burden is on school for creating, deleting, and modifying accounts, resetting passwords, and managing profiles</td>
<td>Burden is on school for maintaining forest/schema system security policies</td>
<td>Must traverse additional trusts for authentication to INSTR resources</td>
<td>Requires management of explicit one-way trust between school domain and INSTR</td>
<td>Minimal chance of Global Catalog impacts due to inadvertent schema changes by domain administrator</td>
<td>May require special DNS settings at the workstations for external trust</td>
<td>Least amount of logon, authentication and replication traffic - most scaleable</td>
<td>1+</td>
<td>Use if domain already exists at school or if school wants additional e-mail accounts or features or for a test lab environment</td>
</tr>
</tbody>
</table>

Table 8: Domain Scenarios
6 Computer Imaging Requirements and Procedures

6.1 Purpose
This section details CPS’s hardware and software requirements and procedures for installing multiple computers with a single image. It is intended for Strategic Sourcing vendors, school Technology Coordinators and others involved in providing and supporting computer equipment to CPS sites.

6.2 Requirements
All new equipment purchased by CPS should be acquired from Strategic Sourcing vendors. See Appendix D for details on the process. The LAN management team requires the following from Strategic Sourcing partners and others who might image CPS computer equipment:

- All hardware sold from a Strategic Sourcing vendor must have a CPS-approved image.
- All hardware sold must be asset-tagged per the asset tagging and tracking policy (see Section 8).
- Strategic Sourcing vendors must meet weekly or bi-weekly with the CPS imaging team.
- All hardware installed by Strategic Sourcing business partners or others must adhere to CPS naming standards and conventions (see Section 4).
- All hardware images used by vendors must be tested and approved by CPS personnel.
- Vendors must provide to CPS the appropriate hardware with significant lead-time for image creation and testing prior to the release of new hardware for purchases.
- Strategic Sourcing vendors, Technology Coordinators, and others must provide licenses for any software used to image new machines.
- The license cost of all ancillary software, utilities and/or packages, i.e., SMS CAL, Office XP, Exchange 2000 CAL, etc., must be included in the purchase price of hardware.
- All installation costs must be included in the purchase price of hardware, i.e., mandatory business partner onsite setup should occur upon hardware delivery.
- Restore CDs with the CPS image for each hardware type should be included with each computer purchase.

6.3 Accounts
The following tables outline the required accounts for computers connected to the CPS network. These accounts should not be changed or deleted.
Image Account Matrices

<table>
<thead>
<tr>
<th>CPS Instructional Network – Local User Accounts:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACCOUNT NAME:</strong></td>
</tr>
<tr>
<td>-------------------</td>
</tr>
</tbody>
</table>
| Architect         | Built-in Administrator account | • User cannot change password  
|                   |                 | • Password never expires  | Administrator | CPS and business partners |
| Guest             | Built-in Guest account | • User cannot change password  
|                   |                 | • Password never expires  
|                   |                 | • Account disabled  | Guest | None |
| School            | Generic login account | • User cannot change password  
|                   |                 | • Password never expires  
|                   |                 | • Account disabled  | Power User *plus the ability to load drivers | School Users |
| TechCo            | Technology Coordinator account | • User cannot change password  
|                   |                 | • Password never expires  | Administrator | Technology Coordinators |
| Administrator     | Bogus account | • User cannot change password  
|                   |                 | • Password never expires  
|                   |                 | • Account disabled  | Guest | None |

<table>
<thead>
<tr>
<th>CPS Administrative Network – Local User Accounts:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACCOUNT NAME:</strong></td>
</tr>
<tr>
<td>-------------------</td>
</tr>
</tbody>
</table>
| Architect         | Built-in Administrator account | • User cannot change password  
|                   |                 | • Password never expires  | Administrator | CPS and business partners |
| Guest             | Built-in Guest account | • User cannot change password  
|                   |                 | • Password never expires  
|                   |                 | • Account disabled  | Guest | None |
| Office            | Generic login account | • User cannot change password  
|                   |                 | • Password never expires  | Power User *plus the ability to load drivers | User |
| Administrator     | Bogus account | • User cannot change password  
|                   |                 | • Password never expires  
|                   |                 | • Account disabled  | Guest | None |

