Meal Plan 2

Meat and Potato Public Computers

Taking the time to complete this meal plan will save you both time and maintenance costs in the long run. We hope this ultimately translates into better service for your patrons and fewer headaches for you.

This section details the elements you need to help you get through the process of managing and configuring your public computers.

TOPICS COVERED:

- A Well-Rounded and Balanced Computer Maintenance Diet
- Checking Your Chops—Are You Ready for Meal Plan 2?
- Two Square Meals You Shouldn’t Go Without: Computer Lock-Down and Disk-Protection
- First Course: Determine Your Library and Patrons’ Needs and Plan Accordingly
- Second Course: Install Antivirus and Anti-spyware Software
- Third Course: Lock-Down Your Computers
- Fourth Course: Install Disk-Protection Software
- Fifth Course: Image Your Computer’s Hard Drive
- Food for Thought—Public Computer Software Comparisons
- Fast Food—Meal Plan 2 Summary

Getting Your Computers to Act Like an Appliance

“Having your computers act like an appliance, where you turn them on and they just work is the main thing. Getting things stable, that’s where Deep Freeze or that multi-user toolkit come in. These can make your computer become more like an appliance, and minimize change. Because once you get your computers to that point . . . other than hardware failure . . . you can just walk away and let them do their thing.”

Anton Pintar
Calumet Public School Library, Calumet, MI
A Well-Rounded and Balanced Computer Maintenance Diet

Meal Plan 2 includes five courses that make up a well-rounded and balanced computer maintenance diet. One could pick and choose from this list, but we have found from other Chefs in a variety of rural libraries that things work best, if you follow all of these steps.

Here are the five key courses:

1. **Determine your library and patrons’ needs and plan accordingly** so you can identify the software and resources you would like to offer. Once you do that, you will be able to set up the security systems needed to plan for the public computer components that you would ideally like to provide, as well as the protections you need to keep computer maintenance manageable for you and your staff.

2. **Install antivirus and anti-spyware software** to help keep those downright nasty intruders out of your public computers and the rest of the computers on your network too.

3. **Lock-down your computers** to prevent patrons from doing damage to your hardware and/or software components...accidentally or intentionally. The thing to keep in mind is that you don't want to lock your computers down so tightly that they become less useful for you patrons. We reference a couple of articles in the "Other Tasty Recipes" section that discuss the issues around this. It is a balancing act between how much latitude to offer your patrons and how much you want to manage their access in order to make maintenance easier for you.

4. **Install disk-protection (reboot and restore) software** that allows you to capture the pristine “baseline” computer setup that you have when everything is working properly. If a patron opens an e-mail and a new virus hits one of your computers, not to worry. Restart the computer to make it disappear. The disk-protection automatically restores the computer system to the “baseline” setup. These tools are effective in cleaning patrons’ “tracks” on a computer, which in turn, helps you protect their privacy. You do not have to worry about “scrubbing” data—such as their web browsing history or saved passwords.

5. **Image your computer’s hard drive** to capture a “model” computer configuration and “clone” the rest of the computers. This saves you the time of configuring each computer individually. Images also act as a backup and recovery tool. If something really catastrophic happens—like hard drive failure — clone the computer to get a running start on getting the computer back online.
Checking Your Chops—Are You Ready for Meal Plan 2?

In order to do some of the courses in this meal plan, you should have some requisite "chops" or technical/computer knowledge. Here are a few guidelines for setting expectations around the competencies that can help you succeed.

In general, across all courses in Meal Plan 2, you should:

- Have a general comfort with computers and have previously installed software on a computer.
- Be able to get around the Windows operating system (e.g., you are familiar with tools such as My Computer and the Control Panel).
- Have administrator-level access to public computers for full control over system settings.

Before taking on the individual Meal Plan 2 courses, we suggest that you review the suggested prerequisite competencies list below. If, after reading this list, you are still not sure if you have the skills to complete the courses, go to a web site that offers the software you are interested in and review the product demos and user guides provided. These resources should give you a more detailed explanation of what it takes to install and configure these tools.

Ultimately, the best way to test and hone your computer chops is to get your hands dirty. If possible, set aside one or two older computers or assign a "learning" computer for you and your staff. A designated computer will allow you to try out the actions suggested in this Cookbook without the potential repercussions of downtime. Many vendors offer free, downloadable trial editions of their software that you can install and use on a limited basis. There is no better substitute for hands-on skill building when it comes to computers.

Here are some suggested competencies to successfully complete the Meal Plan 2 courses.