Table 9: Required Accounts on CPS Images

6.4 Required Image Software

The software detailed in this section is for Wintel systems only. There is no standard image required for Macintosh computers other than the NetOctopus, Timbuktu and Virex clients. In addition to the software listed, the required SMS client must always be included as listed in Section 6.5. The SMS client is always installed after imaging is completed.
6.4.1 Instructional Image - Windows XP

**Operating System:** Windows XP

**Software:** Office XP with sp1, which includes:
- Word XP
- Excel XP
- PowerPoint XP
- Access XP
- MS Front Page XP
- MS Office Classroom Tools

Internet Explorer 6.0
Adobe Acrobat Reader (current version)
Trend Micro Antivirus Software – OfficeScan (current version)
Windows Media Player (current version)
Macromedia Flash Player (current version)
Macromedia Shockwave (current version)
Apple Quick Time (Windows version)
WinZip 8.0

**NOTE:** Always remove Online Services, including AOL, CompuServe, etc., and desktop themes.

6.4.2 Administrative Image

**Administrative Image - Windows XP**

**Operating System:** Windows XP

**Software:** Office XP with sp1, which includes:
- Word XP
- Excel XP
- PowerPoint XP
- Access XP
- MS Front Page XP
- Outlook XP

Internet Explorer 6.0 (5.5 on Kronos machines)
Oracle Chart of Accounts
Oracle access client (version 11.0.300)
MPC - Mapper Presentation Client (current version)
Personal Communications - AS400 application and AIMS terminal emulation
Adobe Acrobat Reader (current version)
Trend Micro Antivirus Software – OfficeScan (current version)
Windows Media Player (current Version)
Macromedia Flash Player (current version)
Macromedia Shockwave (current version)
Apple Quick Time (Windows Version)
WinZip 8.0

**NOTE:** Always remove Online Services, including AOL, CompuServe, etc., and desktop themes.
6.5 Installation Checklist

Before connecting servers, workstations, or laptops to CPS’s WAN, installers should ensure that all systems meet the minimum hardware requirements and that all systems are configured appropriately according to this document.

For all new systems, vendors who supply custom software should also ensure that their software is compatible with CPS-approved images, i.e., pre-loaded software as listed in Section 6.4.

Basic steps required for new systems include:
1. Connect to network
2. Rename PC – (see Section 4: Naming Standards)
3. Complete virus scan of machine
4. Configure OfficeScan to point to distribution server
5. Install critical updates from Microsoft – (see WindowsUpdate.com)
6. Install SMS client (see Manual Installation of SMS in Appendix E)
7. Join network domain
8. Updating OfficeScan should occur automatically

6.6 Joining a Domain

The process of joining a domain from a workgroup will have two effects on NT class machines or above:
• New user profile will be generated
• Domain administrators’ rights on local device will be enabled

The system will be joined into the INSTR domain or the ADMIN domain if at the Central Office.

Once the system has a domain account, a user will need to login with a domain account and password to use the workstation. Each school has generic accounts, or users can login with their own domain accounts and passwords. Account information is available at http://erate.cps.k12.il.us or by calling the Help Desk (3-HELP).

6.7 Creating School-Specific Images

NOTE: OTS will not support machines re-imaged with a school-specific image.

6.7.1 Introduction

To save setup time and resources, many schools utilize disk duplication products, such as Symantec Ghost, in order to clone a master workstation configuration onto multiple clients. While this is a very desirable goal, care must be taken to properly integrate standard elements into the master image in order to maintain compatibility with the CPS network. The guidelines below discuss the CPS-recommended method for performing disk duplication of a Wintel platform.
6.7.2 Process Overview
If the concepts of disk duplication, Sysprep, the remediation script, and SMS installation are familiar, the tables below will provide all of the information that is needed to successfully deploy a duplicated workstation. If they are not familiar, additional information is provided in the C.L.E.A.R. remediation and SMS installation procedures that were distributed to each Technology Coordinator.

6.7.3 Recommended Operating Systems
For maximum hardware and software compatibility, the following is the preferred order of operating systems that should be used for master images:
- Windows XP formatted with NTFS File System
- Windows 2000 formatted with NTFS File System
- Windows 98 Second Edition formatted with WIN32 File System

NT 4 can be cloned as well but is particularly difficult due to the lack of Plug and Play support. As a result, the image owner must be intimately familiar with and install all possible video, sound, network, and disk drivers in the image for a successful deployment.

6.7.4 Sysprep
For Windows NT, 2000 and XP, it is important to use Sysprep on the master image just before duplication. This prepares the system for duplication so that a unique SID and computer name is generated after the device is cloned during the mini-setup phase. It should be noted that this is the only “Microsoft Supported” method of cloning NT class PCs.

6.7.5 Windows Update – Critical Updates Only
It should be noted that the C.L.E.A.R. remediation script focuses solely on Critical Updates since this is where known security exposures lie. The current remediation script brings critical patch levels current through September 23, 2002. Subsequent updates must be applied manually (via Windows Update) at the end of the remediation process.
6.7.6 School Specific Image Steps

The following tables detail basic steps required to create a master image and clone that image onto multiple clients. Consult specific imaging software for additional required steps.

<table>
<thead>
<tr>
<th>Step #</th>
<th>High Level Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a clean base image</td>
<td>If possible, start with a standard, clean CPS image. Otherwise start from a base OS install, install all necessary drivers and then run the C.L.E.A.R. remediation script. This will approximate a “standard” image. &lt;br&gt;Check the Control Panel and make sure that SMS is not installed and uninstall if necessary per the manual SMS (SMSMAN.EXE) procedures (see Appendix E). It is recommended that the C: drive partition be partitioned to at least 8GB or as large as possible. Note also when starting from a standard CPS image: &lt;br&gt;• If there is a recovery partition, it should not be changed or overwritten. &lt;br&gt;• Partition sizes and formatting should not be changed. &lt;br&gt;• User accounts should not be changed or removed. &lt;br&gt;• Software installed on the standard CPS image should not be removed.</td>
</tr>
<tr>
<td>2</td>
<td>Install application software and configure the “All Users” and “Default User” profiles</td>
<td>• Create a local user master account with Administrator privileges and log on as that user to install and customize applications that will be common for all workstations created from this image. On devices with NTFS, be sure to enable user access permissions for typical users. Disable or remove all non-essential services from automatic startup and task bar. &lt;br&gt;• For Windows NT, 2000 or XP, once the system has been fully customized, log off as the local master user and log back on as Administrator. Then copy the local master user profile to the Default Users folder.</td>
</tr>
<tr>
<td>3</td>
<td>Remediate the image as a standalone PC</td>
<td>Run the latest remediation script version to bring the workstation into compliance with current networking standards and patch levels. Remediate the master image as a standalone PC since network related tasks will be performed after duplication. Finally, to prepare the remediation script parameters for cloning, reset a number of registry values such as room #, serial #, etc., by running \cpsclear\common\GhostPrep.exe (included with script) from Explorer or a command prompt.</td>
</tr>
<tr>
<td>4</td>
<td>Validate the image</td>
<td>Create and login under a local user test account. Then run an audit on all applications, including software originally installed by CPS, to verify that the image configuration is correct.</td>
</tr>
<tr>
<td>5</td>
<td>Prepare for duplication</td>
<td>Delete all unnecessary user profiles, temporary files, and printers; clear the recycle bin. &lt;br&gt;• For Windows 95 and 98, run ScanDisk and Disk Defragmenter (both under Accessories\System Tools). &lt;br&gt;• For Windows NT, 2000 and XP, install and run correct OS specific Sysprep version from c: \sysprep. A Sysprep template can be obtained from CPS by contacting 3-HELP.</td>
</tr>
</tbody>
</table>

Table 10: Master Image Steps
(In order to minimize propagation of issues, it is recommended that a re-validation of the workstation image be performed on the first cloned workstation prior to mass duplication of workstations.)