<table>
<thead>
<tr>
<th>MAINTENANCE AREA/TOOL:</th>
<th>COMPETENCIES:</th>
</tr>
</thead>
</table>
| Disk-Protection        | - Familiarity with the software components that require regular updating so that you can configure disk-protection to keep those changes (e.g., Windows updates, anti-virus definitions, MS Office updates).  
- An understanding that disk-protection greatly affects how the computer handles changes you make to a computer (e.g., patrons cannot save work to the protected system drive, you have to turn off disk-protection to install software).  
- Familiarity of hard drive partitioning so that you know which sections of a hard drive are protected and understand how to create parts that are unprotected to save work, if desired. For an overview of hard drive partitioning, see [http://en.wikipedia.org/wiki/Partition_(computing)](http://en.wikipedia.org/wiki/Partition_(computing)) |
<table>
<thead>
<tr>
<th>MAINTENANCE AREA/TOOL:</th>
<th>COMPETENCIES:</th>
</tr>
</thead>
</table>
| Lock-down computers   | - An understanding of computer user accounts and how they limit or grant access to various pieces of the computer's operation (e.g., an administrator should have the ability to change other users' passwords, but regular users should not be able to do this).
  - Familiarity with Microsoft Policies (or Group Policies) to modify user permissions and access is helpful. For an overview of Microsoft Policies, take a look at [http://www.infopeople.org/resources/security/workstation/policies.html](http://www.infopeople.org/resources/security/workstation/policies.html)
| Imaging and cloning   | - The capacity and the ability to manage large files (2 GB and greater) on various media (e.g., recordable DVDs, portable hard drives, servers). Imaging copies the contents of the whole hard drive to one file. This creates “big” files (anywhere from 2 GB on up, depending on what software you have installed on your computer).
  - Familiarity with hard drive partitioning to understand the sections of a hard drive being imaged. Some people will store a copy of an image on the hard drive of the computer, making it much easier to clone the computer if the need arises. It is important to maintain a copy of these images elsewhere as a backup. For an overview of hard drive partitioning, see [http://en.wikipedia.org/wiki/Partition_(computing)](http://en.wikipedia.org/wiki/Partition_(computing))
  - An understanding of available imaging and cloning tools. Some tools, especially older versions, may require the creation of bootable CDs, floppy disks, or flash drives. Newer versions of cloning software are more flexible and offer ways of imaging/cloning that don’t require boot disks. Most imaging software includes tools to create boot CDs.
  - An understanding of third-party imaging and cloning tools. For example, BartPE ([http://www.nu2.nu/pebuilder/](http://www.nu2.nu/pebuilder/)) is an outstanding and free boot CD creation tool, but requires advanced knowledge of Windows operating system and hardware device drivers. There are other options at [http://bootdisk.com](http://bootdisk.com). |
Two Square Meals You Shouldn’t Go Without: Computer Lock-Down and Disk-Protection

Two of the most valuable tools to help libraries maintain their public computers are computer lock-down and disk-protection software.

SAVING TIME AND MONEY ON ROUTINE MAINTENANCE

Lockdown and disk-protection tools can dramatically reduce the amount of time your staff will spend troubleshooting computer problems, not to mention the money you can save on aspirin for all the headaches that come with fixing those problems! Most importantly, these tools can also help reduce a number of regular, costly maintenance activities you need to perform for the health of your system. However, this does come with some up-front work and costs.

MAINTENANCE COMPARISON CHARTS

The charts on the following pages provide a breakdown of the regular computer maintenance tasks and costs required on a computer system. The first chart itemizes the maintenance plan for computers without lock-down and disk-protection software, while the second shows the appropriate tasks and cost after installing the software.

As demonstrated here, the benefits of using lock-down and disk-protection software are:

- Total monthly time savings per workstation, per month (not including time for installing and configuring lock-down and disk-protection software): **12 hrs.**
- Total monthly cost savings per workstation, per month (not including time for installing and configuring lock-down and disk-protection software): **$800 per workstation! (if you are using a technology contractor)**

Bottom Line... One month’s time/cost savings will more than pay for the initial costs of purchasing, installing, and configuring lock-down and disk-protection software on each computer.

OTHER TASTY RECIPES

- Managing Public Access Computers - Best Practices  
  [http://pacomputing.webjunction.org/do/home](http://pacomputing.webjunction.org/do/home)
Maintenance Tasks/Costs: Computers WITHOUT Lock-Down and Disk-Protection Software

Items that must be completed on a regular basis to maintain computers that are NOT locked down and do NOT have disk-protection.

* Monthly time does not include hours required on a quarterly and annual basis.

<table>
<thead>
<tr>
<th>AREA</th>
<th>WEEKLY</th>
<th>MONTHLY</th>
<th>QUARTERLY</th>
<th>ANNUALLY</th>
<th>MONTHLY TIME REQUIRED (PER COMPUTER)</th>
<th>OUTSIDE CONSULTANT @ $50 PER HR.</th>
</tr>
</thead>
</table>
| Security | ▪ Update virus definitions, and run a full antivirus system scan.  
▪ Update spyware definitions, and run a full anti-spyware system scan  
▪ 1 hr. | ▪ Change system passwords.  
▪ Visually inspect computers for signs of tampering.  
▪ 30 min. | ▪ Check for unneeded or unused applications and consider uninstalling them.  
▪ 15 min. | ▪ Renew antivirus software subscription.  
▪ 1 hr. | 4.5 hrs. | $225.00 |
| Computer | ▪ Run “ScanDisk” to check hard drive for errors.  
▪ Run “Defrag” to defragment files.  
▪ Run “Disk Cleanup” to delete Temporary Internet files, Temporary Files, and Recycle Bin.  
▪ Troubleshooting and fixing problems on computers  
▪ 2 hrs. | ▪ Check for the latest Service Packs/Updates for Windows, Office, and Internet Explorer.  
▪ Clean the mouse so it is free of dust and grime.  
▪ Make sure all the plugs are properly connected.  
▪ 1 hr. | ▪ Clean the screens with appropriate screen-cleaning cloth/solution.  
▪ Check printers. Print a test page to ensure printers are producing clean copies, and toner cartridges are full.  
▪ Clean the CD-ROM drive.  
▪ Check supplies (e.g., paper, cartridges, disks, etc.) and order as needed.  
▪ 30 min. | ▪ Check cables for crimps, breaks, wear and tear.  
▪ Clean inside PC.  
▪ Update drivers as needed for printers, modems, sound cards, video cards, and other devices.  
▪ 1 hr. | 9 hrs. | $450.00 |
| Internet | ▪ Clear browser history  
▪ Delete cookies  
▪ 15 min. | ▪ Identify policy and procedure issues  
▪ 1 hr. |  |  | 2 hrs. | $100.00 |
| Patrons | ▪ Restock:  
▪ Computer use policies and procedures  
▪ Instructional handouts for computer and Internet use  
▪ 30 min. | ▪ Review and update as needed:  
▪ Computer use policies and procedures  
▪ Patron instructional materials  
▪ 8 hrs. | ▪ Review and update as needed:  
▪ Library policies  
▪ Patron instructional materials  
▪ 32 hrs. |  | 30 min. | $25.00 |

**TOTAL MONTHLY PER COMPUTER**  
16 hrs.  
$800.00
## Maintenance Tasks/Costs: Computers WITH Lock-Down and Disk-Protection Software

Items that must be completed on a regular basis to maintain computers that ARE locked down and disk-protected.