<table>
<thead>
<tr>
<th>Step #</th>
<th>High Level Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Duplicate workstation</td>
<td>Use any licensed duplication software in order to duplicate the workstation. Once Sysprep has been run on Windows NT, 2000 and XP, the master computer’s hard disk has been triggered to create a unique workstation SID, force Plug and Play detection, and run the Mini-Setup Wizard the next time the system is started.</td>
</tr>
</tbody>
</table>
| 2      | Verify networking protocols and reconfigure if necessary | To cut down on network overhead and increase workstation performance, it is recommended that only the minimal necessary protocols be configured. Specifically, the following rules should be applied:  
- TCP/IP is the protocol of choice and is required for Internet access, SMS, and anti-virus updates. In many cases, this offers the best access path to all resources and is the only protocol necessary.  
- NWLink IPX/SPX (or Novell IPX/SPX) is required for workstations that must attach to a Novell server.  
- NBIPX and NetBEUI should be avoided under normal circumstances due to their broadcast intensive nature. |
| 3      | Run the latest remediation script on networked PCs | This step only applies if the device in question will be connected to the production network. If step 3 on the master image was performed correctly, re-running the script will perform only a minimal number of steps. The purpose of running the remediation process again is to perform several computer-specific tasks such as updating the database, standard naming, synchronizing OfficeScan, joining the domain, and adding necessary global groups. |
| 4      | Install SMS            | Execute the SMS manual installation procedure (SMSMAN.EXE) to ensure that SMS is installed correctly (see Appendix E). |

Table 11: Clone Image Steps
7 Refurbished or Donated Computers

7.1 Purpose
This section is intended for CPS’s Central Office staff, vendors who are responsible for building, configuring, and deploying refurbished or donated workstations, and schools that receive donations (see Appendix F).

Periodically, CPS accepts computer hardware donated from businesses and corporations. CPS is willing to accept computer donations provided the computers meet the established guidelines for connectivity to CPS’s WAN. All donated equipment must first be received by External Resources and Partnerships to ensure that it meets minimum standards and that all required software is installed.

7.2 Configuration Goal
The configuration goal is to provide schools with computer equipment that meets or exceeds CPS’s current minimum hardware, software, and network standard settings.

7.2.1 Assumptions
The following section outlines assumptions for refurbishing each intended workstation.

- All donated or used machines should be re-imaged in order to maintain standards on the network. Licensing rules as noted below apply in the same manner.
- Licenses for the operating system, Client Access Licenses (CALs) and applications, e.g., Office 97, will be included in the bottom line purchase price.
- The scope of software licensing costs includes the operating system, MS Office, Trend Micro OfficeScan, Microsoft SMS CAL, and NT Server CAL only.

7.3 Workstation Requirements
CPS’s Policy for Network Standards outlines the minimum hardware requirements for refurbished or donated workstations. The standards are based on the minimum configurations that are allowed and supported on the CPS WAN. See http://www.cps.k12.il.us/Network_Standards.pdf for the complete standards document.
8 Asset Tagging

8.1 Purpose
Asset tagging is required for all new computer installations. All computer equipment (network and standalone) must be asset-tagged and registered in the OTS database. Vendors must use Board-approved asset tags for continuity and protection against duplicates. Asset tags must be purchased from CG4 Solutions, Inc., 142 East 1200 South, Centerville, Utah 84014, 801-294-4244 x103, Max.Holloway@cg4.com (see also http://www.cg4.com).

8.2 Requirements
Asset tags must meet the following specifications:

- White with black ink
- Bar coding
- Tamper evident
- Size shown: 2 3/4" x 1 1/4"
- Place asset tag on front of machine
- Boot up and log on as appropriate

8.3 Asset Tag Assignment
The following chart shows the asset tag numbering scheme that is assigned to each Strategic Sourcing vendor. The last sequence (009000001 thru 009999999) will be used for vendors outside of Strategic Sourcing.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Asset Tag Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACER</td>
<td>001000001 thru 001999999</td>
</tr>
<tr>
<td>DELL</td>
<td>002000001 thru 002999999</td>
</tr>
<tr>
<td>IBM</td>
<td>003000001 thru 003999999</td>
</tr>
<tr>
<td>Macintosh</td>
<td>004000001 thru 004999999</td>
</tr>
<tr>
<td>PC Rebuilders</td>
<td>005000001 thru 005999999</td>
</tr>
<tr>
<td>OTHER</td>
<td>009000001 thru 009999999</td>
</tr>
</tbody>
</table>

Table 12: Asset Tag Numbers
Server Request Form
One Server per Form
Please FAX this request to 773. 553.3907

Requested by: 
Director's/Principal's Signature: 
Date: 
Phone: 
E-mail: 
Type of Server: 
Server Operating System: 
IP Address: 
Server Name: 
DNS Name: 
Detailed Purpose of Server: 
Domain Name if Applicable: 
New Domain Name if Applicable
(If Windows 2000, will you be using Active Directory?)

Office Use Only
Date Received: 
Trust Implemented: 
Local Users/Groups Configured: 
Firewall Rule Needed: 
Other Issues/Considerations: 
Work Completed by: 
Authorized by: 
Date of Completion:
APPENDIX B: Updating OfficeScan on Standalone Machines

1) From a machine with a CD-ROM burner and Internet access, go to http://www.trendmicro.com/download/pattern.asp.
2) Click on the latest pattern file (LPT351.ZIP in the page shown below).

3) Click on Save and save the file to a local folder.

4) Use WinZip to unzip the downloaded pattern file to the same directory.
5) Copy the file to a CD-R or a ZIP disk.
6) From the standalone machine, copy the pattern file to the OfficeScan directory, i.e., “OFFICESCAN NT” on Windows XP.
7) Restart the workstation.
8) Verify that the new pattern file has been loaded by placing your mouse over the OfficeScan icon on the system tray as shown below.
APPENDIX C: IIS Lockdown Screenshots and Steps

This appendix covers the procedures for:

- IIS Lockdown Procedure
- Uninstall IIS Lockdown Procedure
- Run the IIS Lockdown Wizard Unattended in IIS
- Create a Custom Server Type for Use with the IS Lockdown Wizard.

IIS Lockdown Procedure

Before running the IIS Lockdown Procedure, make sure that the current functionality of the web server to be configured is completely understood. Installation and usage instructions for the IIS Lockdown Wizard can be found at the following URL:

http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q325864&

1) No matter what template is chosen initially, the same customization options are always presented. Be sure to view the template settings.

![Screenshot of IIS Lockdown Wizard]
2) Depending on the template chosen in Step 1, various options are selected by default. Review article Q311113 on the Microsoft website.

3) Active Server Pages is needed for most web servers, and ‘Server side includes’ may be needed for server applications requiring FrontPage extensions or certain scripts.
4) MSADC is needed for most web-to-database interactions. Scripts are needed for many default web server functions, and IISAdmin is needed for remote web administration.

5) Disable URL scan as this option can be very granular and can require detailed analysis and understanding of each particular web server function. Enabling this setting will most likely render the server unusable.
6) Review the settings that will be applied. Pressing Next will apply changes that cannot be undone unless the tool is run again.

- Selected changes:
  - Disable Index Server Web interfaces (*.idq, *.sws, *.idx) script map
  - Disable Internet Data Connector Link script map
  - Disable Hypertext Reasoning (IMAP) script map
  - Disable Internet printing (printers) script map
  - Remove the spool virtual directory
  - Disable Web Distributed Authoring and Versioning (WebDAV)
  - Set file permissions to prevent anonymous IIS users from writing to content directories
  - Remove settings for Remote IIS Users from running system utilities
  - Remove “Script virtual directory”
  - Remove “MSADC virtual directory”

To change your selections, click Back. To apply the new settings, click Next.

7) Review the status of the install.

- A log file Obit-log.log is created in: %windir%\system32\netsrv. The option to view a full report is also available.
NOTE: AT THIS POINT, TEST ALL WEB SERVER FUNCTIONALITY. If there are any issues, re-start the IIS Lockdown Wizard again. The Wizard will automatically recognize that the server was already configured and launch the process to uninstall the configuration changes that were made to the server using the IIS Lockdown Wizard.

Uninstall IIS Lockdown Procedure

1) Rerun the IIS Lockdown Wizard to perform an uninstall. The only choice is to undo ALL of the options during the uninstall. The ability to remove selected features previously applied is not an option.
2) All properties should be restored during this process. The error seen below may occur if any of the defaults in Step 2 of the IIS Lockdown Procedure were changed. All other functions will be restored. Review article Q311113 on the Microsoft website for more details.

![IIS Lockdown Wizard](image)

Additional Undo Notes:

When the IIS Lockdown Wizard is started and the “This Server Was Already Configured” page appears, the previous configuration must be undone before the IIS Lockdown Wizard can be run again.