* Monthly time does not include hours required on a quarterly and annual basis.

### TASK SCHEDULE

<table>
<thead>
<tr>
<th>AREA</th>
<th>WEEKLY</th>
<th>MONTHLY</th>
<th>QUARTERLY</th>
<th>ANNUALLY</th>
<th>MONTHLY TIME REQUIRED (PER COMPUTER)</th>
<th>OUTSIDE CONSULTANT @ $50 PER HR.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update virus definitions</td>
<td>Update spyware definitions</td>
<td>Change system passwords</td>
<td>Check for unneeded or unused programs and consider uninstalling them</td>
<td>Renew antivirus software subscription</td>
<td>1 hr. 30 min.</td>
<td>$75.00</td>
</tr>
<tr>
<td>15 min.</td>
<td></td>
<td>15 min.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Computer</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check for the latest Service Packs/ Updates for Windows, Office, Internet Explorer.</td>
<td>Clean the screens with appropriate screen-cleaning cloth/solution.</td>
<td>Check printers. Print a test page to ensure printers are producing clean copies, and toner cartridges are full.</td>
<td>Check cables for crimps, breaks, wear and tear.</td>
<td>1 hr.</td>
<td>$50.00</td>
<td></td>
</tr>
<tr>
<td>Clean the mouse so it is free of dust and grime.</td>
<td>Check printers.</td>
<td>Clean the CD-ROM drive.</td>
<td>Clean inside PC.</td>
<td>1 hr.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make sure all the plugs are properly connected.</td>
<td>Check printers.</td>
<td>Check supplies (e.g., paper, cartridges, disks, etc.) and order as needed.</td>
<td>Update drivers as needed for printers, modems, sound cards, video cards, and other devices.</td>
<td>1 hr.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 hr.</td>
<td></td>
<td>1 hr.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internet</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify policy and procedure issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 min.</td>
<td></td>
<td>15 min.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Patrons</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restock:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer use policies and procedures</td>
<td>Review and update as needed:</td>
<td>Computer use policies and procedures</td>
<td>Review and update as needed:</td>
<td>15 min.</td>
<td>$12.50</td>
<td></td>
</tr>
<tr>
<td>Instructional handouts for computer and Internet use</td>
<td>– Library policies</td>
<td>Patron instructional materials</td>
<td>– Patron instructional materials</td>
<td>15 min.</td>
<td>$12.50</td>
<td></td>
</tr>
<tr>
<td>15 min.</td>
<td></td>
<td>15 min.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL MONTHLY PER COMPUTER (after installation)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3 hours</td>
<td>$150.00</td>
</tr>
</tbody>
</table>

**Lock-down and disk-protection software install**  
One time installation: 6 hours for first computer, 2 hours for each add'l computer (not counted in total above)  
Approx. $45 - $90 for first computer, $30 for each add'l computer  
Lock-down and disk-protection software install  
One time installation: 6 hours for first computer, 2 hours for each add'l computer (not counted in total above)  
Approx. $45 - $90 for first computer, $30 for each add'l computer  
Lock-down and disk-protection software install  
Note: If you have Windows XP, you can use the free Windows SteadyState for locking down and disk protection.
First Course: Determine Your Library and Patrons’ Needs and Plan Accordingly

Before you set up and configure your computer for usability and security, you must first determine how much public computer access to offer. This may include such issues as which applications you offer, the kinds of content that patrons may download from the Internet (e.g., documents, music, videos, software applications), where they can save their work, etc. There are many choices to make. You should also assess your own needs, as well; particularly when it comes to managing and protecting your computers to keep them up and running at reasonable cost in terms of both time and money. This begins by making some decisions about what you will install on your computers, how to configure them, and how to manage patron use of computers.
FIRST COURSE: Determine Your Library and Patrons' Needs and Plan Accordingly

<table>
<thead>
<tr>
<th>EQUIPMENT AND INGREDIENTS:</th>
<th>TIME TO IMPLEMENT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A dash of diagnostic ability</td>
<td>2 to 8 hrs, depending on the number of patrons you are serving</td>
</tr>
<tr>
<td>A pinch of policy-making</td>
<td></td>
</tr>
</tbody>
</table>

PREPARATION

Computer use: Carefully consider the ways in which your patrons use the computers in your library. Think through the actions you must take to ensure usability and proper security. Ask yourself the following questions:

- What software applications do you want installed on your public computers? Some examples are:
  - Office productivity software (e.g., Microsoft Office, OpenOffice, etc)
  - Games
  - What web browsers (e.g., Internet Explorer, Mozilla, Safari, etc)
  - Antivirus or anti-spyware

- Should user access be the same for everyone? User accounts should be segmented by different patron groups, (e.g., you may want several different patron accounts—one for children, one for young adults, one for adults, etc.)

- Where do patrons save their work, such as resumes or school reports? Our world class Chefs recommend that you have patrons save work on their own media, such as a flash drive, or even online (in a pinch, a patron can send an e-mail to him or herself with the file attached). This way, the responsibility of saving data and keeping it safe resides with the patron, not with the library. It should be made clear to users that they cannot save work on the public computers. Libraries might want to keep a stash of flash drives or recordable CDs on hand which patrons can purchase and use to save their work. There are also web-based services available that allow patrons to store limited amounts of information for free. As an example, Box.net (http://www.box.net/info/pricing-plans) allows up to 1GB and XDrive (http://www.xdrive.com/) offers 5 GB free.

Computer policies: Once you have determined your patron and library needs and have assessed how you want to configure your computers, your next tasks is to create guidelines and policies to document and communicate an agreement between you and your patrons about computer usage. Take the time to sit down together with your library staff and create an acceptable-use policy. By documenting the expectations and rules around your computers for patrons and staff, you will be ahead of the game when it comes time to making decisions around some of the next steps, such as locking down and disk-protecting your computers. Remember, your policy should grow out of your library's particular needs to maintain your computers and serve your patrons' needs.
OTHER TASTY RECIPES

Here are some resources and actual policies viewable on the Internet. Use these to get an idea of what a policy looks like and what issues you might cover.

- Web Junction's Acceptable Use and Computer Policies page
  http://webjunction.org/do/Navigation;jsessionid=88265243D7284B2518D5EC0FC2AA166?category=394

- Rural Library Examples
  SCRLD Public IP Network Terms of Service and Acceptable Use Policy
  https://ssl.publicip.net/legal/zone_terms.php?remote=5482
  http://www.scrld.org/Library_info/Policies/0013ElecAccess.htm

- Milwaukee Public Library
  A more complete policy from a multi-branch city system
  http://www.mpl.org/FILE/computer_policy.htm

- West Lafayette Public Library Computer Use Policy
  A simpler, but still comprehensive policy
  http://www.wlaf.lib.in.us/computerusepolicy.html

A Patron Needs Balancing Act

“I am trying to learn how to allow patrons to download to their iPods, flash drives, and all that kind of good stuff, without jeopardizing the safety of my systems — the worms or spyware...you know, viruses and that type of thing. I'm nervous about letting somebody walk in off the street with a drive full of information and just attach it to my computer. And yet, that's what the public is demanding.”

Susan Ryals
Vinita Public Library, Vinita, OK
Second Course: Install Antivirus and Anti-spyware Software

The first two components that you install on your computer should be antivirus and anti-spyware software.

Disk-Protection is designed to make it easy to revert back to a healthy, baseline computer configuration. So, if you encounter problems with your computer — like a virus — a restart of the computer should allow you to make a full recovery of your system and rid your computer of the virus. **If you have disk-protection installed, do you really need to install antivirus software?**

The answer is “yes.” Many viruses — and their counterparts, worms and spyware — are designed to spread over computer networks. So, if one of your computers gets infected, it puts the other computers on your network at risk. Every library computer connected to the Internet should have antivirus and anti-spyware software installed. You are protecting patrons and other users on the Internet from harmful viruses and spyware, which are designed to propagate to other computers, steal passwords, track web surfing activity, send spam, etc. Antivirus and anti-spyware protects computer users, as well as the computers themselves.

Also, if the public computers in your library do not have antivirus or anti-spyware installed and they share the same network with staff computers that don't have disk-protection, it leaves the public computers in a more vulnerable position.

**Virus Protection and Ongoing Vigilance**

*Notes from a Chef*

“The only time we’ve ever had a virus is when I didn’t put antivirus software on a public computer that we had moved. The computer was donated to us, and when we put it into service, we waited a week before I got that antivirus on there, but it was already full of viruses. That’s the only time we’ve ever had any trouble like that.”

Mary Alice McLeod
Cherokee City Library, Cherokee, OK
SECOND COURSE: Install Antivirus and Anti-spyware Software

EQUIPMENT AND INGREDIENTS:
- Antivirus software
- Optional: Anti-spyware software

TIME TO IMPLEMENT:
- 30 minutes to 1 hour

PREPARATION

- **Virus protection:** It is advised by Chefs "in the know" that you install antivirus software on all your library’s computers. Many new computers come with antivirus software packages. In fact, it has become standard equipment on Windows computers.

- **Spyware protection:** Even though antivirus software has improved when it comes to picking up and squashing spyware (nasty software that monitors user behavior), it's not a bad idea to also install some spyware protection on your computers. There are several free spyware protection offerings, such as Spybot Search & Destroy and Microsoft Windows Defender. As with every type of software, the best anti-spyware solution changes frequently, and you often receive better protection when you pay some money. So if you want the latest information about anti-spyware utilities, or if you want to know more about fee-based software, check out the reviews at PC Magazine.

OTHER TASTY RECIPES

- PC Magazine Spyware Reviews  
  http://tinyurl.com/24zj8x

- Infopeople’s Antivirus Software Overview  
  http://www.infopeople.org/resources/security/general_security/desktop_antivirus.html

- Symantec Antivirus  
  http://www.symantec.com/smb/products/overview.jsp?pcid=vir_prot&pvid=av_corp

- Spybot Search & Destroy  

- Microsoft Windows Defender  
  http://www.microsoft.com/athome/security/spyware/software/default.mspx

- Symantec’s Overview of Common Security Threats  
Third Course: Lock-Down Your Computers

Lockdown (access control) software allows libraries to more easily manage the level of access a user has on a public computer. In short, it keeps patrons from making harmful changes (accidentally or intentionally) to your computers. For example, patrons might delete key operating system files, change passwords, or run unauthorized programs. In addition, some lockdown software tools also include features that help you manage patron usage (e.g., features such as session timers and library card authentication).

Notes from a Chef

“Early on, the White Plains Public Library identified several major challenges to maintaining computer availability. We needed to make sure that we lock-down our computers so that patrons can only access Library-approved web sites, and not access software or applications on the PC or network, and/or make changes to configurations or settings. We also recognized the importance of automatically starting and logging into our computers in the morning, and shutting them down in the evenings.”

Kurt Hadeler
White Plains Public Library, White Plains, NY
THIRD COURSE: Lock-Down Your Computers

EQUIPMENT AND INGREDIENTS:
- A plan and policies to guide your computer lock-down configuration
- Lockdown software

TIME TO IMPLEMENT:
2 to 3 hours for the first computer; 2 hours on additional computers if you take advantage of replication methods such as copying settings files or cloning (See Fifth Course: Image Your Computer’s Hard Drive on page 40 of this Cookbook.)