Please note the following limitations when using Undo:

The Undo operation restores the system settings that were in effect immediately before running the IIS Lockdown Wizard. Note that the Undo operation will remove any changes that were made after running the IIS Lockdown Wizard, including any virtual root directories that were created. Therefore, it is important to test the system promptly after running the IIS Lockdown Wizard. If an Undo is required, perform it immediately.

An Undo of the IIS Lockdown Wizard does not imply that you are uninstalling any of the IIS services. To uninstall an IIS service, use Add/Remove Programs in Control Panels, Add/Remove Windows Components, and select the IIS component to uninstall. Should you choose to reinstall any IIS services, the IIS Lockdown Wizard should be re-run.

When the IIS Lockdown Wizard locks down a server, it creates a log file named Oblt-log.log and saves it in the directory that contains Islockd.exe. This file contains information about every action the IIS Lockdown Wizard implemented on the system.
Run the IIS Lockdown Wizard Unattended in IIS (Q310725)

To learn how to configure the IIS Lockdown Wizard in unattended mode, see the Microsoft article found at the following URL:

http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q310725&

Create a Custom Server Type for Use with the IIS Lockdown Wizard (Q311350)

The latest version of the IIS Lockdown Wizard provides administrators with the ability to create custom server type templates. For more information, see the Microsoft article found at the following URL:

http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q311350&
APPENDIX D: New Computer Acquisition and Deployment Procedure

1. Introduction:
   As described in the *Network Management Guidelines*, network management is required in order to maintain hardware, software, and network standards. When CPS executes a purchase for new computers, it is critical that the CPS-approved image is installed on the new computers and that they are properly asset-tagged and entered into the OTS Technology Database.

2. Purpose:
   This procedure defines ‘who does what’ in order to complete the process for acquisition and deployment of new computers including desktops and servers. The procedure refers to sections in the *Network Management Guidelines* that provide the details required to perform each step in the process. For example, setting up the name of a workstation is referred to in *Section 4.2: Workstation Naming Standard*.

3. Process Steps:

   **Activity 1  Purchase Request For New Computers**
   CPS or school units issue Purchase Requests (PR) for new computers based on need and associated funding. The Strategic Sourcing business model defines approved Strategic Sourcing vendors (SSV) that may be used to provide the new computers. More information regarding acceptable vendors can be found at [http://www.csc.cps.k12.il.us/purchasing/ss_Vendors.html](http://www.csc.cps.k12.il.us/purchasing/ss_Vendors.html).

   **Activity 2  Issue Purchase Order (PO) to SSV**
   CPS Purchasing processes a Purchase Order based on the approved PR and then issues the PO to the selected SSV.

   **Activity 3  Provide SSV CPS-Approved Image Script**
   CPS’s OTS Technical Group maintains and provides the current approved image script to the SSVs. The group also provides the current approved *Network Management Guidelines* to the SSV and other process participants. The guidelines include this procedure along with standards, security, imaging, and other network management information.

   **Activity 4  Install CPS-Approved Image Script and Asset Tag**
   SSV applies the Asset Tag following the *Network Management Guidelines, Section 8: Asset Tagging*. The SSV will procure the asset tags in pre-determined blocks of numbers from the CPS-approved vendor.

   SSV installs the CPS-approved image script. During the execution of the script, the workstation or server will be named using the guidelines in
Section 4: Naming Standards. The script contains the image applications including the anti-virus, SMS and computer programs selected by CPS to be standards for the script.

SSV updates their database with asset tag and school purchasing information and provides monthly reports of purchases by school to CPS Purchasing.

Activity 5 Setup Computers at School
SSV coordinates their specific business partner to setup the computers at the school and obtain the school Technology Coordinator’s concurrence that the installation is complete. Section 5: Security contains guidelines for system installation that cover pre-installation, installation and post-installation information for the Technology Coordinator to follow as the SSV business partner performs the setup process. Section 3: Server Installation and Configuration provides the guidance for setting up servers and the process for establishing a relationship with the CPS central domain. (For the Server Request Form see Appendix A.)

Activity 6 Enter Computer Information into Technology Database
The Technology Coordinator records the computer information, i.e., computer unique name, brand, etc., into the Technology Database at http://erate.cps.k12.il.us.