PREPARATION

Listed below are some actions you can take to lock-down your public computers and make them more foolproof. Although some of the tools discussed here include “templates” or recommended configurations, they also present a number of options when it comes to locking down specific parts of the computer. So, clear policies and a plan of how much you want to permit and/or restrict will help to better utilize these applications.

- **Workstation lockdown applications:** There are a number of tools now available to help manage public computer use. Among other features, these applications help “cage in” patrons to a limited number of available functions. For example, these tools will allow a patron to launch Internet Explorer for access to the Internet and to a word processor, but not anything else. This is especially true for administrative tools such as system files and the Control Panel. These applications may also include other patron management features such as session timers and printing management.

- **Prohibiting application launch:** An interesting application that several library staff members have recommended is the free, downloadable Trust-no-exe. An “exe” is “tech speak” for a file that launches an application. This utility allows you to predetermine the type of application that can be launched on a computer, allowing you to prevent patrons from executing downloaded software or bringing in unauthorized software on removable media such as flash drives or CDs. This type of feature is also included in some of the other lockdown software mentioned above. For some small libraries with tight budgets, however, and/or those who may not need all the other features included in the other more “comprehensive” software packages, this little application might serve you well.

- **The public web browser:** This tool cracks open the hood of Internet Explorer. It provides very granular control of many pieces of the web browser, including menu items and toolbar buttons, and hundreds of other options. By editing a single text file, you have access to literally hundreds of options, a list which may be a little intimidating at first.
Basic Input Output System (BIOS) Lockdown: The BIOS hosts the most fundamental information your computer needs to get itself up and running. It contains a number of configurable options that change how a computer behaves, which could lead to trouble. For example, there is a setting to require a password when the computer powers on. This can be very dangerous if it's set without your knowledge. It could render your computer unusable. See InfoPeople’s Overview of the BIOS link below for more information.

In order to make any changes to the BIOS, you should set a password. This can help prevent unauthorized access to the BIOS. Some of the workstation lockdown software tools mentioned here provide BIOS lockdown features. A very powerful feature is the keyboard shortcuts, which give you access to administrative functions such as logging off the current user or restarting the computer. This way, you can use lock-down tools to limit functionality (e.g., remove “log off” and “shutdown” options from Start Menu to prevent patrons from accidentally turning off the computer), but ensure that you and your staff still have easy access to these functions, provided you know the shortcut and the password.

The Right Tools—The Right Access

We want to give them access to what patrons need, not necessarily what they want. There is a difference. What they need is what you want to give them, but you don’t want them exploring around your computer network or messing with files in My Computer. All those things can be locked down; you give them access to the things that they need.”

Rodney Greensage
Alamo Regional Library System, TX.

OTHER TASTY RECIPES

Here are some links to the lockdown software just discussed. Please take a look for further reading.

TechSoup and WebJunction also offer an article that discusses issues around public access security at
http://www.techsoup.org/learningcenter/techplan/page4892.cfm?cg=searchterms&sg=lock%20down

- Fortres Grand 101

- CybraryN
  http://www.cybraryn.com/

- Microsoft Windows SteadyState for Windows XP
  http://www.microsoft.com/windowsxp/sharedaccess/default.mspx

- CASSIE
  http://www.librarica.com/

- Library Metricks
  http://www.librarymetricks.com/
- Trust-no-exe
  http://www.beyondlogic.org/solutions/trust-no-exe/trust-no-exe.htm

- Public Web Browser
  http://www.teamsoftwaresolutions.com/

- Infopeople’s Overview of the BIOS
  http://infopeople.org/resources/security/workstation/bios.html
Fourth Course: Install Disk-Protection Software

So you forgot to cover the soufflé and it collapsed right before your big dinner party. Now what can you do? Not much…the damage is pretty much done.

But, disk-protection can do for your computer what you can’t for that soufflé. It’s a powerful tool that helps you quickly recover from computer mishaps and meltdowns. When you restart the computer, it returns to the point where disk-protection was turned on. This is sometimes referred to as “reboot-to-restore” software or rollback software. We cannot stress enough how valuable this tool is for libraries in terms of reducing their maintenance costs. This is especially true for the small rural library that often doesn’t have the resources nor time to perform maintenance. It helps minimize the troubleshooting and repairs you have to perform on computers. For some libraries, the simple act of restarting the computers may be the most effective maintenance and troubleshooting technique…thanks to disk-protection software.
FOURTH COURSE: Install Disk-Protection Software

EQUIPMENT AND INGREDIENTS:
- Disk-protection software
- Computers with a “baseline” configuration

TIME TO IMPLEMENT:
2 to 3 hours (after you’ve configured computer to baseline)

PREPARATION

Disk-protection is a way to revert back to the way a computer was configured at a particular point in time. Ideally, you want to start off with a solid configuration that has all the elements to serve your patrons well. This is the configuration that disk-protection will revert back to when you restart your computer.

- Take some time to plan and think about all the elements you want to have on these computers before installing disk-protection. These include:
  - Patron-use software such as office productivity software, games, or alternative browsers such as the Public Web Browser
  - Antivirus or anti-spyware software policies that you use to customize the look-and-feel of the computers
  - Accounts for patron use (e.g., you may want several different patron accounts—one for children, one for teens, one for adults, etc.)
  - Patron management and lock-down software such as the Fortres 101, CybraryN, or CASSIE

- Set up your public computer accordingly, so that changes to the computer will not stick. This brings up some issues that do not apply to a “normal” computer setup. For one thing, as mentioned previously in this section, patrons wishing to save work or downloads from the Internet should use their own media or online. If they save on a disk-protected computer, it will get wiped away when the computer restarts.

  Also, by nature, disk-protection makes it harder for you to change your public computer’s configuration. You must turn disk-protection off before you install new software or upgrade software. For example, if you want to upgrade Microsoft Office to the new version, you will have to turn disk-protection off before you can install it, then turn it back on once its installed.

- If your patrons use a certain kind of software that needs to update configuration information as it is used, configure your setup to accommodate that. For example, a typing tutor program might include a feature that saves the progress of its students so when they return at a later date to do more exercises, the program will know where the student left off. If you don’t configure the typing tutor software to save this progress data to an unprotected area, disk-protection will wipe out this information when you restart the computer. How disappointed your hard working typing students would be!
Along with planning, test the disk-protected setups to make sure things are working as intended, especially after you restart your computer. First, test the computers yourself. Once this is done, ask one or more of your patrons to sample the computer with the new features and setup. If the patrons identify problems, you can address them before installing and setting up the other public computers.

Rebooting Saves Us!

“We’ve never had any real issues with our computers because we can wipe and reboot. All of our public machines are secluded from our staff network so if we end up with someone downloading a virus of some sort, we reboot and they’re fine.”

Josh LeBlanc
Jackson Parrish Library, Jonesboro, LA

Putting It in the Deep Freeze

“I personally consider Deep Freeze to be a big contributing factor in the way that our Internet usage has skyrocketed in the past year - from around 13000 in 2004-05, to over 18000 in 2005-06 and... those figures just keep getting better. This is because the computers are working all the time and not sitting on my desk being worked on!”

Terry Caudle – Hopkins County
Madisonville Public Library (KY) (courtesy of WebJunction: http://webjunction.org/do/DisplayContent?id=14253)

“We use Deep Freeze, which is a program that freezes our system so that changes cannot be made by anyone other than the IT person. A password is entered and the computer stays placed in a thawed state. Then I make any needed changes, put the computers back into the frozen state and reboot. So far this has worked very well in maintaining the security on our system.”

Mindy Farley
Barton Library, El Dorado, Arizona

OTHER TASTY RECIPES

Here are links to some of the disk-protection software just mentioned.

- Faronics Deep Freeze

- Centurion Technologies CenturionGuard
  http://www.centuriontech.com/products/centurionguard

- Centurion Technologies CompuGuard Cornerstone
  http://www.centuriontech.com/products/compuguardcornerstone/

- Fortes Grand Clean Slate

- Microsoft Windows SteadyState
  http://www.microsoft.com/windowsxp/sharedaccess/default.mspx
Fifth Course: Image Your Computer’s Hard Drive

Hard drive failure is one situation in particular where disk-protection cannot save you, but cloning can. If the hard drive on your computer dies, you can replace it and clone it to get it back up and running.

Cloning:

- Offers a way to take a “snapshot” of a computer’s configuration. With this snapshot you can easily re-install the computer configuration if something really goes wrong.
- Should be used to complement disk-protection, not replace it.
- Allows you to “clone” one computer’s setup to another similar computer disk-protection, workstation lockdown — all of this takes time to configure correctly.
- Provides a way of replicating those difficult setups to your other computers, and as a result, saving you valuable time.

Computer Cloning is Worth Paying For

“When we did the last server upgrade, we needed to Ghost all of our computers. I brought someone in to help with that, because it was just too large of a project. I’m a believer in looking at cost-benefit ratios, and that sometimes it just makes more sense to pay someone to set things up properly.”

Lesley Kimball
Wiggin Memorial Library, Stratham, NH
FIFTH COURSE: Image Your Computer’s Hard Drive

EQUIPMENT AND INGREDIENTS:
- Imaging software
- Large amount of disk space to store public computer disk images (5-10 GB per image)

TIME TO IMPLEMENT:
2 to 3 hours

PREPARATION

Use Imaging software such as Symantec Ghost and Acronis True Image. This allows you to take an exact image of a hard drive and copy it on the other computer (the clone). It’s designed to help you install software on one computer and configure it just the way you want it, make an image of it, and clone the rest of the computers. In short, the idea is to build one computer, and clone many of the same. (See the TechSoup article links below for more detail on cloning.)

Remember… Cloning works best when you have identical computers (same make, model, and configuration). The more diverse your public computers are, (e.g., many models of computers, different sets of software installed on each computer, etc.), the less effective cloning becomes. The more images you need to make to reflect the array of computers you have also increases the space requirements to store the large files, such as on recordable DVDs, an external hard drive, or a server.

OTHER TASTY RECIPES

- Description of Cloning
  http://www.techsoup.org/learningcenter/software/page6684.cfm?cg=searchterms&s g=cloning>

- WebJunction Overview of Cloning and Issues to Consider:
  http://www.techsoup.org/learningcenter/software/page6684.cfm

- Symantec Ghost
  http://www.symantec.com/enterprise/products/overview.jsp?pcid=1025&pvid=865_ 1

- Acronis True Image
  http://www.acronis.com/enterprise/products/ATICW/

- DriveImage XML
  http://www.runtime.org/dixml.htm

- Storage Device Example
  http://www.techsoup.org/stock/product.asp?catalog%5Fname=TechSoupMain&key word=network%20storage&product%5Fid=G40279&cg=searchterms&sg=network %20storage
Public Computer Software Comparison Chart

Library public computers aren’t like most “normal” computers. You depend on them to be extra resilient and also very rigid at the same time. Fortunately, there are many great software tools to help you maintain these computers.

The chart on the following pages compares some of the better-known titles that are currently in use in small libraries. We’ve grouped them by family, based on the most prominent public computers’ management features. The pricing and support terms reflect discounts for public library licensing and 15 workstations (where applicable).