END PROCESS
APPENDIX E: Manual Installation of SMS

To install or remove SMS client software from a computer, follow these steps:

1. Logon to the INSTR domain or a local domain and connect to the SMSLOGON share, volume, or directory.
2. Navigate to the appropriate .bin directory (?86.bin) for the computer’s operating system, and open the 00000409 subdirectory.
3. Run the appropriate program for that computer’s operating system:
   - SMSMAN.exe for 32-bit clients
   - SMSMAN16.exe for 16-bit clients
4. Running SMSMAN.exe displays the Systems Management Installation Wizard welcome screen, shown below.

5. Click Next to display the Select A Systems Management Installation Option screen and choose to let the Wizard automatically select installation location or to remove components.
6. Click Next to display the Completing The Systems Management Installation Wizard screen.
7. Click Finish to start the installation process.

To verify a client installation, follow the steps below:

1. Navigate to the Control Panel
2. Locate and double click on the Systems Management icon

3. Within the “General” tab, a screen with similar information as in the following picture should appear:
4. Selecting the “Sites” tab should display the updated information.

5. Selecting the “Components” tab should display individual client agents in an installed or pending state.
Use the following table as a guide to evaluate the component status:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed</td>
<td>The component has been successfully installed on the client.</td>
</tr>
<tr>
<td>Install Pending</td>
<td>The installation process for the component has been initiated, but it has not yet been completed.</td>
</tr>
<tr>
<td>Repair Pending</td>
<td>The component is being verified and reinstalled.</td>
</tr>
<tr>
<td>Reboot Required</td>
<td>The component has been repaired, but it will not initialize until a reboot has taken place.</td>
</tr>
<tr>
<td>Not Available</td>
<td>The component, although enabled at the site server, is not compatible with this computer's current configuration. This could also indicate that the client's IP address no longer falls within the site assignment rules for the SMS site and that the client component has been subsequently uninstalled.</td>
</tr>
</tbody>
</table>

This process may take up to 15 minutes to complete. Once all of the client agents are in an “Installed” state, the client installation has completed successfully. There should be seven components installed.

Please call 3-HELP for assistance, questions or troubleshooting on this process.
APPENDIX F: Donated Computer Processing and Deployment Procedures

1. **Introduction:**
   As described in the *Network Management Guidelines*, network management is required in order to maintain hardware, software, and network standards. When CPS receives a donation for new or used computers it is critical that the CPS-approved image is installed on the donated computers and that they are properly asset-tagged and entered into the Technology Database.

2. **Purpose:**
   This procedure defines ‘who does what’ in order to complete the process for processing and deploying donated computers including laptops, desktops, and servers. The procedure refers to sections in the *Network Management Guidelines* that provide the details required to perform each step in the process.

2. **Process Activities:**

   **Activity 1  Notify CPS about Proposed Donation**
   When CPS or school units are contacted by a potential donor, the donor should be directed to the Division of External Resources and Partnerships (DERP). Donors should contact Cynthia Greenleaf, Director of DERP at (773) 553-1547 or e-mail cgreenleaf@cps.k12.il.us for detailed guidance regarding the donation process. The donor will need to provide configuration details for the donated computers so the DERP can determine whether they meet CPS minimum standards or require some level of refurbishment in order to meet the minimum standards.

   **Activity 2  Process Donated Computers**
   DERP is responsible for processing the donated computers, including obtaining funds for refurbishment when necessary. The donor may select one or several schools to receive the computers. The division manages the coordination required to achieve the donor’s specific donation request.

   **Decision 1  Do the Donated Computers Need Refurbishment?**
   DERP reviews the minimum standard compliance of the donated computers to determine whether the computers need refurbishment, i.e., if they do not meet CPS minimum standards (see the CPS Network Policy at [http://www.cps.k12.il.us/Network_Standards.pdf](http://www.cps.k12.il.us/Network_Standards.pdf)). If the computers do not require refurbishment, the answer is NO; they are ready for deployment (go to step A3). If they do require refurbishment, the answer is YES (go to step D2).

   **Activity 3  Maintain and Provide CPS-Approved Script**
   The OTS Technical Group will maintain and provide the most current approved script to the school Technology Coordinator.
**Activity 4  Setup and Run Script on Computer at School**

The Technology Coordinator receives the CPS compliant computers from the donor via the coordination of DERP. The coordinator sets up the computers and runs the script. The details of this process can be found in the Technology Coordinator’s *Remediation Script Procedures* found in the “Leave Behind Packet.”