Software families and common features:

- **Time management software** offers session time and print management, workstation reservations, public computer usage reporting.
- **Disk-protection** preserves a computer’s baseline configuration and restores it upon restarting or logoff.
- **Workstation lock-down** restricts patron access to a limited number of functions (e.g., web browsing, word processing), tailors the look and feel of desktop and menus, and prevents access to files and folders.
- **Application launch restriction** prevents patrons from launching unapproved applications (e.g., downloaded or brought in on removable media).
- **Web browser customization** modifies the way Internet Explorer looks and locks down its functionality.
- **Workstation remote control and administration** allows library staff to see and interact with the workstation desktop to make changes, troubleshoot, or assist a patron.
- **Patron privacy and data cleanup** can clean patron tracks (e.g., web browsing history, web site usernames/passwords, cookies).

We’ve placed each software program in the family where we believe it has the strongest features; however, please note that some of the features overlap into other categories. We’ve identified these with footnotes, as appropriate.

For filtering software, take a look at this chart: [http://libraryfiltering.org/](http://libraryfiltering.org/).
## Public Computer Software Comparison Chart

<table>
<thead>
<tr>
<th>TYPE OF SOFTWARE</th>
<th>SOFTWARE PUBLISHER AND TITLE</th>
<th>APPROXIMATE COST</th>
<th>INCLUDED SUPPORT, MAINTENANCE, AND SOFTWARE UPGRADE TERMS</th>
</tr>
</thead>
</table>
| **Patron Management** | Librarica CASSIE  
Supports: Windows 95, 98, NT, 2000, XP, 2003, Vista  
Feature list: [http://www.librarica.com/features.html](http://www.librarica.com/features.html) | $995 for 5 workstations  
$1,990 for 10 workstations  
$2,485 for 15 workstations | One year phone, e-mail, online help documentation support (add additional years for 15% of licensing cost per year) |
| | CybraryN Library Solutions¹  
Supports: Windows 98, ME, NT, 2000, XP  
Feature list: [http://www.cybraryn.com/Solutions/](http://www.cybraryn.com/Solutions/) | $774.95 for 5 workstations  
$1,074.95 for 10 workstations  
$2,519 for 15 workstations | One year phone, e-mail, online help, documentation and remote assistance support (add additional years for $375, according to number of workstations) |
| | Userful DiscoverStation¹²³⁴  
Supports: Linux-based thin-client w/ included hardware  
Feature list: [http://userful.com/products/library-ds](http://userful.com/products/library-ds) | $1,740 / year for 5 workstations  
$3,480 / year for 10 workstations  
$5,220 / year for 15 workstations  
(all rates based on 3-year term agreement) | Phone, e-mail, online help, documentation, and remote assistance support |
| | Fortres Grand Time Limit Manager  
Feature list: [http://www.fortresgrand.com/products/tlm/tlm.htm](http://www.fortresgrand.com/products/tlm/tlm.htm) | $125 for 5 workstations  
$250 for 10 workstations  
$195 for 25 workstations | Lifetime phone, e-mail, online help, and documentation support |
| **Disk-Protection** | Faronics Deep Freeze STD  
Supports: Windows 95, 98, ME, 2000, XP, Vista  
$236 for 10 workstations  
$334.90 for 15 workstations | One year phone, e-mail, online help, and documentation support (add additional years for $44, up to three years) |
| | Fortres Grand Clean Slate  
Supports: Windows 2000, XP  
$590 for 10 workstations  
$335 for 15 workstations | Lifetime phone, e-mail, online help, and documentation support |
| | Faronics Deep Freeze Mac  
Supports: Mac OS 10.3 and 10.4  
$364 for 10 workstations  
$516 for 15 workstations | One year phone, e-mail, online help, and documentation support (add additional years for $68, up to three years) |
| | Centurion Technologies CompuGuard CornerStone  
Supports: Windows 2000, XP  
Feature list: [http://www.centuriontech.com/products/compuguardcornerstone](http://www.centuriontech.com/products/compuguardcornerstone) | $462 for 15 workstations | One year phone, e-mail, online help, and documentation support (additional years at 10% of license cost per year) |
<table>
<thead>
<tr>
<th>TYPE OF SOFTWARE</th>
<th>SOFTWARE PUBLISHER AND TITLE</th>
<th>APPROXIMATE COST</th>
<th>INCLUDED SUPPORT, MAINTENANCE, AND SOFTWARE UPGRADE TERMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk-Protection (continued)</td>
<td>Centurion Technologies MacShield Universal Supports: Mac OS 10.3 and 10.4 Feature list: <a href="http://www.centuriontech.com/products/macshielduniversal/">http://www.centuriontech.com/products/macshielduniversal/</a></td>
<td>$453.75 for 15 workstations</td>
<td>One year phone, e-mail, online help, and documentation support (additional years at 10% of license cost per year)</td>
</tr>
<tr>
<td></td>
<td>Faronics Deep Freeze STD Supports: Windows 95, 98, ME, 2000, XP, Vista Feature list: <a href="http://www.faronics.com/html/deepfreeze.asp">http://www.faronics.com/html/deepfreeze.asp</a></td>
<td>$219 for 5 workstations $236 for 10 workstations $334.90 for 15 workstations</td>
<td>One year phone, e-mail, online help, and documentation support (add additional years for $44, up to three years)</td>
</tr>
<tr>
<td></td>
<td>Faronics WINSelect&lt;sup&gt;3&lt;/sup&gt; Feature list: <a href="http://www.faronics.com/html/Winselect.asp">http://www.faronics.com/html/Winselect.asp</a></td>
<td>$295 for 5 workstations $590 for 10 workstations $335 for 15 workstations</td>
<td>Through next version (typically two year lifecycle per version) phone, e-mail, online help, and documentation support</td>
</tr>
<tr>
<td></td>
<td>Faronics Anti-executable standard Supports: Windows 95,98,ME, 2000, XP Feature list: <a href="http://www.faronics.com/html/AntiExec.asp">http://www.faronics.com/html/AntiExec.asp</a></td>
<td>$179 for 5 workstations $236 for 10 workstations $398 for 15 workstations</td>
<td>One year phone, e-mail, online help, and documentation support (add on up to three years for additional fees, according to number of workstations)</td>
</tr>
<tr>
<td>Web Browser Customization</td>
<td>TeamSoftware Solutions Public Web Browser Supports: Windows 95, 98, ME, NT, 2000, XP, 2003, Vista Feature list: <a href="http://www.teamsolutions.com/">http://www.teamsolutions.com/</a></td>
<td>$125 for one year, renewable site license</td>
<td>E-mail, pager, online help, and documentation and discussion forum support</td>
</tr>
</tbody>
</table>
Public Computer Software Comparison Chart (continued)