**Activity 5  Enter Computer Information into Technology Database**

The Technology Coordinator will then run a program that extracts select information about the computer and creates a file that is used to update the Technology Database automatically.

If the path of the flow did not require refurbishing, the process ENDS.

**Decision 2  Will the Donor Pay for Refurbishment?**

If the decision is made that the donated computers need refurbishment, then DERP will pursue funding for the refurbishment cost. If the donor or a donor’s associate agrees to pay for the refurbishment, then the answer is YES (go to step A6). If the donor declines to pay, the answer is NO (go to step D3).

**Activity 6  Refurbish Computers to CPS Standards**

The PC refurbishment vendor will provide the parts and labor to refurbish the computers to meet the CPS minimum standards as defined in the Network Policy. The vendor delivers the computers to the school(s) specified by the donor (go to step A4).

**Decision 3  Will the School Pay for Refurbishment?**

If the decision in D2 is NO, the donor will not pay for refurbishment of the donated computers, then DERP will pursue other donors or the school(s) for funding of the refurbishment cost. If the other donors or the school(s) agree to pay for the refurbishment, then the answer is YES and go to A6. If the answer is NO, the cost of refurbishment is not covered; go to D4.

**Decision 4  Find Other Refurbishment Pay Source?**

If the decision in D3 is NO, the school(s) will not pay for refurbishment of the donated computers, then DERP will pursue any remaining sources for the funding of the refurbishment cost. If a source(s) agrees to pay for the refurbishment, then the answer is YES (go to step A6). If the answer is NO, DERP will inform the donor and close out the process for the specific donation proposal. The donation is then cancelled.

*If the process did not obtain funding for the refurbishment cost, the process ENDS.*
## APPENDIX G: CPS Resources and Services

<table>
<thead>
<tr>
<th>Resource</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project C.L.E.A.R.</td>
<td><a href="http://clear.cps.k12.il.us">http://clear.cps.k12.il.us</a></td>
</tr>
<tr>
<td>Minimum Hardware, Software and Network Standards - <strong>Spring 2002 Update</strong></td>
<td><a href="http://www.cps.k12.il.us/Network_Standards.pdf">http://www.cps.k12.il.us/Network_Standards.pdf</a></td>
</tr>
<tr>
<td>Strategic Sourcing Vendors Listings (SSV)</td>
<td><a href="http://www.csc.cps.k12.il.us/purchasing/ss_Vendors.html">http://www.csc.cps.k12.il.us/purchasing/ss_Vendors.html</a></td>
</tr>
<tr>
<td>Department of Procurement and Contracts</td>
<td><a href="http://www.csc.cps.k12.il.us/purchasing/">http://www.csc.cps.k12.il.us/purchasing/</a></td>
</tr>
<tr>
<td>IP Addressing and Naming Configurations</td>
<td><a href="http://erate.cps.k12.il.us">http://erate.cps.k12.il.us</a></td>
</tr>
<tr>
<td>Virtual Private Network (VPN)</td>
<td><a href="http://vpn.cps.k12.il.us">http://vpn.cps.k12.il.us</a></td>
</tr>
<tr>
<td>Forms</td>
<td><a href="http://intranet.cps.k12.il.us/Forms">http://intranet.cps.k12.il.us/Forms</a></td>
</tr>
<tr>
<td>Instructional Intranet - CPS</td>
<td><a href="http://intranet.cps.k12.il.us/">http://intranet.cps.k12.il.us/</a></td>
</tr>
<tr>
<td>Technology</td>
<td><a href="http://intranet.cps.k12.il.us/Technology">http://intranet.cps.k12.il.us/Technology</a></td>
</tr>
<tr>
<td>OTS Technology Database</td>
<td><a href="http://erate.cps.k12.il.us">http://erate.cps.k12.il.us</a></td>
</tr>
<tr>
<td>Global Directory</td>
<td><a href="https://directory.cps.k12.il.us:8080/">https://directory.cps.k12.il.us:8080/</a></td>
</tr>
</tbody>
</table>