<table>
<thead>
<tr>
<th>TYPE OF SOFTWARE</th>
<th>SOFTWARE PUBLISHER AND TITLE</th>
<th>APPROXIMATE COST</th>
<th>INCLUDED SUPPORT, MAINTENANCE, AND SOFTWARE UPGRADE TERMS</th>
</tr>
</thead>
</table>
| Workstation Remote Control and Administration | GoToMyPC  
Supports: Windows 2000, XP, Vista  
Feature list: [https://www.gotomypc.com/en_US/personalFAB.tmpl?_sid=209346628%3AFE2219DAD0D8CF8](https://www.gotomypc.com/en_US/personalFAB.tmpl?_sid=209346628%3AFE2219DAD0D8CF8) | $777/year for 5 workstations  
$1554/year for 10 workstations  
$2,025/year for 15 workstations | One year phone, e-mail, online help, and documentation support                  |
| VNC  
Supports: Windows 98, ME, 2000, XP, Mac OS 9 and 10.x, Unix, Linux  
(various sites, e.g., [http://www.realvnc.com/](http://www.realvnc.com/)) | Free download | Online help, and documentation support                                           |
| LogMeIn  
Supports: Windows 98, 200, 0, XP, 2003  
Feature list: [https://secure.logmein.com/go.asp?page=products_free](https://secure.logmein.com/go.asp?page=products_free) | Free for LogMeIn Free version | Phone (leave message for call back), e-mail, online help, and documentation support |
| Patron Privacy Data Cleanup | CCleaner  
Supports: Windows 95, 98, ME, NT, 2000, XP, 2003, Vista  
Feature list: [http://ccleaner.com/features.aspx](http://ccleaner.com/features.aspx) | Free download | Online help documentation and discussion forum support                           |

NOTES

1Includes some workstation lockdown features  
2Includes disk-protection functionality  
3Includes some patron management features  
4Requires Linux/Unix  
5Requires Windows XP Service Pack 2

A note about the listed costs: These are prices as reported by the respective vendors in April, 2007. Prices are subject to change, please contact vendor for current rates. In addition, you should always discuss your specific situation with the vendor to get the most appropriate package and pricing for your library.
Fast Food—Meal Plan 2 Summary

- Before taking on the individual Meal Plan 2 courses, make sure you have the right skills, or get someone with the appropriate skills to help you. (See Competency Charts on pages 22 through 23). In general, across all courses in Meal Plan 2, you should:
  - Have a general comfort with computers and have previously installed software on a computer.
  - Be able to get around the Windows operating system (e.g., you are familiar with tools such as My Computer and the Control Panel).
  - Have administrator-level access to public computers for full control over system settings.

- Lockdown and disk-protection tools can dramatically reduce the amount of time your staff will spend troubleshooting computer problems, not to mention the money you can save on aspirin for all the headaches that come with fixing those problems.

- Know the time and cost savings benefit of using lock-down and disk-protection software. One month’s time/cost savings will more than pay for the initial costs of purchasing, installing, and configuring lock-down and disk-protection software on each computer.

<table>
<thead>
<tr>
<th>MENU 2 CHECKLIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine your library and patrons’ needs and plan accordingly so you can identify the software and resources you would like to offer your patrons.</td>
</tr>
<tr>
<td>Consider the ways in which your patrons use your computers in your library.</td>
</tr>
<tr>
<td>Think through the actions you must take to ensure usability and proper security.</td>
</tr>
<tr>
<td>Create guidelines and policies to document and communicate an agreement between you and your patrons about computers usage.</td>
</tr>
<tr>
<td>Install antivirus and anti-spyware software to help keep intruders out of your computers.</td>
</tr>
<tr>
<td>Lock-down your computers to prevent patrons from doing damage to your hardware and/or software components…accidentally or intentionally.</td>
</tr>
<tr>
<td>Establish clear policies and a plan of how much you want to permit and/or restrict patron access.</td>
</tr>
<tr>
<td>Select and use appropriate lock-down software tools to manage patron usage.</td>
</tr>
<tr>
<td>Install disk-protection (reboot and restore) software that allows you to capture the pristine “baseline” computer setup that you have when everything is working properly.</td>
</tr>
<tr>
<td>Take some time to plan and think about all the elements you want to have on these computers before installing disk-protection.</td>
</tr>
<tr>
<td>Set up your public computer accordingly, so that patron changes to the computer will not stick.</td>
</tr>
<tr>
<td>MENU 2 CHECKLIST (continued)</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>☐ If your patrons use a certain kind of software that needs to update configuration information as it is used, configure your setup to accommodate that.</td>
</tr>
<tr>
<td>☐ Along with planning, test the disk-protected setups to make sure things are working as intended, especially after you restart your computer.</td>
</tr>
<tr>
<td>☐ Image your computer’s hard drive to capture a “model” computer’s configuration and “clone” the rest of the computers.</td>
</tr>
<tr>
<td>☐ Use imaging software such as Symantec Ghost and Acronis True Image.</td>
</tr>
</tbody>
</table>